UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010

CONFIRMATION NO. 3271

30565
WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

PUBLICATION NOTICE

OC10000000075162319

Date Mailed: 07/15/2024

Title:METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Publication No.US-2024-0214830-A1
Publication Date:06/27/2024

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be viewed using the USPTO's publicly available Searchable Databases via the Patent Public Search tool at www.uspto.gov. The direct link to access the Patent Public Search tool is currently https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through Patent Center, the USPTO's electronic patent application filing and management system. The direct link to access this status information is currently https://patentcenter.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of Patent Center.

Further assistance in electronically accessing the publication, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010

CONFIRMATION NO. 3271

30565
WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

PUBLICATION NOTICE

OC10000007439530

Date Mailed: 06/28/2024

Title:METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Publication No.US-2024-0214830-A1
Publication Date:06/27/2024

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be viewed using the USPTO's publicly available Searchable Databases via the Patent Public Search tool at www.uspto.gov. The direct link to access the Patent Public Search tool is currently https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through Patent Center, the USPTO's electronic patent application filing and management system. The direct link to access this status information is currently https://patentcenter.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of Patent Center.

Further assistance in electronically accessing the publication, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010	3271

30565 7590 06/18/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EXAMINER	
KHAWAR, SAAD	

ART UNIT	PAPER NUMBER
2412	

NOTIFICATION DATE	DELIVERY MODE
06/18/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketDept@uspatent.com

APPLICATION NO.	ISSUE DATE	PATENT NO.
18/594,375	18-Jun-2024	12015933

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	06/18/2024	12015933	020505-000010	3271

30565 7590 05/29/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (https://patentcenter.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

Sai C. Manapragada, Cypress, TX;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

XiFi Networks R&D Inc., Cypress, TX

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700
Indianapolis, IN 46204-5137

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Blake R. Hartz	(Typed or printed name)
/Blake R. Hartz, Reg. No. 73453/	(Signature)
May 9, 2024	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
18/594,375	March 4, 2024	MANAPRAGADA, Sai C.	020505-000010	3271

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$ 480.00	$ 0.00	$ 0.00	$ 480.00	August 1, 2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
KHAWAR, Saad	2412	370-315000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Woodard, Emhardt, Henry, Reeves & Wagner, LLP
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: XiFi Networks R&D Inc.

(B) RESIDENCE: (CITY and STATE or COUNTRY): Cypress, TX

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. Fees Submitted: ☑ Issue Fee ☑ Publication Fee (if required)

4b. Method of Payment (*Please first reapply any previously paid fee shown above*):

☑ Electronic Payment via Patent Center or EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 233030

5. Change of Entity Status (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29. NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

Applicant asserting small entity status. See 37 CFR 1.27. NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature	/Blake R. Hartz, Reg. No. 73453/	Date	May 9, 2024
Typed or printed name	Blake R. Hartz	Registration No.	73453

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	05/09/2024 11:32:09 AM Z ET	020505-000010

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	65440361	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	03/04/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	E202459B33415073	WALTER MOORE

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2501	UTILITY ISSUE FEE	480.00	1	480.00
			TOTAL AMOUNT:	$480.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	**05/09/2024 11:32:09 AM Z ET**	**020505-000010**

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	65440361	FILING DATE	03/04/2024
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
20505-10 part b fee transmittal.pdf	1	Issue Fee Payment (PTO-85B)	489 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
20505-10 part b fee transmittal.pdf	82A3BDB362D8592C55C45F22E0F79DCB3A122DEEE1EFCA7E6EC3E22883B4BF60407BF9DFB4F6717693817ACE3C4BFA4ECCD5139A691D2E33619A2971122118B4

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

TO: DocketDept@uspatent.com
FROM: noreply@uspto.gov
CC: patentcenter_eofficeaction@uspto.gov
SUBJECT: USPTO: Patent Electronic System - e-Postcard Notification for Customer Number 30565

Wed May 08 05:04:39 EDT 2024

Dear Patent Center Customer:

Correspondence Address:

WOODARD, EMHARDT, HENRY, REEVES &WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS,INDIANA,46204-5137
UNITED STATES

An email notification regarding the correspondence was sent to the following email address(es) associated with customer number 30565:

DocketDept@uspatent.com

This is a courtesy reminder that new correspondence is available for the application. If you have not done so already, please review the correspondence listed below. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Application	Document	Mailroom Date	Attorney Docket No.
18594375	NOA	05/01/2024	020505-000010
18594375	1449	05/01/2024	020505-000010

To view your correspondence online, please sign in to Patent Center and then select Workbench/View correspondence. Or to update your email addresses, select Manage/Manage customer numbers.

If you have any questions, please contact the Patent Electronic Business Center (EBC) at ebc@uspto.gov or 866-217-9197 Monday – Friday, 6 a.m. to midnight ET.

Please do not reply to this email as it was sent from an unmonitored mailbox.

Sincerely,

The Patent Center Team

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

30565 7590 05/01/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EXAMINER	
KHAWAR, SAAD	
ART UNIT	PAPER NUMBER
2412	

DATE MAILED: 05/01/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010	3271

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	08/01/2024

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

30565 7590 05/01/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010	3271

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	08/01/2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
KHAWAR, SAAD	2412	370-315000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via the USPTO patent electronic filing system ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010	3271

30565 7590 05/01/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EXAMINER	
KHAWAR, SAAD	
ART UNIT	**PAPER NUMBER**
2412	

DATE MAILED: 05/01/2024

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/ owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).
https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
2) a federal, state, local, or international agency, in response to its request;
3) a contractor of the USPTO having need for the information in order to perform a contract;
4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
9) the Office of Personnel Management (OPM) for personnel research purposes; and
10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	**Application No.** 18/594,375	**Applicant(s)** Manapragada, Sai C.	
	Examiner SAAD KHAWAR	**Art Unit** 2412	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to communication filed 3/4/24.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-30 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SAAD KHAWAR/
Primary Examiner, Art Unit 2412

Allowable Subject Matter

1. The following is an examiner's statement of reasons for allowance:

Regarding claims 1, of the closest prior arts **Rahman** (US 20080084855 A1) in view of **Kim** (US 20110128919 A1), **Yen** (US 20150098359 A1), and further in view of **Conner** (US 20060140123 A1) disclose features of the instant claim. However, **Rahman** in view of **Kim, Yen,** and **Conner** do not disclose all the features of "A method of improving the performance of circuitry, comprising the steps of: providing a processing interface that is adapted to be connected to an application interface of a wireless networking device, the application interface being associated with a first application, the first application providing, after the circuitry has been connected to the application interface and when the wireless networking device is being used, a first data stream and having a first wireless bandwidth requirement; connecting first and second actual MAC interfaces to the processing interface; connecting first and second actual PHY interfaces respectively to the first and second actual MAC interfaces; respectively associating first and second wireless transceivers with the first and second actual PHY interfaces, wherein each of the first and second wireless transceivers issuitable for use in a wireless local area network, and the first and second wireless transceivers, respectively, (i) have a first and second bandwidth availability up to first and second actual bandwidths, and (ii) are adapted to emit radio signals in first and second different bands of frequencies; forming in the processing interface (i) at least one virtual MAC interface and (ii) first and second virtual PHY interfaces that, after the circuitry has been connected to the application interface and during operation of the wireless networking device, feed information regarding the bandwidth availabilities of the first and second wireless transceivers back to the at least one virtual MAC interface; wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface, (a) request or create (i) a first association between a recipient and the first actual MAC and PHY interfaces and (ii) a second association between the recipient and the second actual MAC and PHY interfaces, (b) identify at least one first portion of the first actual bandwidth of the first wireless transceiver, the identified at least one first portion comprising a set of given resources, (c) evaluate whether any of the given resources of the first identified actual bandwidth portion are unavailable for communication, and (d) use

the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first bandwidth portion that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein, after the circuitry has been connected to the application interface and when the wireless networking is being used, the wireless networking device's utilization of the first available bandwidth portion of the first wireless transceiver does not prevent any wireless networking device devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first wireless transceiver for data transmission or reception purposes at the same time that the first bandwidth portion is being used for data transmission purposes" in combination.

The cited references fail to anticipate or render the above limitations in combination with all the recited limitations of claims 1 obvious, over any of the prior art of record, alone or in combination. The remaining claims depend on claim 1 and contain allowable subject matter for similar reasons.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAAD KHAWAR whose telephone number is (571)272-7948. The examiner can normally be reached Monday - Friday, 9:00am - 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Jiang can be reached on (571)-270-7191. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SAAD KHAWAR/
Primary Examiner, Art Unit 2412

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/594,375	Manapragada, Sai C.
	Examiner	**Art Unit**
	SAAD KHAWAR	2412

CPC							
Symbol						**Type**	**Version**
H04W	/	16	/	26		F	2013-01-01

CPC Combination Sets								
Symbol						**Type**	**Set**	**Ranking**	**Version**
	/		/						

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	30	
/SAAD KHAWAR/ Primary Examiner, Art Unit 2412	23 April 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	8

U.S. Patent and Trademark Office — Part of Paper No.: 20240423

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/594,375	Manapragada, Sai C.
	Examiner	**Art Unit**
	SAAD KHAWAR	2412

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04W16/26	/	16	/	26

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	30	
/SAAD KHAWAR/ Primary Examiner, Art Unit 2412	23 April 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	8

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/594,375	Manapragada, Sai C.
	Examiner	**Art Unit**
	SAAD KHAWAR	2412

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	30	
/SAAD KHAWAR/ Primary Examiner, Art Unit 2412	23 April 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	8

U.S. Patent and Trademark Office — Part of Paper No.: 20240423

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/594,375	Manapragada, Sai C.
	Examiner	Art Unit
	SAAD KHAWAR	2412

CPC - Searched*		
Symbol	Date	Examiner
H04W16	04/23/2024	/SK/

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See search history of family applications	04/23/2024	/SK/
Updated PE2E Search	04/23/2024	/SK/
Updated IP.com Search	04/23/2024	/SK/
Interference Search	04/23/2024	/SK/

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
H04W16		04/23/2024	/SK/

/SAAD KHAWAR/ Primary Examiner, Art Unit 2412	

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	31	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:27 AM
L2	26557	(H04W16$5).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:29 AM
L3	2	L2 AND (distributed NEAR2 (routing logic) DLR) SAME (relay bridge)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:30 AM
L4	454	(distributed NEAR2 (routing logic) DLR!) SAME (relay bridge)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:31 AM
L5	562	(distributed NEAR2 (routing logic) DLR!) SAME (relay$3 bridg$3)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:31 AM
L6	16	(distributed NEAR2 (routing logic) DLR!) SAME (relay$3 bridg$3) SAME (Wi$1Fi WLAN "802.11"$2)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:31 AM
L7	2	("20080084855" "20150098359").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 08:51 AM
L8	0	virtual NEAR link WITH aggregate WITH transceiver WITH availability	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:30 AM
L9	0	virtual NEAR link SAME aggregate WITH transceiver WITH availability	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:30 AM
L10	0	virtual NEAR link SAME transceiver WITH availability	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:30 AM
L11	0	virtual NEAR link SAME transceiver WITH aggregate	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:31 AM
L12	1253	transceiver WITH aggregate	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:31 AM
L13	1799	virtual NEAR link SAME (aggregat$3 combin$5)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM
L14	207	virtual NEAR link SAME (aggregat$3 combin$5) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM
L15	158	virtual ADJ link SAME (aggregat$3 combin$5) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM
L16	0	virtual2 ADJ link SAME (aggregat$3 combin$5)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM

		SAME indicat$3					
L17	192	virtual ADJ2 link SAME (aggregat$3 combin$5) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM
L18	31	virtual ADJ2 link SAME (aggregat$3 combin$5) SAME indicat$3 WITH (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:33 AM
L19	388	virtual ADJ2 link WITH (aggregat$3 combin$5) WITH (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:34 AM
L20	26557	(H04W16$5).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:34 AM
L21	1	virtual ADJ2 link WITH (aggregat$3 combin$5) WITH (resources bandwidth) AND L20	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:34 AM
L22	410871	(H04W$7).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:35 AM
L23	9	virtual ADJ2 link WITH (aggregat$3 combin$5) WITH (resources bandwidth) AND L22	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:35 AM
L24	9	virtual ADJ2 link WITH (aggregat$3 aggrad$3 combin$5) WITH (resources bandwidth) AND L22	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:39 AM
L25	1	virtual NEAR link WITH bandwidth WITH determination	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 12:09 PM
L26	9	(virtual aggregat$3) NEAR link WITH bandwidth WITH determination	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 12:10 PM
L27	180	(virtual aggregat$3) NEAR link WITH bandwidth WITH determin$5	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 12:10 PM
L28	410871	(H04W$7).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 12:11 PM
L29	12	(virtual aggregat$3) NEAR link WITH bandwidth WITH determin$5 AND L28	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 12:11 PM
L30	71	virtual NEAR link WITH (availability availabile)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:22 AM
L31	24	virtual NEAR link WITH resources WITH (aggregat$3 combined combination)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:27 AM

L32	557	virtual NEAR link WITH wire$1less	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:30 AM
L33	29	virtual NEAR link WITH wire$1less SAME (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:30 AM
L34	12895	(transmitter transceiver) WITH (aggregat$3 combin$3 plural$3 multiple) WITH (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:34 AM
L35	2441	(transmitter transceiver) WITH (aggregat$3 combin$3) WITH (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:34 AM
L36	531	(transmitter transceiver) WITH (aggregat$3 combin$3) NEAR2 (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:35 AM
L37	69	(plural$3 multiple second two set) NEAR3 (transmitter transceiver) WITH (aggregat$3 combin$3) NEAR2 (resources bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:35 AM
L38	553	(plural$3 multiple second two set combination) NEAR3 (transmitter transceiver) WITH (aggregat$3 combin$3) NEAR2 (resources bandwidth carrier) NOT L37	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 09:39 AM
L39	485	(plural$3 multiple second two set combination) NEAR3 (transmitter transceiver) WITH (aggregat$3) NEAR2 (resources bandwidth carrier) NOT L37	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:02 AM
L40	0	(plural$3 multiple second two set combination) NEAR3 (transmitter transceiver) WITH (aggregat$3) NEAR2 (resources bandwidth carrier) SAME virtual ADJ2 link NOT L37	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:03 AM
L41	0	(plural$3 multiple second two set combination) NEAR3 (transmitter transceiver) WITH (aggregat$3) NEAR2 (resources	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:11 AM

		bandwidth carrier) AND virtual ADJ2 link NOT L37					
L42	19	(plural$3 multiple second two set combination) NEAR3 (transmitter transceiver) WITH (aggregat$3) NEAR2 (resources bandwidth carrier) WITH link NOT L37	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:11 AM
L43	2	("20070242695" "20130281049").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:14 AM
L44	9	linearly NEAR coupled WITH radially NEAR coupled	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:03 PM
L45	0	linearly NEAR coupled SAME radially NEAR coupled AND radially NEAR coupled WITH arc	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:04 PM
L46	4	access NEAR point WITH linear WITH radial	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:09 PM
L47	19	access NEAR point SAME linear SAME radial	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:09 PM
L48	410871	(H04W$7).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:10 PM
L49	228	linear SAME radial AND L48	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:10 PM
L50	30	(base NEAR station access NEAR point) WITH placement SAME angle	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:13 PM
L51	464	(access NEAR point AP) WITH linear AND L48	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:15 PM
L52	4	(access NEAR point AP) WITH linear WITH (plac$4) AND L48	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 12:18 PM
L53	410871	(H04W$7).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 03:37 PM
L54	0	(mesh) WITH linear WITH (plac$4) AND L53	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 03:37 PM
L55	150	(mesh) WITH linear AND L53	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 03:37 PM
L56	3990	(access point AP) WITH coverage WITH overlap$4 AND L53	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 03:40 PM
L57	4	(access point AP) WITH	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12

		coverage WITH overlap$4 WITH linear$2 AND L53					03:53 PM
L58	141	(access point AP) WITH coverage WITH overlap$4 WITH exten$4	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/15 10:19 AM
L59	77	(access ADJ point AP) WITH coverage WITH overlap$4 WITH exten$4	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/15 10:20 AM
L60	51	(access ADJ point AP) WITH coverage WITH overlap$4 SAME relay	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/15 10:41 AM
L61	164	(access ADJ point AP) WITH overlap$4 SAME relay	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/15 10:43 AM
L62	73	(access ADJ point AP) WITH overlap$4 SAME (relay mesh) SAME coverage	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/15 10:44 AM
L63	4	multiple WITH transceivers! SAME aggregate WITH bandwidth	(US-PGPUB; USPAT)	OR	ON	ON	2019/10/28 10:05 AM
L64	75	transceivers! SAME aggregate WITH bandwidth	(US-PGPUB; USPAT)	OR	ON	ON	2019/10/28 10:05 AM
L65	3	transceivers! WITH aggregate NEAR link	(US-PGPUB; USPAT)	OR	ON	ON	2019/10/28 10:39 AM
L66	22	transceivers! WITH virtual NEAR link	(US-PGPUB; USPAT)	OR	ON	ON	2019/10/28 10:40 AM
L67	81	transceivers! SAME (virtual aggregate) NEAR (link bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2020/02/12 11:00 AM
L68	441445	(H04W$7 H04W16$5).CPC.	(US-PGPUB; USPAT)	OR	ON	ON	2020/02/12 11:00 AM
L69	22	L67 AND L68	(US-PGPUB; USPAT)	OR	ON	ON	2020/02/12 11:00 AM
L70	80	(access ADJ point AP) WITH overlap$4 SAME (relay mesh) SAME coverage	(US-PGPUB; USPAT)	OR	ON	ON	2020/02/12 11:00 AM
L71	60	(transceiver transmitter) WITH (allocat$3 dedicat$3) WITH (bandwidth resources) WITH (first second) NEAR (link connection)	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 12:45 PM
L72	129	(transceiver transmitter) WITH (allocat$3 dedicat$3) WITH (bandwidth resources)	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 12:45 PM

		WITH (first second) NEAR3 (link connection)					
L73	83	transceivers! SAME aggregate WITH bandwidth	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 05:47 PM
L74	90	transceivers! SAME (virtual aggregate) NEAR (link bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 05:47 PM
L75	172	virtual ADJ link SAME (aggregat$3 combin$5) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 05:47 PM
L76	176	virtual ADJ link SAME (aggregat$3 combin$5) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2021/04/23 10:41 AM
L77	96	transceivers! SAME (virtual aggregate) NEAR (link bandwidth)	(US-PGPUB; USPAT)	OR	ON	ON	2021/04/23 10:41 AM
L78	133	(transceiver transmitter) WITH (allocat$3 dedicat$3) WITH (bandwidth resources) WITH (first second) NEAR3 (link connection)	(US-PGPUB; USPAT)	OR	ON	ON	2021/04/23 10:41 AM
L79	96	(access ADJ point AP) WITH overlap$4 SAME (relay mesh) SAME coverage	(US-PGPUB; USPAT)	OR	ON	ON	2021/04/23 10:41 AM
L80	35	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2023/01/30 09:33 AM
L81	14	(Sai NEAR Manapragada).IN.	(USPAT)	OR	ON	ON	2023/01/30 09:34 AM
L82	256560	(H04W16$5).CPC.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/30 09:34 AM
L83	28	L82 AND virtual NEAR link WITH availab$5	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2023/02/01 10:55 AM

			EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L84	175	L82 AND bridge WITH availab$5	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/01 10:56 AM
L85	21574	L82 AND bandwidth WITH availab$5	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:53 AM
L86	221	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO;	OR	ON	ON	2023/02/02 10:54 AM

			JPO; DERWENT; IBM_TDB)				
L87	54506	L82 AND bandwidth WITH availab$5 grant SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:57 AM
L88	4	L82 AND bandwidth WITH availab$5 WITH grant SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:57 AM
L89	5	L82 AND bandwidth WITH availab$5 WITH grant$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:57 AM
L90	5	L82 AND bandwidth WITH (availab$5 free) WITH grant$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2023/02/02 10:57 AM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L91	5	L82 AND bandwidth WITH (availab$5 free unused) WITH grant$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:57 AM
L92	267	L82 AND bandwidth NEAR3 (availab$5 free unused) WITH (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:57 AM
L93	102	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2023/02/02 10:58 AM

			IBM_TDB)				
L94	7731	L82 AND determin$5 WITH (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:00 AM
L95	409	L82 AND determin$5 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:00 AM
L96	71	L82 AND den$5 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:01 AM
L97	19	L82 AND den$3 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS,	OR	ON	ON	2023/02/02 11:02 AM

			IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L98	21	L82 AND (den$3 refus$3 accept$3) WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:02 AM
L99	21	L82 AND (den$3 refus$3 accept$3 reject$3) WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:02 AM
L100	4338	bandwidth NEAR3 (availab$5 free unused) WITH (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:09 AM

L101	3614	bandwidth NEAR3 (availab$5 free unused) WITH (relay mesh)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:09 AM
L102	172552192	@PD<="20131030" @AD<="20131030" @PRAD<="20131030"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:12 AM
L103	2602	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:12 AM
L104	173	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH (accept$3 refus$3 den$3 reject$3) SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO,	OR	ON	ON	2023/02/02 11:13 AM

			MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L105	316	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH indicat$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 11:16 AM
L106	314	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH indicat$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 09:48 AM
L107	151	"10034147" "11429407" "20050089064" "20070110198" "20070121573" "20070180119" "20070242605" "20070270121" "20080002631" "20090034460" "20090074051" "20000141691" "20100128630" "20110110289" "20130028150" "20130258021" "20130281049"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 09:52 AM
L108	57	("10034147"	(US-PGPUB; USPAT;	OR	ON	ON	2023/08/22

		11429407B2 "20050089064" "20070110198" "20070121573" "20070180119" "20070242605" "20070270121" "20080002631" "20090034460" "20090074051" "20000141691" "20100128630" "20110110289" "20130028150" "20130258021" "20130281049").PN.	USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				09:52 AM
L109	15	("10034147" 11429407B2 "20050089064" "20070110198" "20070121573" "20070180119" "20070242605" "20070270121" "20080002631" "20090034460" "20090074051" "20000141691" "20100128630" "20110110289" "20130028150" "20130258021" "20130281049").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/22 09:52 AM
L110	11	("20140003449" "20140056209" "20140075189" "20140269610" "20150023245" "20150098359" "20160014127" "7373443" "9160396" 9198184B2 "9526022" "9603192").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/22 09:54 AM
L111	0	virtual NEAR PHY WITH virtual NEAR MAC WITH feed$4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO;	OR	ON	ON	2023/08/22 10:31 AM

			JPO; DERWENT; IBM_TDB)				
L112	0	virtual NEAR PHY SAME virtual NEAR MAC WITH feed$4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 10:31 AM
L113	0	virtual NEAR PHY SAME virtual NEAR MAC SAME feed$4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 10:32 AM
L114	28	virtual NEAR PHY SAME virtual NEAR MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 10:32 AM
L115	314	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH indicat$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2023/09/11 09:34 AM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L116	172	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH (accept$3 refus$3 den$3 reject$3) SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/11 09:34 AM
L117	24	("20020152305" OR "20040053602" OR "20060114851" OR "20090290524" OR "20120113320" OR "20140075523" OR "20140269560" OR "20150181486" OR "20150237667" OR "5073899" OR "5818830" OR "7664072" OR "7784076" OR "7797723" OR "8411608" OR "8718558" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "8989101" OR "9258712" OR "9560661" OR "9706383").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/11 09:37 AM
L118	35	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/26 10:13 AM
L119	41	("20020152305" OR "20040053602" OR "20060114851" OR "20090290524" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/26 10:14 AM

		"20120113320" OR "20140075523" OR "20140269560" OR "20150181486" OR "20150237667" OR "5073899" OR "5818830" OR "7664072" OR "7784076" OR "7797723" OR "8411608" OR "8718558" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "898910181" OR "9258712" OR "9560661" OR "9706383" OR "0000001" OR "0000002" OR "20130028150" OR "20130196653" OR "20130258921" OR "20130281049" OR "20140003449" OR "20140056209" OR "20140213219" OR "20140269610" OR "20150023245" OR "20150098359" OR "20150110036" OR "20160014127" OR "7373443" OR "77777777777" OR "9603192" OR "9736714" OR "9743345").pn.					
L120	314	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH indicat$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:08 AM
L121	172	L102 AND bandwidth NEAR3 (availab$5 free	(US-PGPUB; USPAT; USOCR; FIT (AU, AP,	OR	ON	ON	2023/09/26 11:08 AM

		unused) WITH (accept$3 refus$3 den$3 reject$3) SAME (relay mesh bridge)	AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L122	172	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH (accept$3 refus$3 den$3 reject$3) SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:11 AM
L123	314	L102 AND bandwidth NEAR3 (availab$5 free unused) WITH indicat$3 SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:11 AM
L124	225	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO,	OR	ON	ON	2023/09/26 11:17 AM

			RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L125	110	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:18 AM
L126	421	L82 AND determin$5 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:18 AM
L127	226	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/10/19 10:07 AM
L128	111	L82 AND bandwidth WITH (availab$5 free unused) WITH access	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY,	OR	ON	ON	2023/10/19 10:07 AM

		SAME (relay mesh bridge)	CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L129	421	L82 AND determin$5 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/10/19 10:08 AM
L130	422	L82 AND determin$5 WITH (relay mesh bridge) WITH (bandwidth)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:14 AM
L132	113	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK,	OR	ON	ON	2023/11/20 09:14 AM

			TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L133	228	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:14 AM
L134	29	virtual NEAR PHY SAME virtual NEAR MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:14 AM
L135	45	virtual NEAR PHY AND virtual NEAR MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:14 AM
L136	193	virtual NEAR3 PHY SAME virtual NEAR3 MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	OR	ON	ON	2023/11/20 09:15 AM

			CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L137	4	virtual NEAR3 PHY SAME virtual NEAR3 MAC SAME bandwidth WITH availability	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:15 AM
L138	17	virtual NEAR3 PHY AND virtual NEAR3 MAC AND bandwidth WITH availability	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:16 AM
L139	46	("20100128630" OR "20110110289" OR "20110128919" OR "20110211541" OR "20120113320" OR "20130028150" OR "20130196653" OR "20130258921" OR "20130281049" OR "20140003449" OR "20140056209" OR "20140075189" OR "20140075523" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/11/20 09:17 AM

		"20140213219" OR "20140269560" OR "20140269610" OR "20150023245" OR "20150098359" OR "20150110036" OR "20150181486" OR "20150237667" OR "20160014127" OR "5073899" OR "5818830" OR "7373443" OR "7664072" OR "7784076" OR "7797723" OR "8411608" OR "8718558" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "8989101" OR "9160396" OR "9198184" OR "9258712" OR "9467379" OR "9526022" OR "9560656" OR "9560661" OR "9603192" OR "9706383" OR "9736714" OR "9743345").pn.					
L140	36	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2023/11/20 09:20 AM
L141	113	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/11/20 09:29 AM
L142	228	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2023/11/20 09:29 AM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L143	115	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/25 09:30 AM
L144	231	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/25 09:30 AM
L145	17	("10044613" OR "10912083" OR "20050195821" OR "20090180451" OR "20110286404" OR "20130201847" OR "20140269505" OR "20140321282" OR "8175539" OR "8279876" OR "8363597" OR "8565178" OR "8767726" OR "9241370" OR "9294926" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/25 09:31 AM

		"9408254" OR "9516540").pn.					
L146	17	("10044613" OR "10912083" OR "20050195821" OR "20090180451" OR "20110286404" OR "20130201847" OR "20140269505" OR "20140321282" OR "8175539" OR "8279876" OR "8363597" OR "8565178" OR "8767726" OR "9241370" OR "9294926" OR "9408254" OR "9516540").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 09:34 AM
L147	65	("10034147" OR "11115834" OR "11429407" OR "20020152305" OR "20040053602" OR "20050089064" OR "20060114851" OR "20060140123" OR "20070110198" OR "20070121573" OR "20070180119" OR "20070242695" OR "20070270121" OR "20080002631" OR "20080084855" OR "20090034460" OR "20090074051" OR "20090141691" OR "20090290524" OR "20100128630" OR "20110110289" OR "20110128919" OR "20110211541" OR "20120113320" OR "20130028150" OR "20130196653" OR "20130258921" OR "20130281049" OR "20140003449" OR "20140056209" OR "20140075189" OR "20140075523" OR "20140213219" OR "20140269560" OR "20140269610" OR "20150023245" OR "20150098359" OR "20150110036" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 09:35 AM

		"20150181486" OR "20150237667" OR "20160014127" OR "5073899" OR "5818830" OR "7373443" OR "7664072" OR "7784076" OR "7797723" OR "8411608" OR "8718558" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "8989101" OR "9160396" OR "9198184" OR "9258712" OR "9467379" OR "9526022" OR "9560656" OR "9560661" OR "9603192" OR "9706383" OR "9736714" OR "9743345").pn.					
L148	115	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/29 09:48 AM
L149	231	L82 AND bandwidth WITH availab$5 WITH relay	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO;	OR	ON	ON	2024/01/29 09:48 AM

			JPO; DERWENT; IBM_TDB)				
L150	21	L82 AND bandwidth WITH (MAC PHY) WITH subset	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/29 09:49 AM
L151	77	L82 AND bandwidth WITH subset SAME (MAC PHY)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/29 09:49 AM
L153	115	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/02/20 09:23 AM
L154	21	L82 AND bandwidth WITH (MAC PHY) WITH subset	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2024/02/20 09:24 AM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L155	79	L82 AND bandwidth WITH subset SAME (MAC PHY)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/02/20 09:24 AM
L156	43	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/15 09:05 AM
L157	8	(Sai NEAR Manapragada).IN. AND (subset WITH frequency).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/15 09:07 AM
L159	6	(Sai NEAR Manapragada).IN. AND (subset WITH frequency AND second NEAR5 requirement).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/15 09:09 AM
L160	115	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/04/15 09:16 AM
L161	82	("10034147" OR "10044613" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/15 09:17 AM

		"10912083" OR "11115834" OR "11429407" OR "20020152305" OR "20040053602" OR "20050089064" OR "20050195821" OR "20060114851" OR "20060140123" OR "20070110198" OR "20070121573" OR "20070180119" OR "20070242695" OR "20070270121" OR "20080002631" OR "20080084855" OR "20090034460" OR "20090074051" OR "20090141691" OR "20090180451" OR "20090290524" OR "20100128630" OR "20110110289" OR "20110128919" OR "20110211541" OR "20110286404" OR "20120113320" OR "20130028150" OR "20130196653" OR "20130201847" OR "20130258921" OR "20130281049" OR "20140003449" OR "20140056209" OR "20140075189" OR "20140075523" OR "20140213219" OR "20140269505" OR "20140269560" OR "20140269610" OR "20140321282" OR "20150023245" OR "20150098359" OR "20150110036" OR "20150181486" OR "20150237667" OR "20160014127" OR "5073899" OR "5818830" OR "7373443" OR "7664072" OR "7784076" OR "7797723" OR "8175539" OR "8279876" OR "8363597" OR "8411608" OR "8565178" OR					

		"8718558" OR "8767726" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "8989101" OR "9160396" OR "9198184" OR "9241370" OR "9258712" OR "9294926" OR "9408254" OR "9467379" OR "9516540" OR "9526022" OR "9560656" OR "9560661" OR "9603192" OR "9706383" OR "9736714" OR "9743345").pn.					
L162	214	virtual NEAR3 PHY SAME virtual NEAR3 MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/04/15 09:43 AM
L163	43	(Sai NEAR Manapragada).IN.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/23 08:56 AM
L164	82	("10034147" OR "10044613" OR "10912083" OR "11115834" OR "11429407" OR "20020152305" OR "20040053602" OR "20050089064" OR "20050195821" OR "20060114851" OR "20060140123" OR "20070110198" OR "20070121573" OR "20070180119" OR "20070242695" OR "20070270121" OR "20080002631" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/23 09:11 AM

		"20080084855" OR "20090034460" OR "20090074051" OR "20090141691" OR "20090180451" OR "20090290524" OR "20100128630" OR "20110110289" OR "20110128919" OR "20110211541" OR "20110286404" OR "20120113320" OR "20130028150" OR "20130196653" OR "20130201847" OR "20130258921" OR "20130281049" OR "20140003449" OR "20140056209" OR "20140075189" OR "20140075523" OR "20140213219" OR "20140269505" OR "20140269560" OR "20140269610" OR "20140321282" OR "20150023245" OR "20150098359" OR "20150110036" OR "20150181486" OR "20150237667" OR "20160014127" OR "5073899" OR "5818830" OR "7373443" OR "7664072" OR "7784076" OR "7797723" OR "8175539" OR "8279876" OR "8363597" OR "8411608" OR "8565178" OR "8718558" OR "8767726" OR "8818276" OR "8837454" OR "8923816" OR "8982762" OR "8989101" OR "9160396" OR "9198184" OR "9241370" OR "9258712" OR "9294926" OR "9408254" OR "9467379" OR "9516540" OR					

		"9526022" OR "9560656" OR "9560661" OR "9603192" OR "9706383" OR "9736714" OR "9743345").pn.					
L165	115	L82 AND bandwidth WITH (availab$5 free unused) WITH access SAME (relay mesh bridge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/04/23 09:39 AM
L166	215	virtual NEAR3 PHY SAME virtual NEAR3 MAC	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/04/23 09:39 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N80	15214	(H04W16/$5).CPC.	(USPAT)	OR	ON	ON	2021/04/23 10:44 AM
N81	8	(H04W16/$5).CPC. AND (virtual NEAR link).CLM.	(USPAT)	OR	ON	ON	2021/04/23 10:44 AM
N82	29	(H04W16/$5).CPC. AND ((virtual$3 logic$2) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2021/04/23 10:44 AM
N83	29	(H04W16/$5).CPC. AND ((virtual$4 logic$2) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2021/04/23 10:44 AM

N84	48	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2021/04/23 10:45 AM
N85	64	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2023/08/22 10:27 AM
N89	3	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/22 10:32 AM
N90	65	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2023/09/11 09:35 AM
N91	3	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/11 09:35 AM
N92	65	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2023/10/19 10:08 AM
N93	3	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/10/19 10:08 AM
N94	4	(virtual NEAR PHY AND virtual NEAR MAC AND bandwidth).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/11/20 09:16 AM
N95	4	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/11/20 09:17 AM
N96	65	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2023/11/20 09:17 AM
N97	4	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2023/11/20 09:17 AM
N98	9	(virtual NEAR PHY AND virtual NEAR MAC AND feed$4).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 10:23 AM
N99	14	N80 AND (bandwidth WITH subset AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 10:24 AM
N100	9	N80 AND (bandwidth WITH virtual AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 10:24 AM
N101	19	N80 AND (bandwidth AND virtual AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/29 10:24 AM
N102	19	N80 AND (bandwidth AND virtual AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 09:20 AM

N103	21	N80 AND (bandwidth AND virtual AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/15 10:30 AM
N104	21	N80 AND (bandwidth AND virtual AND (MAC PHY)).CLM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/04/23 09:44 AM
N105	69	(H04W16/$5).CPC. AND ((virtual$4 logic$2 aggregat$3) NEAR3 link).CLM.	(USPAT)	OR	ON	ON	2024/04/23 09:44 AM

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-10034147 B2	07-24-2018	Shelby et al.	
	2	US-10044613 B2	08-07-2018	Kazmi et al.	
	3	US-10912083 B2	02-02-2021	Amini et al.	
	4	US-11,115,834 B2	09-07-2021	Manapragada	
	5	US-11115834 B2	09-07-2021	Manapragada	
	6	US-11429407 B2	08-30-2022	Smith et al.	
	7	US-20020152305 A1	10-17-2002	Jackson et al.	
	8	US-20040053602 A1	03-18-2004	Wurzburg	
	9	US-20050089064 A1	04-28-2005	Zimmerman et al.	
	10	US-20050195821 A1	09-08-2005	YUN et al.	
	11	US-2006/0140123 A1	06-29-2006	Conner et al.	
	12	US-20060114851 A1	06-01-2006	Gupta et al.	
	13	US-20060140123 A1	06-29-2006	Conner et al.	
	14	US-2007/0242695 A1	10-18-2007	Xu	
	15	US-20070110198 A1	05-17-2007	Skarby et al.	
	16	US-20070121573 A1	05-31-2007	Zuckerman et al.	
	17	US-20070180119 A1	08-02-2007	Khivesara et al.	
	18	US-20070242695 A1	10-18-2007	Xu	
	19	US-20070270121 A1	11-22-2007	Shao et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country[3] Code Number[4] Kind Code (if known)[5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
	20	EP 1878169 B1	01-16-2008	Rune		
	21	KR 20070061684A	06-14-2007	Jeonghoon Oh		✓
	22	WO 2014020407 A1	02-06-2014	Huang et al.		
	23	EP 2016750 B1	01-21-2009	Lee et al.		
	24	EP 2055072 B1	05-06-2009	Falk et al.		✓
	25	GB 2516132A	01-14-2015	Stephens et al.		

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	26	US-2008/0002631 A1	01-03-2008	Ramachandran	
	27	US-2008/0084855 A1	04-10-2008	Rahman	
	28	US-20080002631 A1	01-03-2008	Ramachandran	
	29	US-20080084855 A1	04-10-2008	Rahman	
	30	US-20090034460 A1	02-05-2009	Moratt et al.	
	31	US-20090074051 A1	03-19-2009	Manapragada et al.	
	32	US-20090141691 A1	06-04-2009	Jain	
	33	US-20090180451 A1	07-16-2009	Alpert et al.	
	34	US-20090290524 A1	11-26-2009	Seok	
	35	US-2010/0128630 A1	05-27-2010	Barak et al.	
	36	US-20100128630 A1	05-27-2010	Barak et al.	
	37	US-2011/0110289 A1	05-12-2011	Venkatachalam et al.	
	38	US-2011/0128919 A1	06-02-2011	Kim et al.	
	39	US-2011/0211541 A1	09-01-2011	Yuk et al.	
	40	US-20110110289 A1	05-12-2011	Venkatachalam et al.	
	41	US-20110128919 A1	06-02-2011	KIM et al.	
	42	US-20110211541 A1	09-01-2011	Yuk et al.	
	43	US-20110286404 A1	11-24-2011	Abraham et al.	
	44	US-20120113320 A1	05-10-2012	PLATZER	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country[3] Code Number[4] Kind Code (if known)[5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
	45	EP 2555578A1	02-06-2013	Deb et al.		
	46	EP 2713670 A1	04-02-2014	Smadi		
	47	EP 3174323 B1	11-14-2018	Montemurro		
	48	EP 3220697 B1	06-06-2018	Kiukkonen		
	49	TW I500350B	04-16-2015	Yen et al.		✓

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	50	US-2013/0281049 A1	10-24-2013	Lee et al.	
	51	US-20130028150 A1	01-31-2013	Ma et al.	
	52	US-20130196653 A1	08-01-2013	Morrison	
	53	US-20130201847 A1	08-08-2013	Chincholi et al.	
	54	US-20130258921 A1	10-03-2013	Gevorkov et al.	
	55	US-20130281049 A1	10-24-2013	Lee et al.	
	56	US-2014/0056209 A1	02-27-2014	Park et al.	
	57	US-2014/0075189 A1	03-13-2014	Abraham et al.	
	58	US-2014/0269610 A1	09-18-2014	Hiben et al.	
	59	US-20140003449 A1	01-02-2014	Li	
	60	US-20140056209 A1	02-27-2014	Park et al.	
	61	US-20140075189 A1	03-13-2014	Abraham et al.	
	62	US-20140075523 A1	03-13-2014	TUOMAALA et al.	
	63	US-20140213219 A1	07-31-2014	MOHEBBI	
	64	US-20140269505 A1	09-18-2014	Medard et al.	
	65	US-20140269560 A1	09-18-2014	Jain et al.	
	66	US-20140269610 A1	09-18-2014	HIBEN et al.	
	67	US-20140321282 A1	10-30-2014	Pragada et al.	
	68	US-2015/0023245 A1	01-22-2015	Du et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country[3] Code Number[4] Kind Code (if known)[5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	69	US-2015/0098359 A1	04-09-2015	Yen et al.	
	70	US-2015/0110036 A1	04-23-2015	Zhang et al.	
	71	US-20150023245 A1	01-22-2015	Du et al.	
	72	US-20150098359 A1	04-09-2015	YEN et al.	
	73	US-20150110036 A1	04-23-2015	Zhang et al.	
	74	US-20150181486 A1	06-25-2015	Vallabhu et al.	
	75	US-20150237667 A1	08-20-2015	GHAI et al.	
	76	US-20160014127 A1	01-14-2016	Mohebbi	
	77	US-5073899	12-17-1991	Collier et al.	
	78	US-5818830	10-06-1998	Daane et al.	
	79	US-7373443 B2	05-13-2008	Seto	
	80	US-7664072 B1	02-16-2010	Ho et al.	
	81	US-7784076 B2	08-24-2010	Demircin et al.	
	82	US-7797723 B2	09-14-2010	Demircin et al.	
	83	US-8175539 B2	05-08-2012	Diener et al.	
	84	US-8279876 B2	10-02-2012	Chang et al.	
	85	US-8363597 B2	01-29-2013	Abraham et al.	
	86	US-8411608 B2	04-02-2013	Chandra et al.	
	87	US-8565178 B2	10-22-2013	Cheng et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country[3] Code Number[4] Kind Code (if known)[5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	88	US-8718558 B2	05-06-2014	Montemurro	
	89	US-8767726 B2	07-01-2014	Petry et al.	
	90	US-8818276 B2	08-26-2014	Kiukkonen et al.	
	91	US-8837454 B2	09-16-2014	Hegde	
	92	US-8923816 B2	12-30-2014	Lee et al.	
	93	US-8982762 B2	03-17-2015	Smadi et al.	
	94	US-8989101 B1	03-24-2015	Mishra	
	95	US-9160396 B2	10-13-2015	Soltanian et al.	
	96	US-9198184 B2	11-24-2015	Yeh et al.	
	97	US-9241370 B2	01-19-2016	Amini et al.	
	98	US-9258712 B2	02-09-2016	Kiukkonen et al.	
	99	US-9294926 B2	03-22-2016	Pragada et al.	
	100	US-9408254 B2	08-02-2016	Jain	
	101	US-9467379 B2	10-11-2016	Merlin et al.	
	102	US-9516540 B2	12-06-2016	Emmanuel et al.	
	103	US-9526022 B2	12-20-2016	Gupta	
	104	US-9560656 B2	01-31-2017	Damnjanovic et al.	
	105	US-9560661 B2	01-31-2017	Elhaddad et al.	
	106	US-9603192 B2	03-21-2017	Mohebbi	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	107	US-9706383 B2	07-11-2017	Kiukkonen et al.	
	108	US-9736714 B2	08-15-2017	Zhao et al.	
	109	US-9743345 B2	08-22-2017	Yen et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country[3] Code Number[4] Kind Code (if known)[5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	7	of	9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	110	Choi et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part I". IEEE 11-14/0804r1. [PowerPoint presentation].	
	111	Choi et al. (November 11, 2013) "Discussion on OFDMA in HEW". LG Electronics. [PowerPoint presentation].	
	112	English Abstract of TWI500350B obtained from Espacenet.net on July 7, 2023.	
	113	English Translation of EP2055072B1 obtained from Google Patents on September 1, 2023.	
	114	English Translation of KR20070061684A obtained from Google Patents on January 9, 2024.	
	115	Gong, D.; Yang, Y; and Li, H. "An Efficient Cooperative Retransmission MAC Protocol for IEEE 802.11n Wireless LANs" in: IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, 2013. pp. 191-199.	
	116	Hiertz et al. (November 12, 2013) "Proposed direction and priorities for HEW". IEEE 11-13-1331-01. [PowerPoint presentation].	
	117	Huang et al. (September 16, 2013) "DL-MU-MIMO Transmission with Unequal Bandwidth". IEEE 802.11-13/1154r1. [PowerPoint presentation].	
	118	IEEE std 802.11ac(tm)-2013. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancemenets for Very High Throughput for Operation in Bands below 6 GHz. IEEE Computer Society. (2013).	
	119	Inoue et al. (March 19, 2013) "Beyond 802.11ac – A Very High Capacity WLAN". IEEE 11-13/0287r3. [PowerPoint presentation].	

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	120	Kakumanu, S. and Sivakumar, R. "Glia: A Practical Solution for Effective High Datarate Wifi-Arrays". MobiCom '09, September 20-25, 2009.	
	121	Kim et al. (September 16, 2013) "Multicast Transmission for HEW". IEEE 802.11-13/1061r0. [PowerPoint presentation].	
	122	Koskela et al. (July 15, 2013) "Discussion on Potential Techniques for HEW". IEEE 802.11-13/0871r0. [PowerPoint presentation].	
	123	Li, H. and Xie, J. "A Channel Splitting Strategy for Reducing Handoff Delay in Internet-Based Wireless Mesh Networks" in: IEEE Transactions on Vehicular Techonolgy, (July 2012), vol 61, no. 6. pp. 2740-2752.	
	124	Lim et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part II". IEEE 11-14/0801r0. [PowerPoint presentation].	
	125	Liu et al. (May 9, 2013) "Discussions on 11ac PHY Efficiency". IEEE 802.11-13/0544r3. [PowerPoint presentation].	
	126	Prasad, S.S; Shukla, C.K.; and Chisab, R.F. "Performance Analysis of OFDMA in LTE" in: IEEE (July 26-28, 2012).	
	127	Raman, V. and Vaidya, N.H. "WiSP: A Protocol for Overcoming MAC Overheads Using Packet Size Dependent Channel Widths" in: 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2011. pp. 28-36.	
	128	Selvakumar, V.; Nemalladinne, S.S.; and Arumugam, P. "Analysis of LTE Radio Frame by eliminating Cyclic Prefix in OFDM and comparison of QAM and Offset-QAM". Degree project. Linnaeus University, September 10, 2012.	
	129	U.S. Provisional Patent Application No. 61/835,488, entitled "WLAN SENSOR GATEWAY WITH COEXISTENCE SOLUTION", filed Jun. 14, 2013	

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	9	of	9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	130	U.S. Provisional Patent Application No. 61/836,571, entitled "COEXISTENCE AND TRAFFIC MANAGEMENT FOR USING MULTIPLE WLAN RADIOS IN A SYSTEM", filed Jun. 18, 2013	
	131	U.S. Provisional Patent Application No. 61/870,762, entitled "COEXISTENCE AND TRAFFIC MANAGEMENT WITH ALIGNMENT OF PACKETS AND CHANNEL STEERING", filed Aug. 27, 2013	
	132	U.S. Provisional Patent Application No. 61/888,692, entitled "WIRELESS DESIGN FOR USING A ROUTERS OR RESIDENTIAL GATEWAY AS SENSOR GATEWAY", filed Oct. 9, 2013	
	133	U.S. Provisional Patent Application No. 61/890,713 entitled "SIMULTANEOUS USAGE OF DIFFERENT WLAN MODULES", filed Oct. 14, 2013	
	134	U.S. Provisional Patent Application Ser. No. 61/824,338 entitled "ADVANCED WIRELESS COMMUNICATION SYSTEMS AND TECHNIQUES", filed May 16, 2013	
	135	Wee et al. "Discretionary bandwidth granting scheme for homogenous real-time applications". EURASIP Journal on Wireless Communications and Networking (2013). http://jwcn.eurasipjournals.com/content/203/1/135	
	136	Yang et al. (September 18, 2013) "Discussion on Access Mechanism for HEW". IEEE 11-13/1105r0. [PowerPoint presentation].	

Examiner Signature	/SAAD KHAWAR/ (04/23/2024)	Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

18594375
Search History

Report Run Date: 2024-04-23 UTC
Searches: 1
Markers: 1

Samsung Ex. 1004, Page 68 of 563

Search #	Timestamp	Results	Page
1	2024-04-23 13:39 UTC	~11,814,304	4

Content: Patents + NPL (193)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Luxembourg Applications | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Patents | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IEEE Xplore Publications: Ericsson Technology Review | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 2024-04-23 13:39 UTC | ~11,814,304 results from

De-Dup: Extended Family Numbers (PAT only) | **Relevance Cut-off:** None | **Sort:** Relevance

Main Concept: Text

A method of improving the performance of circuitry, comprising the steps of: providing a processing interface that is adapted to be connected to an application interface of a wireless networking device, the application interface being associated with a first application, the first application providing, after the circuitry has been connected to the application interface and when the wireless networking device is being used, a first data stream and having a first wireless bandwidth requirement; connecting first and second actual MAC interfaces to the processing interface; connecting first and second actual PHY interfaces respectively to the first and second actual MAC interfaces; respectively associating first and second wireless transceivers with the first and second actual PHY interfaces, wherein each of the first and second wireless transceivers issuitable for use in a wireless local area network, and the first and second wireless transceivers, respectively, (i) have a first and second bandwidth availability up to first and second actual bandwidths, and (ii) are adapted to emit radio signals in first and second different bands of frequencies; forming in the processing interface (i) at least one virtual MAC interface and (ii) first and second virtual PHY interfaces that, after the circuitry has been connected to the application interface and during operation of the wireless networking device, feed information regarding the bandwidth availabilities of the first and second wireless transceivers back to the at least one virtual MAC interface; wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface, (a) request or create (i) a first association between a recipient and the first actual MAC and PHY interfaces and (ii) a second association between the recipient and the second actual MAC and PHY interfaces, (b) identify at least one first portion of the first actual bandwidth of the first wireless transceiver, the identified at least one first portion comprising a set of given resources, (c) evaluate whether any of the given resources of the first identified actual bandwidth portion are unavailable for communication, and (d) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first bandwidth portion that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein, after the circuitry has been connected to the application interface and when the wireless networking is being used, the wireless networking device's utilization of the first available bandwidth portion of the first wireless transceiver does not prevent any wireless networking device devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first wireless transceiver for data transmission or reception purposes at the same time that the first bandwidth portion is being used for data transmission purposes.

Concept Modifiers: None

Filters: None

Bibliographic Data

Application No: 18/594,375

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /SAAD KHAWAR/ (Examiner's Signature) | (Initials)

Title: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
03/04/2024	370	2412	020505-000010
RULE			

APPLICANTS

XiFi Networks R&D Inc., Cypress, TX, UNITED STATES

INVENTORS

Sai C. Manapragada,

CONTINUING DATA

This application is a CON of 18532175 12/07/2023 PAT 11950105

18532175 is a CON of 18448281 08/11/2023 PAT 11849337

18448281 is a CON of 17468509 09/07/2021 PAT 11818591

17468509 is a CON of 16039660 07/19/2018 PAT 11115834

16039660 is a CON of 14526799 10/29/2014 PAT 10034179

14526799 has PRO of 61897216 10/30/2013

14526799 has PRO of 61897219 10/30/2013

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/13/2024

**** SMALL ENTITY ****

STATE OR COUNTRY

ADDRESS

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP

111 MONUMENT CIRCLE, SUITE 3700

INDIANAPOLIS, IN 46204-5137

UNITED STATES

FILING FEE RECEIVED

$2,800

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
18/594,375	03/04/2024	Manapragada, Sai C.	020505-000010

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EXAMINER	
--	
ART UNIT	PAPER
--	20240427-SIC1pt

DATE MAILED: 27 April 2024

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

PTO-90C (Rev.04-03)

Notice of Potential Erroneous Release of Patent Application Titles

On February 5, 2024, the United States Patent and Trademark Office (USPTO), replaced the Electronic Patent Assignment System (EPAS) and Electronic Trademark Assignment System (ETAS) with Assignment Center.

Between February 5, 2024 and March 29, 2024, the USPTO, unintentionally, through a computer programming error, permitted bibliographic information to be viewed by unauthorized individuals with access to registered Assignment Center accounts. This bibliographic information was limited to the application number (the two-digit series code plus the six-digit serial number) and title of the invention.

You are receiving this notification because your application's patent title may have been viewed during that time frame by individual(s) who lacked permission to do so. The software error was first reproduced by USPTO on March 28, 2024, and was corrected on March 29, 2024. Only application numbers and titles were disclosed; it is important to note that your specification and claims were not part of the information made available and were not accessed.

Any improper access of the application information between the dates of February 5, 2024 and March 29, 2024, is not considered a publication of such applications under 35 U.S.C. 122(b). No rights in United States patents are threatened by the access to unpublished applications. It is extremely unlikely that the title could disclose the invention in a way that would constitute patent-defeating prior art in any jurisdiction. To the extent any issue is raised, the USPTO will assist applicants by confirming that the disclosure was erroneous and inadvertent.

We're committed to data security and are taking enhanced steps to prevent incidents such as this from happening in the future. The USPTO sincerely regrets this error and is instituting more testing controls, both manual and automated testing, to prevent similar processing errors in the future.

Inquiries regarding this matter may be directed to Mark Polutta, Senior Legal Advisor, at (571) 272-7709 or Andrew Stclair, Legal Advisor, at (571) 270-0238, both of the Office of Patent Legal Administration or via email addressed to Patent.Practice@uspto.gov.



Henry "Jamie" Holcombe
Chief Information Officer
US Patent and Trademark Office
Office +1 (571) 272-9400

Dated: April 27th, 2024

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
* 18/594,375 *	18/594,375	Manapragada, Sai C.	
	Examiner	**Art Unit**	
	KHAWAR, SAAD	2412	

Document Code - DISQ	**Internal Document - DO NOT MAIL**

TERMINAL DISCLAIMER	☑ APPROVED	☐ DISAPPROVED
Date Filed: 04 March 2024	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

/FELICIA D ROBERTS/

Technology Center: OPLC

Telephone: (571)272-0550

9 TDs approved with this filing date

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/594,375	03/04/2024	Sai C. Manapragada	020505-000010	3271

30565 7590 04/09/2024

WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

EXAMINER
CENTRAL, DOCKET

ART UNIT	PAPER NUMBER
OPAP	

NOTIFICATION DATE	DELIVERY MODE
04/09/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketDept@uspatent.com

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 18/594,375	**Applicant(s)** Manapragada, Sai C.	
	Examiner FIKIRTE A GEREMEW	**Art Unit** OMBL	**AIA (FITF) Status** Yes

1. THE REQUEST FILED 04 March 2024 IS **GRANTED** .

The above-identified application has met the requirements for prioritized examination

A. ☑ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims** , or a multiple dependent claim;

C. filing a **request for continued examination** ;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to FIKIRTE GEREMEW at (703) 756-1930. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/FIKIRTE A GEREMEW/ PROGRAM SUPPORT SPECIALIST, OMBL	

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 18/594,375

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	64		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	280		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	320		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	* 10	x 40 =	400	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x =	0			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1064		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
18/594,375	03/04/2024		1064	020505-000010	30	1

CONFIRMATION NO. 3271

30565
WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP
111 MONUMENT CIRCLE, SUITE 3700
INDIANAPOLIS, IN 46204-5137

FILING RECEIPT



Date Mailed: 03/18/2024

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Sai C. Manapragada, Cypress, TX;

Applicant(s)

XiFi Networks R&D Inc., Cypress, TX;

Power of Attorney: The patent practitioners associated with Customer Number 30565

Domestic Priority data as claimed by applicant

This application is a CON of 18/532,175 12/07/2023 PAT 11,950,105
which is a CON of 18/448,281 08/11/2023 PAT 11,849,337
which is a CON of 17/468,509 09/07/2021 PAT 11,818,591
which is a CON of 16/039,660 07/19/2018 PAT 11,115,834
which is a CON of 14/526,799 10/29/2014 PAT 10,034,179
which claims benefit of 61/897,219 10/30/2013
and claims benefit of 61/897,216 10/30/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 03/13/2024
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/594,375**
Projected Publication Date: 06/27/2024
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

WELCOME TO THE UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

*Congratulations on taking the first step to protect your invention. You can now advertise or mark any products covered by this application for your invention as **"Patent Pending"** for as long as this application is pending!*

We are here to help you on the rest of your journey.

New to the process? The Patent Basics page will take you from "What is a patent?" to assistance with the application process.

- **www.uspto.gov/PatentBasics**

Consider cost savings. You might qualify for small entity or micro entity status, which means a discount on most USPTO patent fees.

- **www.uspto.gov/EntityStatus**

Become a registered electronic filer (eFiler). You'll gain access to the full capabilities of Patent Center. As a registered eFiler, you can electronically view your submission, track the progress of your application, and respond to USPTO correspondence.

- **www.uspto.gov/NewPatentFilers**

Learn how to identify which of your creative ideas might be intellectual property assets and how to protect them by using the USPTO Intellectual Property (IP) Identifier.

- **ipidentifier.uspto.gov**

We also provide Pro Se Assistance, support specifically geared for **independent inventors without an attorney or agent.** Follow the link below, call us at 866-767-3848, or email **proseassistancecenter@uspto.gov**.

- **www.uspto.gov/ProSePatents**

Need help near you? We have regional offices across the country, as well as Patent and Trademark Resource Centers in libraries in nearly every state, with specialists standing by to help you at no cost.

- **www.uspto.gov/locations**
- **www.uspto.gov/ptrc**

Contact us:

- **General information:** USPTO Contact Center
  - **www.uspto.gov/help**
- **Patent Center:**
  Patent Electronic Business Center
  - **www.uspto.gov/EBC**
- **Pre or post-examination:** Application Assistance Unit
  - **www.uspto.gov/PatentAssistance**

Want to learn more?

- **Access our free services** all in one spot. Find all of our contact centers, nationwide services, events, education, and training.
  - **www.uspto.gov/FreeServices**
- **Connect with us** on Instagram, LinkedIn, Twitter, Facebook, and YouTube.
- **Hear about resources for startups, inventors, and entrepreneurs,** as well as our initiatives engaging women, the military community, and others. These programs offer helpful tips and tricks on identifying and managing your IP, finding options for funding, and expanding your network to support your business.
  - **www.uspto.gov/startups**
  - **www.uspto.gov/inventors**
  - **www.uspto.gov/initiatives**
- We hope you connect with us by subscribing to receive important notifications by email.
  - **www.uspto.gov/subscribe**

Kathi Vidal

Kathi Vidal
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

Derrick Brent
Deputy Under Secretary of Commerce for Intellectual Property and
Deputy Director of the United States Patent and Trademark Office

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11856414 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — Signature
March 4, 2024 — Date

Blake R. Hartz, Reg. No. 73453 — Typed or printed name

Attorney of Record — Title
317-713-4970 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/25 (04-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 18/594,381, filed, March 4, 2024, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent granted on the pending **reference** application expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/	March 4, 2024
Signature	Date
Blake R. Hartz, Reg. No. 73453	
Typed or printed name	
Attorney of Record	317-713-4970
Title	Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11115834 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — Signature
March 4, 2024 — Date

Blake R. Hartz, Reg. No. 73453 — Typed or printed name

Attorney of Record — Title
317-713-4970 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/25 (04-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 18/532,175, filed, December 7, 2023, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent granted on the pending **reference** application expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/	March 4, 2024
Signature	Date
Blake R. Hartz, Reg. No. 73453	
Typed or printed name	
Attorney of Record	317-713-4970
Title	Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11849337 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — Signature
March 4, 2024 — Date

Blake R. Hartz, Reg. No. 73453 — Typed or printed name

Attorney of Record — Title
317-713-4970 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/25 (04-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 18/470,540, filed, September 20, 2023, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent granted on the pending **reference** application expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/	March 4, 2024
Signature	Date
Blake R. Hartz, Reg. No. 73453	
Typed or printed name	
Attorney of Record	317-713-4970
Title	Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	**03/04/2024 03:11:07 PM Z ET**	**020505-000010**

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	64538555	FILING DATE	-
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 9

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
10 TD over -7.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -5.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -6.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -2.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -4.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -3.pdf	1	Terminal Disclaimer Filed	406 KB
10 TD over -8.pdf	1	Terminal Disclaimer Filed	414 KB
10 TD over -9.pdf	1	Terminal Disclaimer Filed	414 KB
10 TD over -11.pdf	1	Terminal Disclaimer Filed	414 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
10 TD over -7.pdf	252E50CBDCE7586A040BBB84CA1634E4B8CFEC8254EF887B 82AC6D1D65019E90D6276D429182BC755B4B9D1E5EC542FD 3D86A0A5A42FD5F60CD438AFA594ABEE
10 TD over -5.pdf	DE0BA0003DA96C1C03D987BF2B218D5AEC99A4ECA987C7D 1B84B531DA3C88002261B6B507737425E5997F3339D5C73C96 A4407B1064A1306A6A12606EA821A8C
10 TD over -6.pdf	B7FB066F798F600980110455BC9C95FF9AC3D28D783E7AC91 2F3CE6CD9912BBE73FA1B859E481E46AC42CA30609AF716C D352ACE4B9292BF292B4063991A20BC
10 TD over -2.pdf	0E27C7EA1C2703E0D221A398276DC75261B6C6BBF8A17CA7 F2ADF848EFA04B1AC0BB05CFC1414076A8220480701729D22 7980E72EDDD5FDC32DF28E18E23977D
10 TD over -4.pdf	933C03C56335E4B280346EBC046EF4FE7EA5C40995B3265A6 3AC79A2D4FFF764355E6E902BABED45FC5F6FB04F9E01637 C15444F9CEDA4F5029E2F4621EDEEA1
10 TD over -3.pdf	DEC9B2BE0C873377DAE91CB151FB39BE258AAA4B982417AD B5E6D3F7AAF33512CE1005AEAE71F1D79B0232FD26C030CC CD880620C0A1E73B705039BFCA339101
10 TD over -8.pdf	9E1CF955CB912414E4628629218CB6CC4A4C484AADE79F2E 15983512291B7DBF39CB0B221C8CF8682332B9ADC36677A2C A665AFEFA445F9D157E806DCF1873B5
10 TD over -9.pdf	1ECDAF7117D16B81712850B3DBAC76CD9DC51D2EC56A7547 2CFDF14DCD61C1B698347F8BA9574F359C6FD7B18FCFE6B3 02562B013E4B785A572804F580A4E304
10 TD over -11.pdf	AF3EE8F9EEC2025238A73BA9AC444C0A8F16BE071697C0F23 C9171A3F0E0A6C5C2FA76997ADCE83101F11DF346527A5DD 0661B0E46CB452A031344FE9DCF5C7A

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage

submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 9788305 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — Signature
March 4, 2024 — Date

Blake R. Hartz, Reg. No. 73453 — Typed or printed name

Attorney of Record — Title
317-713-4970 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 11818591 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — March 4, 2024
Signature — Date

Blake R. Hartz, Reg. No. 73453
Typed or printed name

Attorney of Record — 317-713-4970
Title — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	**03/04/2024 03:11:07 PM Z ET**	**020505-000010**

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	64538555	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	**E202434F11585377**	**WALTER MOORE**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	9	1530.00
			TOTAL AMOUNT:	**$1,530.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/26 (04-14)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 020505-000010

In re Application of: Sai C. Manapragada

Application No.: 18/594,375

Filed: March 4, 2024

For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

The applicant, XiFi Networks R&D Inc., owner of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 10034179 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The applicant hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ The undersigned is the applicant. If the applicant is an assignee, the undersigned is authorized to act on behalf of the assignee.

I hereby acknowledge that any willful false statements made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 73453

/Blake R. Hartz, Reg. No. 73453/ — Signature
March 4, 2024 — Date

Blake R. Hartz, Reg. No. 73453 — Typed or printed name

Attorney of Record — Title
317-713-4970 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Attorney Docket No.: <PSYC.P101>

DECLARATION (37 CFR 1.63) FOR PROVISIONAL, UTILITY, DESIGN, OR NATIONAL STAGE OF PCT APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention: **SYSTEM AND METHOD FOR EXTENDING RANGE AND COVERAGE OF BANDWIDTH INTENSIVE WIRELESS DATA STREAMS**

As a below named inventor, I hereby declare that:

This declaration is directed to:

___X__ The attached application, or

_____ United States Provisional Application Number **[Enter App** #] filed on **[Enter Date]**, or

_____United States Application Number _____, filed on _____.

The above-identified application was made or authorized to be made by me.

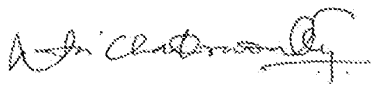
I have authorized and/or hereby do authorize my assignee to file patent applications claiming priority from the application referenced above, including provisional, non-provisional, design, divisional, continuation, continued prosecution, continuation-in-part, substitute, supplemental examination application, and other applications related to the subject matter of the application referenced above. I have authorized and/or hereby do authorize my assignee to make changes to the application for matters of formality.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under Section 1001 of Title 18 of the United States Code by fine or imprisonment of not more than five (5) years, or both.

Warning: Declarant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent.

Legal Name of Inventor:

Inventor: Sai C. Manapragada	Date: 10/28/2014
Signature: 	

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	**03/04/2024 01:44:34 PM Z ET**	**020505-000010**

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	64531364	FILING DATE	-
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 48

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
20505-10 Specification - Chipset Claims-APP.TEXT.docx	28	Application body structured text document	72 KB
Warning: Bookmarks were found and have been removed.			
ADS 20505-10.pdf	4	Application Data Sheet	128 KB
Warning: This is not a USPTO supplied ADS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.			
Declaration 20505-10.pdf	1	Oath or Declaration filed	196 KB
IDS transmittal 20505-10.pdf	4	Transmittal Letter	128 KB
General POA 20505-10.pdf	1	Power of Attorney	305 KB

Track One Request 20505-10.pdf	1	Track One Request	429 KB
20505-10 Specification - Chipset Claims.pdf	28	Auxiliary PDF of Application	192 KB
Drawings 20505-10.pdf	11	Drawings-only black and white line drawings	1227 KB
Stmt Under 37 CFR 3_73c 20505-10.pdf	2	Power of Attorney	665 KB
PTO SB08 20505-10.pdf	9	Information Disclosure Statement (IDS) Form (SB08)	1987 KB

Warning: This is not a USPTO supplied IDS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.

for_EP2016750B1.pdf	22	Foreign Reference	353 KB
for_EP2713670A1.pdf	28	Foreign Reference	501 KB
for_EP2055072B1.pdf	31	Foreign Reference	513 KB
for_EP3174323B1.pdf	31	Foreign Reference	398 KB
for_TWI500350B.pdf	24	Foreign Reference	1097 KB
for_EP3220697B1.pdf	41	Foreign Reference	1663 KB
npl_2011 WiSP-A-protocol-for-overcoming-MAC-overheads-using-packet-size-dependent-channel-widths.pdf	9	Non Patent Literature	617 KB
npl_2013 July 15 hew-discussion-on-potential-techniques-for-hew.pdf	13	Non Patent Literature	191 KB
npl_2013 March 19 beyond-802-11ac-a-very-high-capacity-wlan.pdf	12	Non Patent Literature	138 KB
npl_2013 Nov 11 hew-discussion-on-ofdma-in-hew.pdf	11	Non Patent Literature	56 KB
npl_2013 May 9 discussions-on-11ac-phy-efficiency.pdf	11	Non Patent Literature	314 KB
npl_2013 Nov 12 11-13-1331-02-0hew-proposed-direction-and-priorities-for-hew.pdf	17	Non Patent Literature	192 KB

npl_2013 Sept 16 hew-dl-mu-mimo-transmission-with-unequal-bandwidth.pdf	5	Non Patent Literature	49 KB
npl_2013 September 16 hew-multicat-transmission-for-hew.pdf	10	Non Patent Literature	83 KB
for_WO2014020407A1.pdf	45	Foreign Reference	1644 KB
npl_2014 July 9 ax-envisioning-11ax-phy-structure-part-ii.pdf	12	Non Patent Literature	76 KB
npl_2013 Sept 18 hew-discussion-on-access-mechanism-for-hew.pdf	10	Non Patent Literature	54 KB
npl_2014 July 14 ax-envisioning-11ax-phy-structure-part-i.pdf	11	Non Patent Literature	185 KB
npl_TWI500350B.pdf	2	Non Patent Literature	62 KB
npl_Jan 13 2013 Publication 1687-1499-2013-135.pdf	17	Non Patent Literature	1369 KB
npl_80211ac-2013.pdf	425	Non Patent Literature	4107 KB
npl_Performance_analysis_of_OFDMA_in_LTE.pdf	7	Non Patent Literature	5027 KB
npl_Reference 10.pdf	12	Non Patent Literature	6410 KB
npl_2013 Oct 16 An-Efficient.pdf	9	Non Patent Literature	262 KB
npl_2012 July A-Channel-Splitting.pdf	13	Non Patent Literature	1584 KB
npl_EP2055072B1.pdf	15	Non Patent Literature	8871 KB
npl_2012 OFMDA LTE.pdf	74	Non Patent Literature	12702 KB
for_EP2555578A1.pdf	17	Foreign Reference	300 KB
for_KR20070061684A.pdf	27	Foreign Reference	828 KB
npl_22862_61836571.pdf	19	Non Patent Literature	2073 KB
npl_22862_61835488.pdf	20	Non Patent Literature	2011 KB
for_GB2516132A.pdf	37	Foreign Reference	2072 KB
npl_22918_61888692.pdf	26	Non Patent Literature	1572 KB

npl_22918_61890713.pdf	41	Non Patent Literature	3699 KB
npl_31817_61824338.pdf	81	Non Patent Literature	3892 KB
npl_22918_61870762.pdf	68	Non Patent Literature	9272 KB
npl_KR20070061684A.pdf	8	Non Patent Literature	7726 KB
for_EP1878169B1.pdf	91	Foreign Reference	18974 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
20505-10 Specification -Chipset Claims-APP.TEXT.docx	0DB67133186FCE428859720FD1A179D6AFCB5BB5FD64B3BC BE4326749766670E0507FEF3A9540D46608A4AACEC9C0F94A 08E1EA54BB878F83FFE27F4AD8334A8
ADS 20505-10.pdf	0537E4A9E14D3F3B9E9F8060553389D1251C5B06C88C4FB6A BCEAEDE3C592093A2E276A3061801DB0260A382FF55140D94 43336F5EB9D7AA068C79BF86EA9802
Declaration 20505-10.pdf	E44B1E070A12FC3DA4BBF99F51166E5142D21150DB9BB8166 8C0E2DBA940D2BF9CA6D9EF661A01ADC4C6429D0D27524A5 6BDFFFBA97DE3C0CF36E366BDDAC85C
IDS transmittal 20505-10.pdf	E9841A95612E68187AB2804DF59D2AB5F7374AD8CF65C3046 146902C4F95F6DACE3774EE8B6DB4086FAFA0E6715AA87D8 191E484EA32D63A7415AD33992CBB5A
General POA 20505-10.pdf	21BF0DAB00D40A13B5034E735E76E457CE253D81921393010 55A74E17E8F3413DED3CD9715136C7A1362A1D16942E72976 8E603659F5969A5BD75DCB4C07BE26
Track One Request 20505-10.pdf	8E73E3CA91BA9BC2128E2EC1A9B77E3514611C68CBB654F0 A5E06A3692986D2EF50844A4C075CDF69898EC440C5F5D2DF 80E75121B421956E76039B4A98D50EB
20505-10 Specification -Chipset Claims.pdf	6BD61A7A196DA83A021F697A202C5F95AAE9C439F4516D0D B50924C959A616FB3E8B161BB184828048A334EB0F1668F5C0 FFC1EA1F627F04274F10B5ECA53781
Drawings 20505-10.pdf	440F9689B6A106FDCC0EDEBCDF4E63BD789D76C4D950C655 0E1032429A99F257C5650C6D0B506375CD33390F6DC041E2C 62383DCC7A72D81941E6C822C39BBA5
Stmt Under 37 CFR 3_73c 20505-10.pdf	F24EAEF539ACA5D704A90B8630EA5F49971F2F6AFF35B6541 BB92417D44A6EFBE0CC7D29C6026C5B15580EAB603E7556A A409137B01348F1F7F5CB90BA7009F7
PTO SB08 20505-10.pdf	952C771F1A05C62DA662CDE20C86F016F25D8B08C04DD939 32C61EED9C3DA99ADC3607373B600651C6902FD4E26463E41

	6D49326158BD4FA8F79F46C5F3A607C
for_EP2016750B1.pdf	5C2CA4633498891C7CC37DB3D9B87702AA75A840BFDA049E B70B9DF40E2A7E77C429001C0ADED3ACA8A1BB0DA64DCA9 D1A489124D4EE33B4C04DC0C8F2A4BA24
for_EP2713670A1.pdf	D309034C1D92F0223E7354D2F2AB7A427F9712B7D1F54274A 7BE1130CBA231A130FB52A6FB214A1D81DD47F1ACBA1CFB0 B27927943387783C54815EE77E63BE6
for_EP2055072B1.pdf	9D25FDA5D3D2C02FCBC8A5B945681B3C974A5FF0A763B9AF E4EF22999433924A774DBF183FCD6A6C8AAB23282CCCAF84 020449A0F33B8219F17B220654FF3021
for_EP3174323B1.pdf	1106407D4184786449FC2C0AAF990B2A7928D5C5743B445A45 91223710FD8938B330B14937CD1D098C41A331D3AED41D0B2 4526B715303D11E95C8D7FB5E3ED5
for_TWI500350B.pdf	2A000ADDC8412D9E5F3D239BC2BB1B135699922BB9A65C99 B427F1248730557060442A6877F014E1118A515B156CE79ABD FFD22505CC9A24DE8E89CAD361ACDD
for_EP3220697B1.pdf	F90C74266902E8C14C2107CC02FC21AA7B12C24525115339B 2F956DA61382FC8F5531433176FF9CE367DBA1BACD72CF13 EB962F23E1F076B105D3756CB464C4C
npl_2011 WiSP-A-protocol-for-overcoming-MAC-overheads-using-packet-size-dependent-channel-widths.pdf	A48832E58768E2755F8D0BB61A43AE75A3611A3A776F4A1BF 0DE2CC98CE23F06D17EA4DA4AD3758744A2737818F87339C7 482B6E8549753CA6971C6226697F03
npl_2013 July 15 hew-discussion-on-potential-techniques-for-hew.pdf	BC34B3734A2F68E38302904CF0FA40DEAE5100041B07A3DCE 04B59D9BEDAA579D1924F2EB0F1C7D81BBE25ADE144DA5B C4181B74018FF966BC0CE6A6E9F8B22A
npl_2013 March 19 beyond-802-11ac-a-very-high-capacity-wlan.pdf	9F085867BDA21190385406970D3C334FACD5A66C35DF163F2 50D3C7C6D163D127CE4AB777840C821184931D46CBF90FBF BA4C23F17B84EC72EC7AE3F0C24376C
npl_2013 Nov 11 hew-discussion-on-ofdma-in-hew.pdf	5DFA22F587A184A597B34832FCE32A743252965679B136B381 93F8175493004D265C6E5B554985BAF7D98CB5DD9C49BF168 8E0FCC0F25F51C485DEE9BAD6F96E
npl_2013 May 9 discussions-on-11ac-phy-efficiency.pdf	E74FDD326ACEA3D29C6BEFACE28A38530E1E7D13715A6691 4C1E3341EE6590BC1580831E68B3D318CCEEB76850D530630 BEE0A1A33C550616E73A638C8A92961
npl_2013 Nov 12 11-13-1331-02-0hew-proposed-direction-and-priorities-for-hew.pdf	601D6BA15F858CA86097F071EBE11F30A7C6CE6D789332E89 73F7874BBCE8D9201C987C86FFC1893433011C65F5FBEDDB 3575B05E3E37786CB19C34910F054D0
npl_2013 Sept 16 hew-dl-mu-mimo-transmission-with-unequal-bandwidth.pdf	19E03ADEDAFB8A5C5D2C26CB7AEF11DA9CCD35D02AB1116 544AB3DCA2010C39AD5384547DC7874F5C8EC75C0ED5AE70 E9AFAF0AC53CFA85B866ACC65DCF76462

npl_2013 September 16 hew-multicat-transmission-for-hew.pdf	E51E2A58C69BC72A416E9051C05D5BF0C43E005557BC4322DC5B00CE1F48A1DA23076436D99AD93EAFC40DBF37DAF97E7EE180138AD96FE455CEE3E1226DE86B
for_WO2014020407A1.pdf	E27965FE5F588B5E251353BDF7141D2AF4B2665731BE7A706914E9571215FAB45498B82C265DA589B10BD0DFD040FEEC73C7B5041F1ACE7B5D6F37AF5AFE2AC0
npl_2014 July 9 ax-envisioning-11ax-phy-structure-part-ii.pdf	9FC232726897C2527248F09B8CD59837615DFFC93ED8D631528C3A6943DD77DB70D757AD71D38F3875213059832FA6A2F287DD6FC2255DBCDCB637F1AB9B11BB
npl_2013 Sept 18 hew-discussion-on-access-mechanism-for-hew.pdf	CE4E2EF7A953FFCEDAAF7B511A6D93E35E422D55305D3814730B37073F49458298C71A947368A7EFD5EF2B0CA88915701CCF830E43ED4918AFDFD6E5A17AD720
npl_2014 July 14 ax-envisioning-11ax-phy-structure-part-i.pdf	B963B4763E98556CD02A7029CD0C3F8678A843736FFE9BC7EF6D36096481430F5265F24AB4800B22D2CB012864111DB9CAC7E821B881AB75D61A9FA8FAAD03E0
npl_TWI500350B.pdf	6898E7CAF03CA3488DC69E57288573F6BC41ABEF1B0006320E5439DC3EB8F6878F48A8AC1736C1FD4744800C4A0CB422CA5F42F5B4EA0E0AF753DAB665273993
npl_Jan 13 2013 Publication 1687-1499-2013-135.pdf	E0ABF7B6E016FA7404BB54CE1BFED7204F5D191ED88500EA904DFCEF241D0CBBC6AE24DE087E915CAB857B06A29979CA89D3CEABADE2D64333DCF6A991CF1851
npl_80211ac-2013.pdf	152C5B7E98E5DE608C85C57ED69109B40A39C580F84A14A92A59946DFB9FD799A50FB1906CEDC91D386157AD0030C6D25AC7F5BF7F08EE1911E667FBAACB472E
npl_Performance_analysis_of_OFDMA_in_LTE.pdf	545016E766232F2FAA6B3A5E79B5C2932E65299D6C61780387FE02332481A44AFEDB5AC4E6B809E83E524A29C2DEB5BC2835FE9FAD974C5B436C69ADD21AD09B
npl_Reference 10.pdf	DDE455A473686A48E280237782A435AF1FCA7A7057B9CB61F03CFC50184079599A920361DA081CFCE223489BDA84CA0ABE6D905FB8F7780DE9156AD04267D1D2
npl_2013 Oct 16 An-Efficient.pdf	CB7D637C1185C0101205BB858C5562FF30EF75BFFB7C8272D9B0C3104ED48C671F27093C8FE4C46F2928C4210EA4954F7706AF1C3173A688C889DC0D079529ED
npl_2012 July A-Channel-Splitting.pdf	7E20E028E9EBCBC4F25854C055631EEA30E4F5D370A7CCDDAA77C63F189E2D7CFD5D837B537562C8216D5FEC1E6EB8785CFA0D544DCD16E9E1F0E979A7918041
npl_EP2055072B1.pdf	B1D0A0D1282AAB7D17634DF41E9857F520075CB38FAA0ECC3B538B7E607C7EFDF784589057C510567FDFBAE477ADBA94FCCF5834A13A944BDBBBBC9C1737AC87
npl_2012 OFMDA LTE.pdf	AE607AD3B61ED2BB2336645F4ADA8E618C56076DBBB4B287CF8763B52EBA5074A903C88A7BA701C637CDB93BFE5D821C

	93F35FF66850342FB62ED3432CD179C8
for_EP2555578A1.pdf	57AF22DEDCBFF4A12B7F641F85A5D04C9A61102BB96E7D19 46BFF13B89AF64161948FF00C30670FABADEC4BD92455683A 63A6B6F7EC249692FA3281C68116D32
for_KR20070061684A.pdf	53635E755AD526740B4B06D185D0ACFB8DFA3F10181A9E583 27526A4C92BF5D9FF14B26103686DC5C88904F7A5402C890A 3420DBF7D42B7FB0985F6A1DEEAC7A
npl_22862_61836571.pdf	358CEC9DE7B011F72E9D0C694920D53614F4EA4711380256A 0A6994D5A9A1FD47485D09D7758031B8E5BC16674D79C89E4 2826AF1810894B586D6FB143276327
npl_22862_61835488.pdf	626767760D0CDC938CC469CFB3A73E705E25C9983BFBBA96 AA1158561159119BE311B2820D4CF537C7E8844462F2513573 7C275B280FA3DB21DC3673F79DB642
for_GB2516132A.pdf	A4BCD0708EA4FE265582646E24A7C3CA9ACDED316BCBE2D 6B1FADEB062CCE3481A4F3C4BBE11E4483C4FE74F250F55D 9C391F2B0E60F791A00490481609D8B43
npl_22918_61888692.pdf	8A4B19ED82D2D74FE5630026406986D3EA1213581A2C8D955 6E8BD8810556832B437C17F3A647FCA645CC15466B48971A5 6D18DFAC11FCAF288BB4DC7C0C85B3
npl_22918_61890713.pdf	8EEA2025025E31B30DE55A050D9F303A46FD345A800FCF1AF 19BD049ECCBAA3AD365FFB461EF7680DB402684852D51BB6 4D0008C943453CAAB66E87949922A40
npl_31817_61824338.pdf	AA71645432A1B8A69CABBBDD612CD7DC64B4739B865369FE BDCE219E2A7518DEFC5847AF64FC1C43CBFB09611F2E5E71 044205DB541CB344976BDF8C8A456A0C
npl_22918_61870762.pdf	F605211D424A6425FF82A7F6FACE107DD53FC71FE4AFA12F1 66EB270D89AF2E0C277ACFC7A7CACD570E0D654EE71FEBB 942D7C0F1C550288763C8E425FC2C1AA
npl_KR20070061684A.pdf	78ACC50F643502F9DD3CDADF91BF1C940DD1B2EF4F5E5C1 77A8874C920B45F58942055161E2C2710DEFB16223D3C8E62 C7214B29C23A1EF4495651D5A10029CB
for_EP1878169B1.pdf	15B257C7642CD41194758BC8B3E51E4B22AB4E855BCD100D BBD391C97DE8C69A88329DADAC9EA0227506BC9425EFF504 BC5202601116E3A09F2E454B78C4A275

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 713 670 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.04.2014 Bulletin 2014/14

(51) Int Cl.:
H04W 76/00 *(2009.01)*

(21) Application number: **12186237.9**

(22) Date of filing: **27.09.2012**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **BlackBerry Limited**
Waterloo, ON N2K 0A7 (CA)

(72) Inventors:
- **Smadi, Mohammed Nawaf**
  Waterloo
  Ontario N2L 3W8 (CA)
- **Montemurro, Michael Peter§**
  Mississauga
  Ontario L4W 0B5 (CA)

(74) Representative: **Hibbert, Juliet Jane Grace et al**
Kilburn & Strode LLP
Electronics
20 Red Lion Street
London WC1R 4PJ (GB)

(54) Methods and apparatus for use in communicating in a peer-to-peer (p2p) network

(57) Techniques for use in a wireless device which is configured to operate as a group owner (GO) in a peer-to-peer (P2P) network are described. The group owner sends a first multicast message to one or more first P2P devices in the P2P network. The first multicast message includes first notice of absence (NoA) data. The group owner also sends a second multicast message to one or more second P2P devices in the P2P network. The second multicast message includes second NoA data. Partitioning in the P2P network in this fashion may be set based on the different types of communications established with the P2P devices (e.g. different traffic classes or Quality of Service (QoS) types).

EP 2 713 670 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND

Field Of The Technology

[0001] The present disclosure relates generally to communication devices configured for wireless communications, such as IEEE 802.11 based communications, including techniques for use in communicating in a peer-to-peer (P2P) network.

Description Of The Related Art

[0002] A wireless communication device, such as a portable wireless telephony device or smartphone, may be configured to communicate in wireless communication networks. For example, such a device may communicate via access points (APs) of wireless local area networks (WLANs) in accordance with IEEE 802.11 standards or the like. Such devices may also communicate using peer-to-peer communication techniques, for example, in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification, and/or be certified as a "Wi-Fi Direct" device.

[0003] There is a need for efficiently facilitating communications in these and similar environments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Embodiments of present disclosure will now be described by way of example with reference to attached figures, wherein:

FIG. 1 is an illustrative representation of a communication system which includes wireless communication networks (e.g. WLANs) with which a wireless communication device may communicate;
FIG. 2 is an example of a schematic block diagram of the wireless device of FIG. 1;
FIGs. 3 and 4 are some examples of different types of wireless devices of the present disclosure, which include a smartphone (FIG. 3) and a tablet computer (FIG. 4);
FIG. 5 is an illustrative representation of a part of the communication system of FIG. 1 which may involve different types of wireless networks and communications;
FIG. 6 is an illustrative representation of a portion of memory of the wireless device, where the memory has a plurality of profiles stored therein, where each profile is associated with a first type of wireless connection (e.g. a client station type) or a second type of wireless connection (e.g. a peer-to-peer type);
FIG. 7 is a block diagram for illustrating concurrent operations of the wireless device which may operate as a group owner (GO) in a P2P network;
FIG. 8 is an illustration of the format of a message which may be utilized for multicast addressing for communicating different Notice of Absence (NoA) data to different multicast groups;
FIG. 9 is a flowchart for describing a method for use in communicating in a P2P network;
FIG. 10 is a timing diagram of communications involving the wireless device operating as a group owner in a P2P network, scheduling absences in the P2P network by communicating NoA data without use of the technique of FIG. 9;
FIG. 11 is another timing diagram of communications involving the wireless device operating as a group owner in a P2P network, scheduling absences in the P2P network by communicating different NoA data to different multicast groups using the technique of FIG. 9; and
FIG. 12 is a close-up of a portion of the timing diagram of FIG. 11, showing the differences in doze periods of the different multicast groups based on the different NoA data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0005] Techniques for use in a wireless device which is configured to operate as a group owner (GO) in a peer-to-peer (P2P) network are described herein. The group owner sends a first multicast message to one or more first P2P devices in the P2P network. The first multicast message includes first notice of absence (NoA) data. The group owner also sends a second multicast message to one or more second P2P devices in the P2P network. The second multicast message includes second NoA data. Partitioning in the P2P network in this fashion is set based on the different types of communications established with the P2P devices (e.g. different traffic classes or Quality of Service (QoS) types).

[0006] To illustrate one environment within which the techniques of the present disclosure may be practiced, FIG. 1 illustrates a wireless communication device 201 which may communicate in a communication system 100. In the communication system 100, wireless device 201 may communicate with one or more wireless communication networks. For example, wireless device 201 may communicate with a wireless communication network 104 which is a wireless local area network (WLAN). Here, wireless network 104 and wireless device 201 may operate in accordance with IEEE 802.11 standards.

[0007] In this example, wireless network 104 has a plurality of wireless access points (APs) 112, 114, and 116 for wireless communications with wireless device 201. WLANs may be identified by a wireless device 201 with use of a wireless network identifier which is communicated from the WLAN. The wireless network identifier may be, for example, a Set Service Identifier (SSID) or Extended SSID (ESSID). In this example, wireless network 104 includes one or more servers 106, a redirect server 108, and a gateway 110. Server 106 may provide

Samsung Ex. 1004, Page 109 of 563

data, applications, and/or functionality for communication services for wireless device 201.

[0008] Wireless network 104 may be a public Wi-Fi "hotspot" for public use, and include what may be referred to as a "captive portal" or "walled garden." For devices connected in wireless network 104 via one of wireless APs 112, 114, and 116, gateway 110 is configured to permit or deny access to the data, applications, and/or functionality, as well as to permit or deny external access outside of wireless network 104 to Internet 120. To do this, gateway 110 has a set of IP address filters which define a set of addresses that are permissible/impermissible, if any at all, for access by devices. Access by a device depends on whether or not a device has been authorized and what access rights are given upon authorization.

[0009] Typically, when a request by a device in wireless network 104 is made prior to proper authorization, gateway 110 is configured to redirect the request to redirect server 108. In response, redirect server 108 is configured to respond to wireless device 201 to provide data for producing information (e.g. Web page information) which is rendered in a visual display of wireless device 201 via a Web browser application. The information may solicit a user response. For example, the information may solicit a user registration or login with user fields for entering a user name and/or password information. Gateway 110 identifies whether the received user response is sufficient (e.g. whether the user name and password match prestored user name and password information, whether the user payment is accepted, whether the user acceptance is confirmed, etc.). If the user response is deemed sufficient, gateway 110 permits access to the data, applications, and/or functionality in or outside of wireless network 104.

[0010] Wireless device 201 may also operate for communications in other different wireless networks, such as a wireless network 122 which is also a WLAN. In this example, wireless network 122 is a private communication network of an enterprise (e.g. an organization, a company, a corporation, etc.) of wireless device 201. Similar to wireless network 104, wireless network 122 has a plurality of wireless APs 128, 130 and 132, one or more servers 124, and a gateway 126. For devices connected in wireless network 122 via one of wireless APs 128, 130, and 132, gateway 126 may be configured to permit or deny access to the data, applications, and/or functionality offered via wireless network 122 depending on whether or not a device has been authorized and what access rights are given upon authorization. For devices attempting to access wireless network 122 via Internet 120, gateway 126 is configured to permit or deny internal access to the data, applications, and/or functionality in wireless network 122.

[0011] Such wireless networks (e.g. infrastructure WLANs) may provide or allow access to various data and communication services to its terminals. For example, the wireless networks may provide for communication access to Internet 120 via the Web browser application, or voice telephony communication service with use of Voice over IP (VoIP) communication, or other communication services. For "push-type" data or message synchronization services, for example, wireless device 201 may be enabled to maintain data synchronization with a server (e.g. server 106 or 118) for user data of an application associated with a user account. The application of wireless device 201 and the server may be or include, for example, an electronic mail (e-mail) application program for the communication of e-mail messages.

[0012] Wireless device 201 may be additionally configured to access communication services via a Public Land Wireless Network (PLMN) 136 (e.g. a cellular telecommunications network). PLMN 136 includes a core network 134, a plurality of base station controllers such as a base station controller (BSC) 138 coupled to core network 134, and a plurality of base stations such as a base station (BS) 140 and a base station 142 coupled to associated BSCs 138. Core network 134, BSC 138, and BS 140 operate in a conventional fashion as well-documented. Other PLMNs in the environment have a similar or the same architecture as PLMN 136. For communication with PLMNs, wireless device 201 may be configured in accordance with one or more cellular telecommunication standards, such as Global Systems for Mobile (GSM) and/or General Packet Radio Service (GPRS) technologies. However, such wireless device may additionally or alternatively operate in accordance with other such cellular standards, such as Enhanced Data rates for GSM Evolution (EDGE) or Enhanced GPRS (EGPRS), Universal Mobile Telecommunications System (UMTS), Long-Term Evolution (LTE), or EVolution-Data Only (EV-DO) (for CDMA) technologies, as a few examples.

[0013] Further, in additional to being operative for communications with infrastructure WLANs (e.g. IEEE 802.11 infrastructure WLANs), wireless device 201 may additionally or alternatively communicate using peer-to-peer communication techniques, for example, in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification, and/or be certified as a "Wi-Fi Direct" device. The Wi-Fi Peer-To-Peer (P2P) Technical specification is hereby incorporated by reference herein.

[0014] Accordingly, illustrating further in FIG. 1, wireless device 201 and one or more other wireless devices 195 and 197 in FIG. 1 may be operative to establish Wi-Fi P2P network connections with each other in a Wi-Fi P2P network. Here, one of the communicate devices may be configured to enter into an AP mode of operation, so that other communication devices may associate with them for direct RF communications therebetween. In some environments, a wireless device may operate in an AP mode of operation as what is referred to as a group owner (GO). Such operation provides a benefit due to the high data rates available over WLAN links. Here, again, data may be communicated directly between the wireless devices without the data traversing any wireless network infrastructure, where one of the devices is set

to operate or serve as an AP (switching operation from as an end terminal) and the other device operates as an end terminal to associate and connect with the AP (i.e. wireless device 201 operating as an AP) for communications. Wireless device 201 may operate such that, when operating as an AP with other communication devices 195 and 197, it also operates as a client station with another AP (see e.g. discussion later in relation to FIG. 5).

[0015] Reference will now be made to FIG. 2 which illustrates one example of a schematic block diagram of wireless device 201 in which example embodiments may be applied. In the illustrated example embodiment, wireless device 201 is a communication device and, more particularly, is a mobile communication device having data and voice communication capabilities, and configured to communicate with other computer systems (e.g. via the Internet). It will, however, be appreciated that wireless device 201 may take other forms.

[0016] Depending on the functionality provided by wireless device 201, in various example embodiments wireless device 201 may be a multiple-mode communication device configured for both data and voice communication, a mobile telephone, such as a smartphone, a wearable computers such as a watch, a tablet computer such as a slate computer, a personal digital assistant (PDA), or a computer system. Wireless device 201 may take other forms apart from those specifically listed above. The electronic device may also be referred to as a mobile communications device, a communication device, a mobile device and, in some cases, as a device.

[0017] Wireless device 201 includes a controller including one or more processor 240 (such as a microprocessor) which controls the overall operation of wireless device 201. The processor 240 interacts with device subsystems such as a wireless communication subsystem 211 for exchanging radio frequency signals with wireless network 104 to perform communication functions. The processor 240 is communicably coupled with additional device subsystems including one or more output interfaces 205 (such as a display 204 and/or a speaker 256 and/or electromagnetic (EM) radiation source 257), one or more input interfaces 206 (such as a camera 253, microphone 258, keyboard (not shown), control buttons (not shown), a navigational input device (not shown), and/or a touch-sensitive overlay (not shown)) associated with a touchscreen display 204, an orientation subsystem 249, memory (such as flash memory 244, random access memory (RAM) 246, read only memory (ROM) 248, etc.), auxiliary input/output (I/O) subsystems 250, a data port 252 (which may be a serial data port, such as a Universal Serial Bus (USB) data port), a near field communications (NFC) subsystem 265, a short-range communication subsystem 262 and other device subsystems generally designated as 264. Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions.

[0018] In at least some example embodiments, wireless device 201 may include a touchscreen display which acts as both an input interface 206 (i.e. touch-sensitive overlay) and an output interface 205 (i.e. display). The touchscreen display may be constructed using a touch-sensitive input surface which is connected to an electronic controller and which overlays the display 204. The touch-sensitive overlay and the electronic controller provide a touch-sensitive input interface 206 and the processor 240 interacts with the touch-sensitive overlay via the electronic controller. In at least some example embodiments, the touch-sensitive overlay may have a touch-sensitive input surface which is larger than the display 204. For example, in at least some example embodiments, the touch-sensitive overlay may extend overtop of a frame 312 (of FIG. 3) which surrounds the display 204. In such example embodiments, the frame 312 (of FIG. 3) may be referred to as an active frame since it is capable of acting as an input interface 206. In at least some example embodiments, the touch-sensitive overlay may extend to the sides of wireless device 201.

[0019] As noted above, in some example embodiments, wireless device 201 may include a communication subsystem 211 which allows wireless device 201 to communicate over wireless network 104. The communication subsystem 211 includes a receiver 212, a transmitter 213, and associated components, such as one or more antenna elements 214 and 215, local oscillators (LOs) 216, and a processing module such as a digital signal processor (DSP) 217. The antenna elements 214 and 215 may be embedded or internal to wireless device 201 and a single antenna may be shared by both receiver and transmitter. The particular design of the wireless communication subsystem 211 depends on wireless network 104 in which wireless device 201 is intended to operate.

[0020] In at least some example embodiments, wireless device 201 may communicate with any one of a plurality of stations or access points (APs) of wireless network 104 within its geographic coverage area. Wireless device 201 may send and receive communication signals over wireless network 104 after the required network registration or activation procedures have been completed. Signals received by the antenna 214 through wireless network 104 are input to the receiver 212, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, etc., as well as analog-to-digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in the DSP 217. In a similar manner, signals to be transmitted are processed, including modulation and encoding, for example, by the DSP 217. These DSP-processed signals are input to the transmitter 213 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification, and transmission to wireless network 104 via the antenna 215. The DSP 217 not only processes communication signals,

Samsung Ex. 1004, Page 111 of 563

but may also provide for receiver and transmitter control. For example, the gains applied to communication signals in the receiver 212 and the transmitter 213 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 217.

[0021] In some example embodiments, the auxiliary input/output (I/O) subsystems 250 may include an external communication link or interface; for example, an Ethernet connection. Wireless device 201 may include other wireless communication interfaces for communicating with other types of wireless networks; for example, a wireless network such as an orthogonal frequency division multiplexed (OFDM) network. The auxiliary I/O subsystems 250 may include a vibrator for providing vibratory notifications in response to various events on wireless device 201 such as receipt of an electronic communication or incoming phone call, or for other purposes such as haptic feedback (touch feedback).

[0022] The data port 252 may be used for synchronization with a user's host computer system (not shown). The data port 252 enables a user to set preferences through an external device or software application and extends the capabilities of wireless device 201 by providing for information or software downloads to wireless device 201 other than through wireless network 104. The alternate download path may for example, be used to load an encryption key onto wireless device 201 through a direct, reliable and trusted connection to thereby provide secure device communication.

[0023] In at least some example embodiments, wireless device 201 also includes a device orientation subsystem 249 including at least one orientation sensor 251 which is connected to the processor 240 and which is controlled by one or a combination of a monitoring circuit and operating software. The orientation sensor 251 detects the orientation of the device 201 or information from which the orientation of the device 201 can be determined, such as acceleration. In some example embodiments, the orientation sensor 251 is an accelerometer, such as a three-axis accelerometer. An accelerometer is a sensor which converts acceleration from motion (e.g. movement of the device 201 or a portion thereof due to the strike force) and gravity which are detected by a sensing element into an electrical signal (producing a corresponding change in output). Accelerometers may be available in one, two or three axis configurations. Higher order axis configurations are also possible. Accelerometers may produce digital or analog output signals depending on the type of accelerometer.

[0024] An orientation sensor 251 may generate orientation data which specifies the orientation of wireless device 201. The orientation data, in at least some example embodiments, specifies the orientation of the device 201 relative to the gravitational field of the earth.

[0025] In some example embodiments, the orientation subsystem 249 may include other orientation sensors 251, instead of or in addition to accelerometers. For example, in various example embodiments, the orientation subsystem 249 may include a gravity sensor, a gyroscope, a tilt sensor, an electronic compass or other suitable sensor, or combinations thereof. In some example embodiments, the device orientation subsystem 249 may include two or more orientation sensors 251 such as an accelerometer and an electronic compass.

[0026] Wireless device 201 may, in at least some example embodiments, include a near field communications (NFC) subsystem 265. The NFC subsystem 265 is configured to communicate with other wireless devices 201 and/or tags, using an NFC communications protocol. NFC is a set of short-range wireless technologies which typically require a distance of 4 cm or less for communications. The NFC subsystem 265 may include an NFC chip and an NFC antenna.

[0027] Wireless device 201 may include a microphone and/or one or more speakers. In at least some example embodiments, wireless device 201 may include a plurality of speakers 256. For example, in some example embodiments, wireless device 201 may include two or more speakers 265. The two or more speakers 256 may, for example, be disposed in spaced relation to one another. That is, in at least some example embodiments, wireless device 201 may include a first speaker and a second speaker and the first speaker and the second speaker may be spatially separated from one another within wireless device 201. In at least some example embodiments, the display 204 may be disposed between the first speaker and the second speaker of the electronic device. In such example embodiments, the first speaker may be located at one side of the display 204 and the second speaker may be located at another side of the display which is opposite the side of the display where the first speaker is located. For example, the first speaker may be disposed at a left side of the display and the second speaker may be disposed at a right side of the display. In at least some example embodiments, each speaker 256 may be associated with a separate audio channel. The multiple speakers may, for example, be used to provide stereophonic sound (which may also be referred to as stereo).

[0028] Wireless device 201 may also include one or more cameras 253. The one or more cameras 253 may be capable of capturing images in the form of still photographs or motion video. In at least some example embodiments, wireless device 201 includes a front facing camera 253. A front facing camera is a camera which is generally located on a front face of wireless device 201. The front face is typically the face on which a display 204 is mounted. That is, the display 204 is configured to display content which may be viewed from a side of wireless device 201 where the camera 253 is directed. The front facing camera 253 may be located anywhere on the front surface of the electronic device; for example, the camera 253 may be located above or below the display 204. The camera 253 may be a fixed position camera which is not movable relative to the display 204 of wireless device 201 and/or the housing of wireless device 201. In such

Samsung Ex. 1004, Page 112 of 563

example embodiments, the direction of capture of the camera is always predictable relative to the display 204 and/or the housing. In at least some example embodiments, the camera may be provided in a central location relative to the display 204 to facilitate image acquisition of a face.

[0029] In at least some example embodiments, wireless device 201 includes an electromagnetic (EM) radiation source 257. In at least some example embodiments, the EM radiation source 257 is configured to emit electromagnetic radiation from the side of the electronic device which is associated with a camera 253 of that wireless device 201. For example, where the camera is a front facing camera 253, wireless device 201 may be configured to emit electromagnetic radiation from the front face of wireless device 201. That is, in at least some example embodiments, the electromagnetic radiation source 257 is configured to emit radiation in a direction which may visible by the camera. That is, the camera 253 and the electromagnetic radiation source 257 may be disposed on wireless device 201 so that electromagnetic radiation emitted by the electromagnetic radiation source 257 is visible in images obtained by the camera.

[0030] In some example embodiments, the electromagnetic radiation source 257 may be an infrared (IR) radiation source which is configured to emit infrared radiation. In at least some example embodiments, the electromagnetic radiation source 257 may be configured to emit radiation which is not part of the visible spectrum. The camera 253 may be a camera which is configured to capture radiation of the type emitted by the electromagnetic radiation source 257. Accordingly, in at least some example embodiments, the camera 253 is configured to capture at least some electromagnetic radiation which is not in the visible spectrum.

[0031] In some example embodiments, wireless device 201 is provided with a service routing application programming interface (API) which provides an application with the ability to route traffic through a serial data (i.e., USB) or Bluetooth® (Bluetooth® is a registered trademark of Bluetooth SIG, Inc.) connection to a host computer system using standard connectivity protocols. When a user connects their wireless device 201 to the host computer system via a USB cable or Bluetooth® connection, traffic that was destined for wireless network 104 is automatically routed to wireless device 201 using the USB cable or Bluetooth® connection. Similarly, any traffic destined for wireless network 104 is automatically sent over the USB cable Bluetooth® connection to the host computer system for processing.

[0032] Wireless device 201 also includes a battery 238 as a power source, which is typically one or more rechargeable batteries that may be charged for example, through charging circuitry coupled to a battery interface 236 such as the data port 252. The battery 238 provides electrical power to at least some of the electrical circuitry in wireless device 201, and the battery interface 236 provides a mechanical and electrical connection for the battery 238. The battery interface 236 is coupled to a regulator (not shown) which provides a regulated voltage V to the circuitry for powering wireless device 201.

[0033] Wireless device 201 includes a short-range communication subsystem 262 which provides for wireless communication between wireless device 201 and other wireless devices 201. The short-range communication subsystem 262 may be used to provide a preferred device mode between wireless device 201 and another wireless device 201 which may, in at least some example embodiments, be a wireless device which is the same or similar to wireless device 201 discussed with reference to FIG. 1. In at least some example embodiments, the short-range communication subsystem 262 is a wireless bus protocol compliant communication mechanism such as a Bluetooth® communication module to provide for communication with similarly-enabled systems and devices.

[0034] Wireless device 201 stores data 227 in an erasable persistent memory, which in one example embodiment is the flash memory 244. In various example embodiments, the data 227 includes service data including information required by wireless device 201 to establish and maintain communication with wireless network 104. The data 227 may also include user application data such as email messages, address book and contact information, calendar and schedule information, notepad documents, image files, and other commonly stored user information stored on wireless device 201 by its user, and other data. The data 227 stored in the persistent memory (e.g. flash memory 244) of wireless device 201 may be organized, at least partially, into one or more databases or data stores. The databases or data stores may contain data items of the same data type or associated with the same application. For example, email messages, contact records, and task items may be stored in individual databases within the device memory.

[0035] Wireless device 201 may, in some example embodiments, be a mobile communication device which may provide two principal modes of communication: a data communication mode and a voice communication mode. In the data communication mode, a received data signal such as a text message, an email message, or Web page download will be processed by the communication subsystem 211 and input to the processor 240 for further processing. For example, a downloaded Web page may be further processed by a browser application or an email message may be processed by an email messaging application and output to the display 204. A user of wireless device 201 may also compose data items, such as email messages; for example, using the input devices in conjunction with the display 204. These composed items may be transmitted through the communication subsystem 211 over wireless network 104.

[0036] In the voice communication mode, wireless device 201 provides telephony functions and operates as a typical cellular phone. The overall operation is similar, except that the received signals would be output to the

Samsung Ex. 1004, Page 113 of 563

speaker 256 and signals for transmission would be generated by a transducer such as the microphone 258. The telephony functions are provided by a combination of software/firmware (i.e., a voice communication module) and hardware (i.e., the microphone 258, the speaker 256 and input interfaces 206). Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on wireless device 201. Although voice or audio signal output is typically accomplished primarily through the speaker 256, the display screen 204 may also be used to provide an indication of the identity of a calling party, duration of a voice call, or other voice call related information.

[0037] The processor 240 operates under stored program control and executes software modules 221 stored in memory such as persistent memory; for example, in the flash memory 244. As illustrated in FIG. 1, the software modules 221 include operating system software 223 and other software applications 225 such as preferred device mode module 260. In the example embodiment of FIG. 1, the preferred device mode module 260 is implemented as a stand-alone application 225. However, in other example embodiments, the preferred device mode module 260 could be implemented as part of the operating system 223 or another application 225.

[0038] The software applications 225 on wireless device 201 may also include a range of additional applications, including for example, a notepad application, Internet browser application, voice communication (i.e. telephony) application, mapping application, or a media player application, or any combination thereof. Each of the software applications 225 may include layout information defining the placement of particular fields and graphic elements (e.g. text fields, input fields, icons, etc.) in the user interface (e.g. the display 204) according to the application.

[0039] The software modules 221 or parts thereof may be temporarily loaded into volatile memory such as the RAM 246. The RAM 246 is used for storing runtime data variables and other types of data or information, as will be apparent to those skilled in the art. Although specific functions are described for various types of memory, this is merely one example, and those skilled in the art will appreciate that a different assignment of functions to types of memory could also be used.

[0040] A predetermined set of applications that control basic device operations, including data and possibly voice communication applications will normally be installed on wireless device 201 during or after manufacture. Additional applications and/or upgrades to the operating system 223 or software applications 225 may also be loaded onto wireless device 201 through wireless network 104, the auxiliary I/O subsystem 250, the data port 252, the short-range communication subsystem 262, or other suitable subsystem 264. The downloaded programs or code modules may be permanently installed; for example, written into the program memory (i.e. the flash memory 244), or written into and executed from the RAM 246 for execution by the processor 240 at runtime.

[0041] Example Smartphone Electronic Device. Referring now to FIG. 3, what is shown is a front view of an example wireless device 201 which is a smartphone 350. The smartphone 350 is a mobile phone which offers more advanced computing capability than a basic non-smartphone cellular phone. For example, the smartphone 350 may have the ability to execute third party applications which are stored on the smartphone.

[0042] The smartphone 350 may include the components discussed above with reference to FIG. 2 or a subset of those components. The smartphone 350 includes a housing 294 which houses at least some of the components discussed above with reference to FIG. 2.

[0043] In the example embodiment illustrated, the smartphone includes a display 204, which may be a touchscreen display which acts as an input interface 206. The display 204 is disposed within the smartphone 350 so that it is viewable at a front side 292 of the smartphone 350. That is, a viewable side of the display 204 is disposed on the front side 292 of the smartphone. In the example embodiment illustrated, the display 204 is framed by the housing 294.

[0044] The example smartphone 350 also includes other input interfaces 206 such as one or more buttons, keys or navigational input mechanisms. In the example illustrated, at least some of these additional input interfaces 206 are disposed for actuation at the front side 292 of the smartphone.

[0045] The example smartphone also includes a speaker 256. In the example embodiment illustrated, the smartphone includes a single speaker 256 which is disposed vertically above the display 204 when the smartphone 350 is held in a portrait orientation where its height is longer than its width. The speaker 256 may be disposed on the front face of the smartphone 350.

[0046] While the example smartphone 350 of FIG. 3 includes a single speaker 256, in other example embodiments, the smartphone 350 may include a greater number of speakers 256. For example, in at least some example embodiments, the smartphone 350 may include a second speaker 256 which is disposed vertically below the display 204 when the smartphone is held in a portrait orientation where its height is longer than its width (i.e. the orientation illustrated in FIG. 3).

[0047] The example smartphone 350 also includes a microphone 258. In the example illustrated, the microphone 258 is vertically disposed below the display 204 when the smartphone is held in the portrait orientation. The microphone 258 and at least one speaker 256 may be arranged so that the microphone is in close proximity to a user's mouth and the speaker 256 is in close proximity to a user's ear when the user holds the phone to their face to converse on the smartphone.

[0048] The example smartphone 350 also includes a front facing camera 253 which may be located vertically above the display 204 when the smartphone 350 is held in a portrait orientation where its height is longer than its

Samsung Ex. 1004, Page 114 of 563

width. The front facing camera 253 is located so that it may capture images of objects which are located in front of and/or surrounding the front side of the smartphone 350.

[0049] The example smartphone 350 also includes an electromagnetic radiation source 257. The electromagnetic radiation source 257 is disposed on the front side 292 of the smartphone 350. In this orientation, electromagnetic radiation which is produced by the electromagnetic radiation source 257 may be projected onto objects which are located in front of and/or surrounding the front side of the smartphone 350. Such electromagnetic radiation (or the projection of electromagnetic radiation onto objects) may be captured on images obtained by the camera 253.

[0050] Example Tablet Electronic Device. The wireless device may be a tablet computer 300 ("table"), one of which is illustrated in FIG. 4. Tablet computer 300 of FIG. 4 may include many of the same features and components of the smartphone 350 of FIG. 3. However, tablet computer 300 of FIG. 3 is generally larger than the smartphone 350 of FIG. 3. Tablet computer 300 may include the components discussed above with reference to FIG. 2 or a subset of those components. Tablet computer 300 includes a housing 394 which houses at least some of the components discussed above with reference to FIG. 2.

[0051] Tablet computer 300 includes a display 304, which may be a touchscreen display which acts as an input interface 206. The display 304 is disposed within tablet computer 300 so that it is viewable at a front side 302 of tablet computer 300. That is, a viewable side of the display 304 is disposed on the front side 302 of tablet computer 300. In the example embodiment illustrated, the display 304 is framed by the housing 394, with use of a frame 312 which surrounds the display 304. The frame 312 is portion of the housing 394 which provides a border around the display 304. In at least some example embodiments, the frame 312 is an active frame 312. That is, the frame has a touch sensitive overlay which allows wireless device 201 to detect a touch applied to the frame, thereby allowing the frame 312 to act as an input interface 206 (of FIG. 1).

[0052] The example tablet computer 300 includes a plurality of speakers 256. In the example embodiment illustrated, the tablet includes two speakers 256. The two speakers 256 are disposed on opposing sides of the display 304. More particularly, when tablet computer 300 is held in a landscape orientation (such as the orientation illustrated in FIG. 3) where its width is longer than its height, one of the two speakers is disposed on a right side 306 of the display 304 and one of the speakers is disposed on the left side 308 of the display 304. Both speakers 256 are disposed on the front side 302 of tablet computer 300.

[0053] The example tablet computer 300 also includes a microphone 258. In the example illustrated, the microphone 258 is vertically disposed below the display 304 when the tablet computer is held in the landscape orientation illustrated in FIG. 4. The microphone 258 may be located in other locations in other example embodiments.

[0054] The example tablet computer 300 also includes a front facing camera 253 which may be located vertically above the display 304 when tablet computer 300 is held in a landscape orientation (i.e. the orientation of FIG. 3). The front facing camera 253 is located so that it may capture images of objects which are located in front of and/or surrounding the front side of tablet computer 300.

[0055] The example tablet computer 300 also includes an electromagnetic radiation source 257. The electromagnetic radiation source 257 is disposed on the front side 304 of tablet computer 300. In this orientation, electromagnetic radiation which is produced by the electromagnetic radiation source 257 may be projected onto objects which are located in front of and/or surrounding the front side 302 of tablet computer 300. Such electromagnetic radiation (or the projection of electromagnetic radiation onto objects) may be captured on images obtained by the camera 253.

[0056] Although a specific wireless device 201 has just been described, any suitable wireless communication device or terminal may be part of the methods and apparatus which will be described in fuller detail below. Also, although the description of the architecture relates to a specific example for illustration, where the wireless network or WLAN is an IEEE 802.11-based network, different environments may be applicable as well. The wireless network may be a WiMAX-based network (i.e. IEEE 802.16), or an Ultra-WideBand (UWB)-based network (i.e. IEEE 802.15), as a few examples.

[0057] Example Wireless Network Configurations/ Connections. FIG. 5 is an illustrative representation of a part of the communication system 100 of FIG. 1, which illustrates different types of wireless network configurations which may involve wireless device 201. Wireless networks 104 and 122 are WLANs of the traditional "WLAN, infrastructure" type, which typically provide for external network connectivity, as described earlier in relation to FIG. 1. For example, wireless networks 104 and 122 are configured to provide or facilitate access to the Internet 120 (or other communication network, such as a public communication network) for wireless device 201 when connected therewith. In this case, wireless device 201 may make use of its WLAN profiles for connecting with such WLANs.

[0058] Other wireless networking configurations in FIG. 5 include Wi-Fi peer-to-peer (P2P) networking configurations. For these networking configurations, wireless device 201 may operate as a group owner (GO) in relation to various wireless devices. When wireless device 201 is utilized as such, using one or more Wi-Fi P2P network connections, data may be communicated "directly" between wireless device 201 and the other devices (i.e. without the data traversing any fixed wireless network infrastructure).

[0059] In FIG. 5 it is shown that wireless device 201

Samsung Ex. 1004, Page 115 of 563

may establish a Wi-Fi P2P connection with a display device 504 (or monitor) which includes a wireless transceiver 502. Such Wi-Fi P2P network connection may be suitable for applications such as, for example, a streaming media application, or a display or presentation application. It is also shown that wireless device 201 may establish a Wi-Fi P2P network connection with a printer device 508 which includes a wireless transceiver 506. Such Wi-Fi P2P network connection may be suitable for applications such as, for example, a print application or a facsimile application. Even further in FIG. 5, it is shown that wireless device 201 may establish a Wi-Fi P2P network connection with a tablet 514 which includes a wireless transceiver 512. An example tablet was previously shown and described in relation to FIG. 4. Such Wi-Fi P2P network connection may be suitable for an applications such as, for example, a "bridge" or "bridging" application, where wireless device 201 is further configured for cellular telecommunications (e.g. equipped with a cellular transceiver) but tablet 514 is not. In such application, tablet 514 is able to achieve external network (e.g. Internet) connectivity, being connected to wireless device 201 for communications via the cellular telecommunication network. It is further shown in FIG. 5 that wireless device 201 may establish a Wi-Fi P2P network connection in an ad hoc wireless network 550 which includes one or more other wireless devices 520, 522, and 524. Such Wi-Fi P2P network connection may be suitable for applications such as, for example, a file sharing application, a conference meeting application, a game or gaming application, or a military application. Such ad hoc wireless networks may or may not provide external network (e.g. Internet) connectivity.

[0060] As described earlier, wireless device 201 has different types of applications stored therein. These applications may include, as examples, a messaging application, a voice telephony application, a Web browsing application, a streaming media application, a file sharing application, a game application, a printer application, a facsimile application, a display or presentation application, a military application, as examples. Wireless device 201 is optimized to establish the appropriate wireless networks based on which type of application is invoked.

[0061] Referring now to FIG. 6, an illustrative representation of another portion of memory 224 of wireless device 201 is shown. Memory 224 is shown to store a plurality of profiles for wireless networking. The profiles include one or more profiles 602 associated with WLAN infrastructure networks, and/or one or more profiles 604 associated with applications and/or services which utilize Wi-Fi P2P network connections. In FIG. 6, profiles 602 are shown to include profiles 605, 615, and 625, whereas profiles 604 are shown to include profiles 610, 620, and 630. Profiles 602 may be or be referred to as WLAN profiles, whereas profiles 604 may be or be referred to as Wi-Fi P2P networking profiles or Wi-Fi Direct profiles.

[0062] Each one of profiles 602 is associated with a particular WLAN infrastructure network, and includes a plurality of parameters and/or properties for accessing the particular WLAN. The WLAN information may include an identification which identifies the WLAN to access (e.g. a SSID or ESSID). The WLAN information may also include authentication and/or security information for obtaining access to the WLAN (e.g. a network key, passkey, security key, etc.). One of the WLANs appropriate WLAN from profiles 602 will be selected for communication when available, as prioritized in a prioritized list of the profiles 602. When not connected in a WLAN, the wireless device normally operates to search for WLANs identified in its stored profiles 602. Conversely, the wireless device normally refrains from searching for and communicating in WLANs other than those WLANs identified in stored profiles 602.

[0063] On the other hand, each one of profiles 604 is associated with one of the applications and/or services which utilizes a particular type and/or configuration of Wi-Fi P2P network (or Wi-Fi Direct network). Each one of profiles 604 includes parameters and/or properties associated with establishing the particular type and/or configuration of Wi-Fi P2P network for the application and/or service. Profiles 604 may be created, viewed, updated, enabled, and disabled.

[0064] Properties in profiles 604 may include the following. Properties may include a device type property which indicates a device type of the device for the Wi-Fi P2P network connection to be established. The device type may be the device type that is being searched for in the discovery. Note that there may be two device types specified in the profile: a primary device type and a secondary device type. The device types may be or include the appropriate device types in the Wi-Fi Direct Network as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex B thereof). The device types may be or include the predefined values as set forth therein. The device type may be or include category identification (ID) and/or subcategory identification (ID). Examples of such types are as follows: a computer, an input device, a printer, a camera, a display (monitor), a gaming device, an audio device, a multimedia device, or a telephone device.

[0065] Properties may additionally or alternatively include an advertised device type property which indicates the device type of wireless device 201. The advertised device type may be the device type to be advertised by wireless device 201. Note that there may be two advertised device types specified in the profile: a primary advertised device type, and a secondary advertised device type. The advertised device types may be or include the appropriate device types in the Wi-Fi Direct Network as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex B thereof). The device types may be or include the predefined values as set forth therein. The advertised device type may be or include category identification (ID) and/or subcategory identification (ID). Examples of such types are as follows: a computer, an input device, a printer, a camera, a display

Samsung Ex. 1004, Page 116 of 563

(monitor), a gaming device, an audio device, a multimedia device, or a telephone device.

[0066] Properties in profiles 604 may additionally or alternatively include a service type property which indicates a service type which identifies the service associated with the device. For example, the service types may be or include the appropriate service types as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex E thereof). Examples of such types are as follows: a file sharing service, or a printing service. Alternatively, examples of such types are as follows: Apple File Sharing (AFP) service (or AFP over TCP service), or IP Printing (IPP) Bonjour service.

[0067] Properties in profiles 604 may additionally or alternatively include a discovery mode property which indicates a mode utilized for the discovery of devices for the Wi-Fi P2P network connection. The discovery mode property may be set to one of the following: a triggered mode of discovery, or a periodic mode of discovery. Alternatively, the discovery mode may be set to one of the following: a triggered mode of discovery, a periodic mode of discovery, or a Group Owner (GO) mode of discovery.

[0068] Properties in profiles 604 may additionally or alternatively include a persistent property or indication which indicates whether or not the Wi-Fi P2P network is persistent. If the network is persistent, when an application is opened or activated, the wireless device connects to a previously-established Wi-Fi P2P network.

[0069] Properties in profiles 604 may additionally or alternatively include a coexistence indication or property which indicates whether the Wi-Fi P2P network connection associated with this profile may be maintained while the wireless device operates as a client in an infrastructure network. Properties may additionally or alternatively include another coexistence indication or property which indicates whether the Wi-Fi P2P network connection associated with this profile may be maintained while maintaining another Wi-Fi P2P network connection.

[0070] More On Use Cases; Additional/Alternative Profile Details. It is noted that many peer-to-peer "use cases" for Wi-Fi P2P networking lend themselves to different modes of operation. For example, if a wireless device supports a network gateway feature (e.g. a mobile hotspot or MHO feature), then the wireless device may be configured to establish a persistent Wi-Fi P2P network when the service is enabled. As another example, the same wireless device may require a printer service to allow an application to print a document. In this case, the Wi-Fi P2P network may be established on-demand based on an application trigger. In another example, a social networking application may periodically search for other communication devices running the same social networking application, which may result in the wireless device operating in a periodic discovery mode for other devices which advertise the same service.

[0071] To accommodate for such various use cases, profiles associated with the various application/services utilizing Wi-Fi P2P networks are created and stored on the wireless device. These profiles are enabled when needed, such as enabled in response to an activation of an application associated therewith. Further, the profiles may be enabled concurrently.

[0072] In one embodiment, the profiles may have data structures defined for compatibility with the Wi-Fi Peer-To-Peer (P2P) Technical specification. Each profile may include information specific to Wi-Fi P2P network operation, including device discovery behavior, service discovery options, co-existence with infrastructure connectivity, as well as operational characteristics of the network (e.g. whether it is persistent, or triggered on application launch). These profiles may be provisioned as defaults in the wireless device, and/or may be configured by applications when installed.

[0073] The profiles are used to manage the behavior of the WLAN or Wi-Fi driver of the wireless device to accommodate for the various application/services. The driver may be configured to support each particular use case. More particularly, the driver may use the profile information to manage peer-to-peer communications on the wireless device, as well as to arbitrate between Wi-Fi P2P network and other modes of connectivity (e.g. infrastructure STA mode). The driver may be further configured to support other application requirements, such as sleep modes, discovery modes, and/or co-existence with an infrastructure network connection over WLAN, etc. An example set of properties and/or parameters relating to the behavioral characteristics were provided earlier above.

[0074] FIG. 7 illustrates that wireless device 201 may be configured to communicate concurrently with two different wireless networks. In this example, wireless device 201 may be particularly configured as a "P2P concurrent device" in accordance with the protocols in the Wi-Fi Peer-To-Peer (P2P) Technical specification. Here, wireless device 201 has a first MAC entity 702 operating as a client station in a WLAN (i.e. a "WLAN-STA") (e.g. with AP 116 of the WLAN) and a second MAC entity 704 operating as a peer-to-peer device (e.g. with P2P device 195 and P2P device 197). Dual MAC functionality may be implemented as, for example, two virtual MAC entities over one physical layer (PHY) entity. Thus, wireless device 201 may operate to concurrently maintain two different types of wireless connections, via the same wireless transceiver or PHY entity.

[0075] Referring now ahead to FIG. 9, what is shown a flowchart for describing a method for use in communicating in a P2P network. The method of FIG. 9 may be performed by wireless device 201 described in relation to FIGs. 1-8 above. In such technique, the wireless device may operate substantially in accordance or compatible with the Wi-Fi P2P network protocols in the Wi-Fi Peer-To-Peer (P2P) Technical specification.

[0076] The techniques described in relation to the flowchart of FIG. 9 may be performed by one or more controllers or processors of the wireless device along with its wireless or RF transceiver(s). A computer program

Samsung Ex. 1004, Page 117 of 563

product which may embody the technique may include a computer readable medium (e.g. memory of the communication device, computer disk, CD-ROM, etc.) having computer instructions stored therein which are executable by the one or more processors of the wireless device for performing the technique.

[0077] Beginning at a start block 902 of FIG. 9, a wireless device operates to establish a P2P network with other P2P devices (step 904 of FIG. 9). Here, the wireless device operates in an access point "AP" mode of operation, so that P2P devices may associate with it for direct RF communications. Data may be communicated directly between the P2P devices without the data traversing any fixed wireless network infrastructure. For this purpose, the wireless device may operate as a group owner (GO) in the P2P network. For example, the wireless device may operate as a GO (substantially) in accordance with or compatible with the Wi-Fi Peer-To-Peer (P2P) Technical specification.

[0078] In addition, the wireless device may perform concurrent operations as a client station with another AP (see e.g. the discussion in relation to FIG. 7). In order to communicate with this other AP as a client station, the wireless device must temporarily cease communications with the P2P devices. Further, in order to ensure that the P2P devices will not attempt to communicate with the wireless device while it communicates with the other AP, the wireless device communicates the times during which it will be absent or unavailable for communications with the P2P devices. This operation will be described in more detail below.

[0079] Next, the wireless device identifies the type of communications which are established (or to be established) with each one of the P2P devices (step 906 of FIG. 9). There may be a plurality of different types of communications established between the P2P devices and the group owner. For example, the type of communications may be defined by (at least in part) a (minimum) bandwidth requirement for the communications.

[0080] In some embodiments, the type of communications may be identified by a traffic class or Quality of Service (QoS) criteria associated with the communications.

[0081] Note that a traffic class may be a conversational or voice traffic class, a streaming traffic class, an interactive traffic class, or a background traffic class. A conversational or voice traffic class is associated with traditional voice communications, which are usually two-way and sensitive to delay, delay variation, and data loss. A streaming traffic class is typically associated with one-way communications which are less sensitive to delay and data loss, but are sensitive to delay variations and typically require a high bandwidth. An example of streaming traffic class is a video player application. On the other hand, an interactive traffic class is typically associated with two-way "busty" types of communications. These communications can tolerate moderate delay and data loss and have variable bandwidth requirements. On-line video game and web-surfing (browser) applications are examples of the interactive traffic class. Finally, a background traffic class is typically associated with communications which are highly tolerant of delay and data loss and may have variable bandwidth requirements. Examples of these applications include e-mail and file transfer applications.

[0082] The wireless device assigns or groups the P2P devices into different multicast groups (step 908 of FIG. 9). In some embodiments, the wireless device assigns or groups the P2P device into different multicast groups based on the identifying in step 906. More particularly, the wireless device assigns or groups one or more P2P devices having the same (or substantially the same) type of communications into the same multicast group. Thus, each multicast group is associated with the same (or substantially the same) type of communications, but with a different type of communications from all other multicast groups.

[0083] In some embodiments, each multicast group may simply include one or more P2P devices determined to have a bandwidth requirement within a predetermined range. In some other embodiments, each multicast group may include one or more P2P devices having communications with the same traffic class or QoS criteria. For example, the wireless device may group one or more first P2P devices having communications associated with a voice traffic class into a first multicast group, and one or more second P2P devices having communications associated with a streaming traffic class into a second multicast group.

[0084] In the technique, a multicast address is assigned to each one of the multicast groups. The assignment and communication of the multicast address may be done in any suitable manner. In some embodiments, a multicast address may be determined and communicated by the group owner when each P2P device joins the group (e.g. the assignment may be communicated in an association frame). In some other embodiments, the multicast address may be negotiated between P2P devices using a new Public Action frame (e.g. a newly-defined frame named "NoAGroupRequest/Response" frame). In yet other embodiments, a multicast address may be determined and communicated as part of an application or service, where the application or service includes information indicating the traffic class or QoS criteria. Here, there may be a multicast group assigned to each application type (e.g. printing, video streaming, VoIP, etc.).

[0085] The wireless device then calculates (or otherwise determines or selects) different Notice of Absence (NoA) data for each multicast group (step 901 of FIG. 9). Each NoA data includes at least a time period of absence for communicating with the P2P devices of the multicast group. If communications are necessary, the wireless device will communicate with the P2P devices outside of the time period of absence from the first NoA data.

[0086] In some embodiments, the NoA data may be or

Samsung Ex. 1004, Page 118 of 563

include a NoA attribute. The NoA attribute may be defined in the Wi-Fi Peer-To-Peer (P2P) Technical specification, for example. Here, the NoA attribute includes a start time, an interval, a duration, and a count. In some embodiments, the durations of absence for each multicast group are set to be different, but the start times, the intervals, and the counts are set to be the same for each multicast group. In some other embodiments, the counts may be set to be different for each multicast group.

[0087] The duration of absence for each multicast group may be determined based on the (minimum) bandwidth requirement for the multicast group. More particularly, the duration of absence for a multicast group may be calculated to be inversely related to the bandwidth requirement for the multicast group. For example, the multicast group with the largest bandwidth requirement may be calculated to have the smallest duration of absence. The counts may similarly be varied.

[0088] The wireless device then produces and sends a multicast message with the NoA data associated with a multicast group (step 912 of FIG. 9). In order to communicate with all of the P2P devices in the multicast group, the multicast message includes the multicast address associated with the group (see e.g. FIG. 8). If there are one or more additional multicast groups to be processed as identified at step 914 of FIG. 9, the wireless device will produce and send a multicast message with the NoA data associated with this additional multicast group, repeating step 912.

[0089] Multicast addressing is now discussed with reference back to FIG. 8, which is an illustration of a format of a message including an address field 800 which may be populated with an address for multicast messaging. The address may be referred to as a MAC address or a layer-2 address. MAC is used for access to the physical layer from the data link layer according to the ISO/OSI model. Address field 800 may include an indication which indicates whether the address is a unicast address or a multicast address. The indication may be a bit indication in address field 800 (e.g. the least significant bit of the most significant octet of the address). If the least significant bit of the most significant octet of the address is set to zero ("0"), the frame is intended to reach only a single receiving device. This type of communication or addressing may be referred to as unicast communication or addressing. Here, a unicast frame is transmitted to all nodes within the collision domain, which typically ends at the nearest network switch or router. Only the node with the matching hardware MAC address will accept the frame, and network frames with non-matching MAC addresses are ignored. On the other hand, if the least significant bit of the most significant octet of the address is set to one ("I"), the frame will still be sent only once; however, devices may accept the frame based on different criteria than a matching MAC address. For example, devices may accept the frame based on a configurable list of accepted multicast MAC addresses. This type of communication or addressing may be referred to as multicast communication or addressing.

[0090] In some embodiments, wireless device may send such messages in a beacon frame in step 912 of FIG. 9. In IEEE 802.11, a typical beacon frame is approximately fifty bytes long, with about half of that being a common frame header and cyclic redundancy checking (CRC) field for error detection capability. The beacon frame body resides between the header and the CRC field and constitutes the other half of the beacon frame. As with other frames, the header includes source and destination MAC addresses as well as other information regarding the communications process. For traditional broadcasts, the destination address is set to all ones, which is the broadcast MAC address. This causes all stations on the channel to receive and process each beacon frame. Using multicast groups per the present disclosure, the destination address is set to a multicast address associated with the specific multicast group.

[0091] In some embodiments, a plurality of multicast groups may be communicated in a single beacon. This may be done, for example, by communicating with use of an existing or newly-defined IEEE 802.11 element. The newly-defined IEEE 802.11 element may have the following format, for example:

* Element ID: TBD value - an integer assigned by IEEE or a vendor specific element
* Length: 3-255 octets
* Number of NoA Groups: variable - the number of NoA Groups
* Group 1: NoA Address - 6 octet group (multicast) address; NoA Schedule element (as per Wi-Fi P2P Specification)
* Group 2: ...
* Group N

In other embodiments, the wireless device may send a group (multicast) management frame which includes the NoA data for a specific multicast group.

[0092] Continuing with FIG. 9, if there is a new message to be processed (step 916 of FIG. 9), then the wireless device repeats steps 912 and 914 for again producing and sending the messages. If a new P2P device has entered in the P2P network (step 918 of FIG. 9), the wireless device repeats the technique at step 906 (i.e. to identify the type of communications for any new P2P device), step 908 (i.e. to group the P2P devices into different multicast groups), step 910 (i.e. to calculate or adjust the NoA data for each multicast group), etc. Otherwise, the technique repeats step 916. Note that step 918 may additionally or alternatively include identifying whether an existing P2P device has left the P2P network, whether the type of communications for an existing P2P device has changed to a different type of communications, or some or all of the above.

[0093] FIG. 10 is a timing diagram 1000 of communications involving the wireless device 201 operating as a group owner (GO) in a P2P network, scheduling absenc-

Samsung Ex. 1004, Page 119 of 563

es in the P2P network by communicating NoA data in a broadcast message, without use of the technique of FIG. 9. A time line 1020 depicts communications for the wireless device 201 which is the group owner, a time line 1022 depicts communications for P2P device 195, and a time line 1024 depicts communications for P2P device 197. P2P device 195 is operating in active mode, whereas P2P device 197 is operating in power saving (PS) mode. For wireless device 201, time line 1020 illustrates the absence period (e.g. an absence period 1002), data or communication periods (e.g. a data or communication period 1003), the intervals, the durations, and the counts. In the active state, P2P device 195 places itself in a doze state during a doze period 1004 corresponding to each absence period 1002, and exits the doze state and communicates (if necessary) in each data period 1006 which follows the doze period 1004. In the PS mode, P2P device 197 places itself in a doze state during a doze period 1008 which spans across multiple absence periods of the wireless device 201.

[0094] FIG. 11 is another timing diagram 1100 of communications involving the wireless device operating as a group owner in a P2P network, scheduling absences in the P2P network by communicating different NoA data to different multicast groups, using the technique of FIG. 9 and the present disclosure. Relatedly, FIG. 12 is a close-up of a portion of the timing diagram 1100 of FIG. 11, showing the differences in doze periods of the different multicast groups, which is based on the different NoA data. The timing diagram 1100 shows the absence periods (e.g. an absence period 1102), data or communication periods (e.g. a data or communication period 1104), the intervals, the durations, and the counts.

[0095] In the present embodiment, P2P device 195 is in a first multicast group and P2P device 197 is in a second multicast group. In the timing diagram 110, both P2P devices 195 and 197 are operating in the active mode. P2P device 195 of the first multicast group places itself in a doze state during a doze period 1106 corresponding to each absence period 1102, and exits the doze state and communicates (if necessary) in each data period 1108 which follows the doze period 1106. On the other hand, P2P device 197 of the second multicast group places itself in a doze state during a doze period 1110 and exits the doze state and communicates (if necessary) in each data period 1112 which follows the doze period 1110.

[0096] As mentioned, the wireless device 201 operating as the group owner sends different NoA data to the first and the second multicast groups. In particular, the first multicast group which includes P2P device 195 receives a first absence period from the wireless device 201, and the second multicast group which includes P2P device 197 receives a second absence period from the wireless device 201 that is greater than the first absence period received by the first multicast group.

[0097] In this example, the first multicast group may be of the voice or conversational traffic class and/or or have a relatively low minimum bandwidth requirement, whereas the second multicast group may be of the streaming traffic class and/or have a relatively high minimum bandwidth requirement.

[0098] Thus, as described herein, a wireless device is configured to operate as a group owner (GO) in a peer-to-peer (P2P) network. The wireless device sends a first multicast message to one or more first P2P devices in the P2P network. The first multicast message includes first notice of absence (NoA) data. The wireless device also sends a second multicast message to one or more second P2P devices in the P2P network. The second multicast message includes second notice of absence (NoA) data. Partitioning in the P2P network in this fashion may be set based on the different types of communications established for the P2P devices (e.g. the different traffic classes or Quality of Service (QoS) types).

[0099] In addition, other techniques for a wireless peer-to-peer (P2P) device which is configured to communicate in a P2P network having a group owner (GO) are described. In one illustrative example, a technique involves the actions of receiving from the group owner a multicast message which includes notice of absence (NoA) data. The NoA data includes a time period of absence from the P2P network. The wireless P2P device may communicate with the group owner outside of the time period of absence indicated in the NoA data of the multicast message. On the other hand, the wireless P2P device refrains from communicating with the group owner during the time period of absence in the NoA data of the multicast message. The time period of absence with the group owner may be based on the type of communications established with the wireless P2P device (i.e. the traffic class or Quality of Service (QoS) type).

[0100] The above-described embodiments of the present disclosure are intended to be examples only. Those of skill in the art may affect alterations, modifications and variations to the particular embodiments without departing from the scope of the application. Although the description relates to specific examples for illustration, where the WLAN is an IEEE 802.11-based network, for example, different environments may be applicable as well. As a few other examples, the wireless networking may be based on a WiMAX network (i.e. IEEE 802.16), or an Ultra-WideBand (UWB) network (i.e. IEEE 802.15). The invention described herein in the recited claims intends to cover and embrace all suitable changes in technology.

Claims

1. A method in a wireless device which is configured to operate as a group owner (GO) in a peer-to-peer (P2P) network, the method comprising:

   sending a first multicast message to one or more first P2P devices in the P2P network, the first

Samsung Ex. 1004, Page 120 of 563

multicast message including first notice of absence (NoA) data; and
sending a second multicast message to one or more second P2P devices in the P2P network, the second multicast message including second NoA data.

2. The method of claim 1, wherein the first NoA data includes a first time period of absence for communicating with the first P2P devices, and the second NoA data includes a second time period of absence for communicating with the second P2P devices, the method further comprising:

identifying that the one or more first P2P devices are associated with a first type of communications;
identifying that the one or more second P2P devices are associated with a second type of communications; and
calculating the first and the second time periods of absences based on the first and the second types of communications.

3. The method of claim 1, wherein communications of the one or more first P2P devices are associated with a first traffic class or first Quality of Service (QoS) criteria, and communications of the one or more second P2P devices are associated with a second traffic class or second first QoS criteria.

4. The method of claim 3, further comprising:

identifying that the communications of the one or more first P2P devices are associated with the first traffic class or the first QoS criteria; and identifying that the communications of the one or more second P2P devices are associated with the second traffic class or the second QoS criteria.

5. The method of claim 4, further comprising:

calculating the first NoA data for the one or more first P2P devices in response to identifying their association with the first traffic class or the first QoS criteria; and
calculating the second NoA data for the one or more second P2P devices in response to identifying their association with the second traffic class or second QoS criteria.

6. The method of claim 1, wherein at least the first multicast message is included in a beacon frame.

7. The method of claim 1, wherein the first NoA data is indicative of a first period of absence for communicating with the first P2P devices, and the second NoA data is indicative of a second period of absence for communicating with the second P2P devices, the method further comprising:

communicating with the one or more first P2P devices outside of the first period of absence indicated in the first NoA data; and
communicating with the one or more second P2P devices outside of the second period of absence indicated in the first NoA data.

8. The method of claim 6, wherein the first NoA data comprises a first NoA attribute which includes a first start time, a first interval, a first duration, and a first count field, and wherein the second NoA data comprises a second NoA attribute which includes a second start time, a second interval, a second duration, and a second count field.

9. A wireless communication device, comprising:

one or more processors;
a radio frequency (RF) transceiver (RF) coupled to the one or more processors; and
the one or more processors being configured to operate the wireless communication device as a group owner (GO) in a peer-to-peer (P2P) network by performing the method of any one of claims 1-8.

10. A method in a wireless peer-to-peer (P2P) device which is configured to communicate in a P2P network having a group owner (GO), the method comprising:

receiving from the group owner a multicast message which includes notice of absence (NoA) data, the NoA data including a time period of absence from the P2P network; and
refraining from communicating with the group owner during the time period of absence indicated in the NoA data of the multicast message.

11. The method of claim 10, further comprising:

entering into a doze state during the time period of absence indicated in the NoA data of the multicast message.

12. The method of claim 10, further comprising:

communicating with the group owner outside of the time period of absence indicated in the NoA data of the multicast message.

13. The method of claim 10, further comprising:

wherein the time period of absence is set in ac-

Samsung Ex. 1004, Page 121 of 563

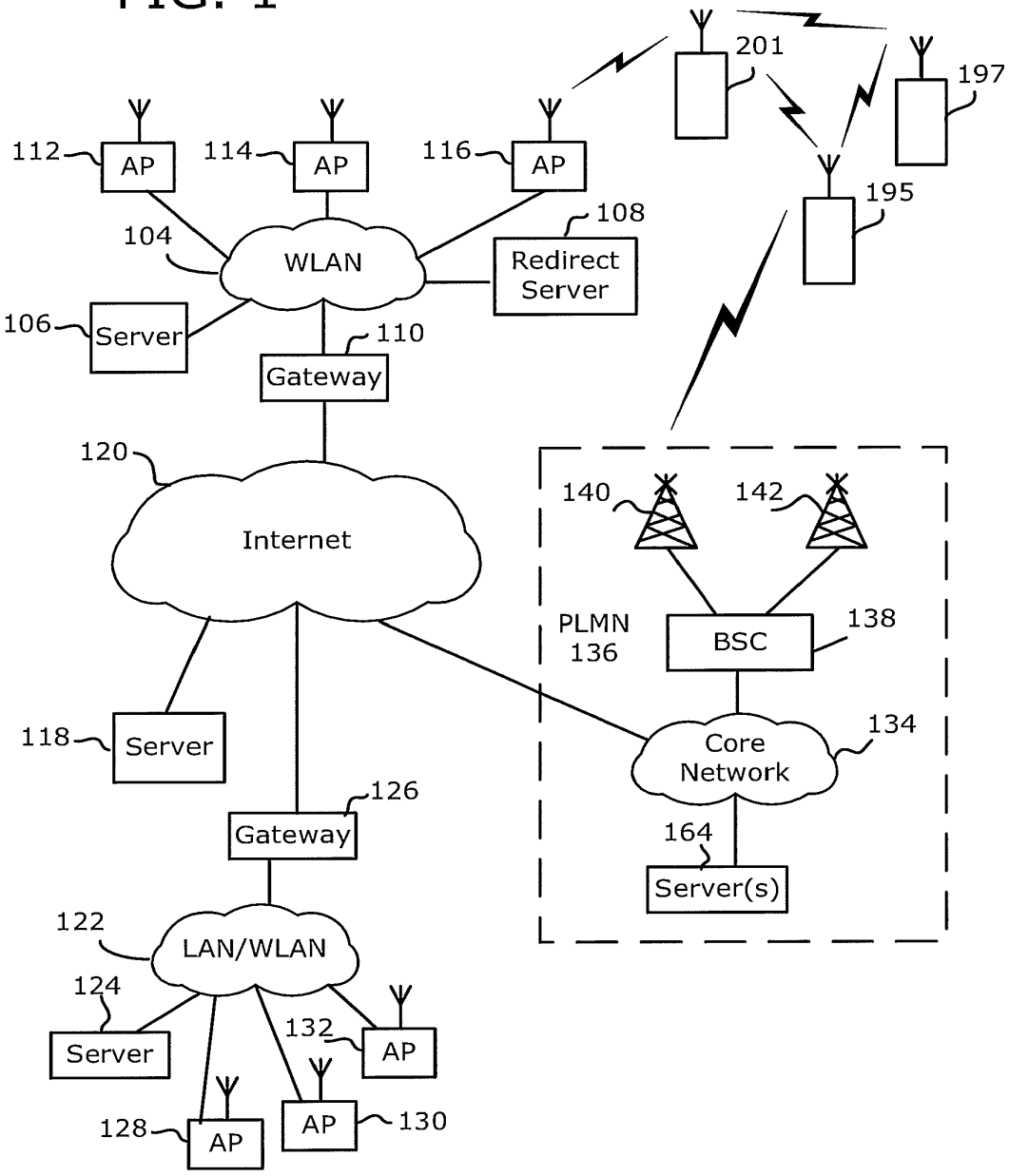
cordance with a type of communications established with the P2P device; or
wherein the time period of absence is set in accordance with a traffic class or Quality of Service (QoS) criteria of communications of the P2P device; or
wherein the time period of absence is inversely related to a bandwidth requirement of communications of the P2P device via the group owner.

14. A wireless communication device, comprising:

one or more processors;
a radio frequency (RF) transceiver coupled to the one or more processors; and
the one or more processors being operative to communicate in a peer-to-peer (P2P) network having a group owner (GO) by being configured to perform the method of any one of claims 10-13.

Samsung Ex. 1004, Page 122 of 563

FIG. 1


201
197
195
112
AP
114
AP
116
AP
104
WLAN
108
Redirect Server
106
Server
110
Gateway
120
Internet
140
142
PLMN 136
BSC
138
118
Server
134
Core Network
126
Gateway
164
Server(s)
122
LAN/WLAN
124
Server
132
AP
128
AP
AP
130
100

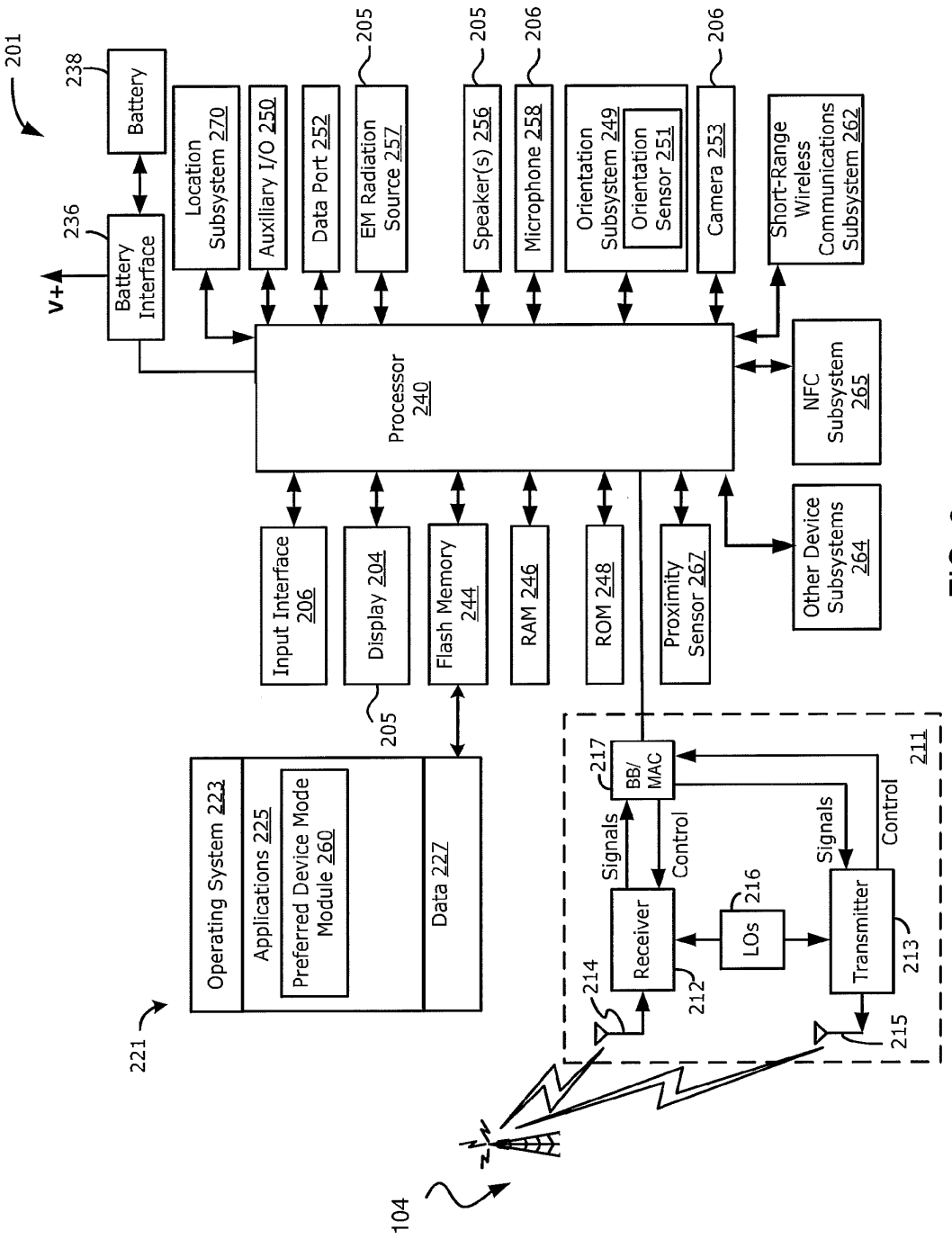

201
238
Battery
236
Battery Interface
V+
Location Subsystem 270
Auxiliary I/O 250
Data Port 252
205
EM Radiation Source 257
205
Speaker(s) 256
206
Microphone 258
Orientation Subsystem 249
Orientation Sensor 251
206
Camera 253
Short-Range Wireless Communications Subsystem 262
Processor 240
NFC Subsystem 265
Other Device Subsystems 264
Input Interface 206
Display 204
Flash Memory 244
RAM 246
ROM 248
Proximity Sensor 267
205
Operating System 223
Applications 225
Preferred Device Mode Module 260
Data 227
221
217
BB/ MAC
211
Signals
Control
Receiver
212
214
LOs
216
Signals
Control
Transmitter
213
215
104

FIG. 2

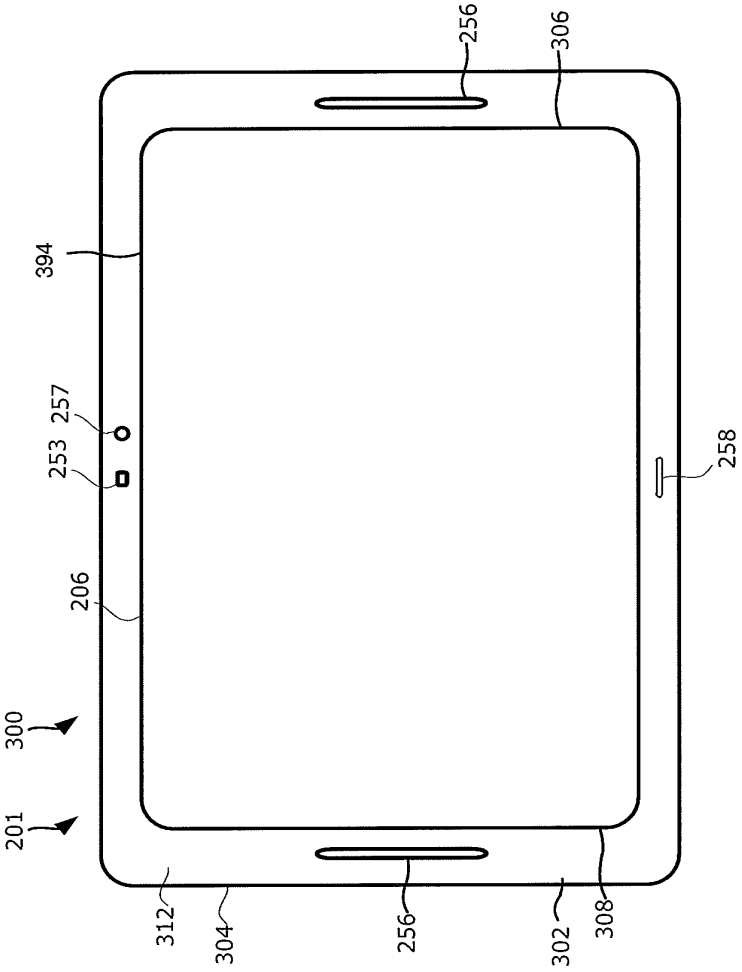

256
306
394
257
253
258
206
300
201
312
304
256
302
308

FIG. 4

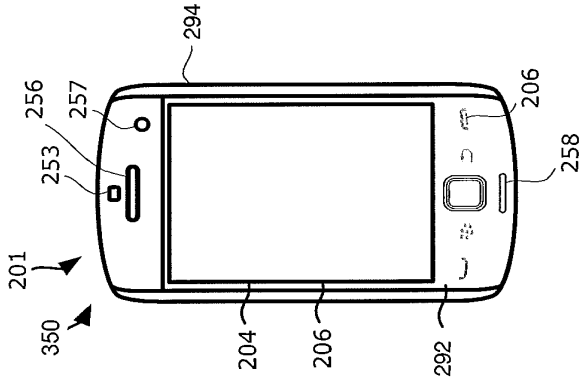

294
256
257
206
253
258
201
350
204
206
292

FIG. 3

FIG. 5

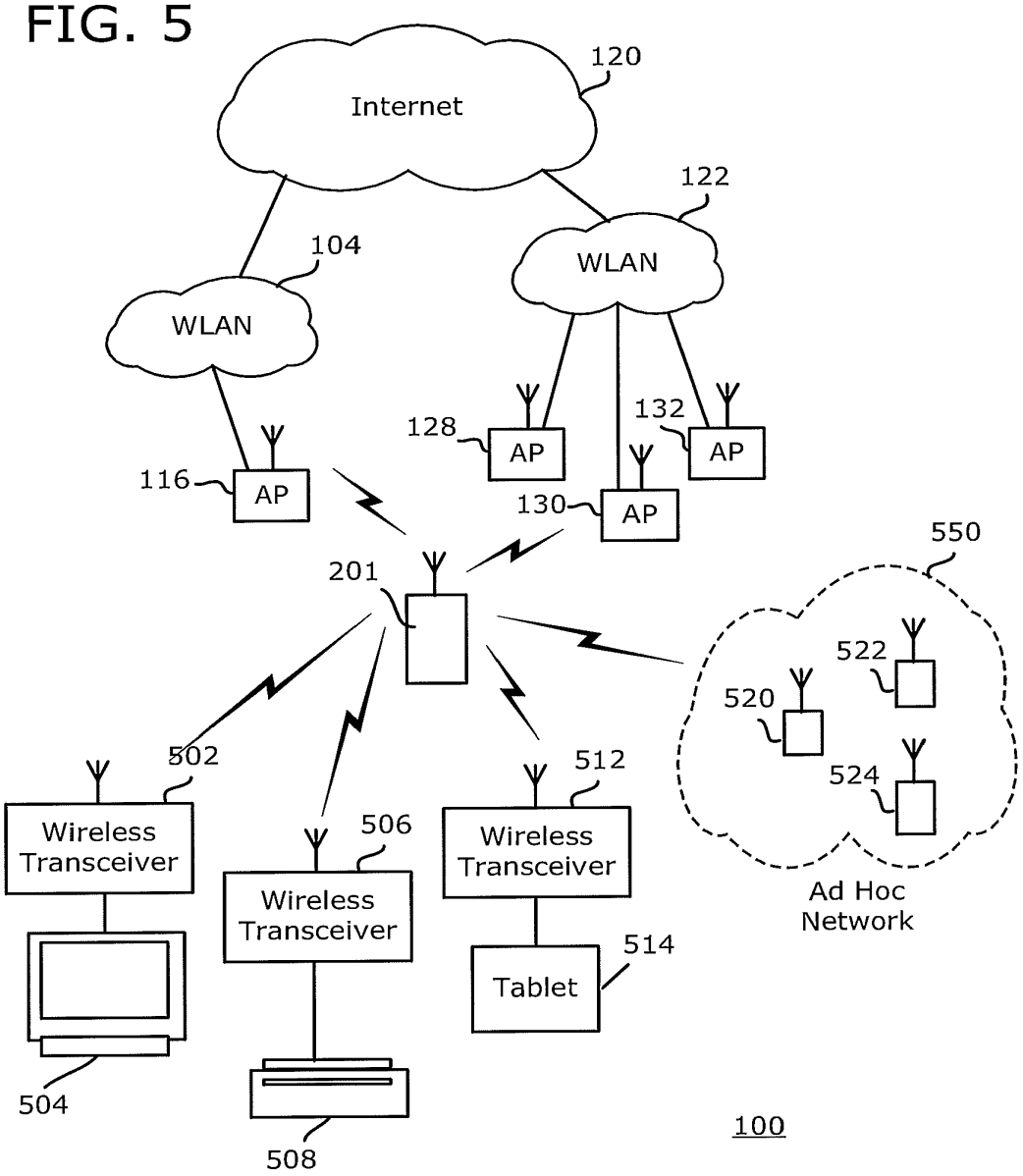

Internet
120
122
WLAN
104
WLAN
128
AP
132
AP
116
AP
130
AP
550
201
522
520
524
Ad Hoc
Network
502
512
506
Wireless
Transceiver
Wireless
Transceiver
Wireless
Transceiver
514
Tablet
504
508
100

FIG. 6

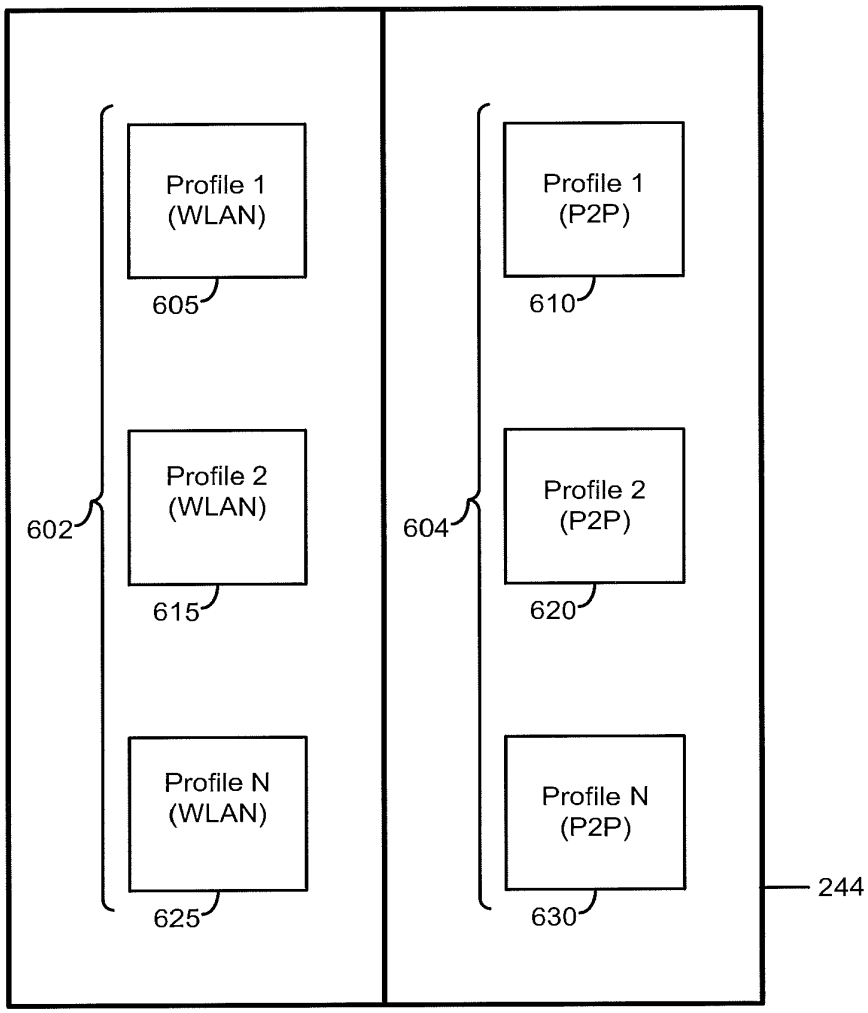
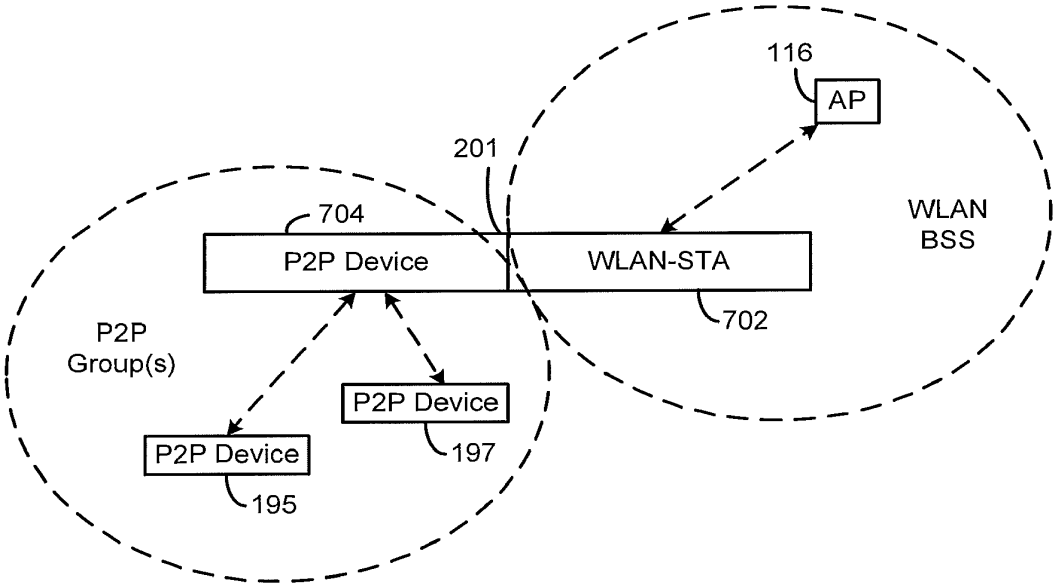

Profile 1 (WLAN)
605
Profile 2 (WLAN)
615
Profile N (WLAN)
625
602
Profile 1 (P2P)
610
Profile 2 (P2P)
620
Profile N (P2P)
630
604
244

FIG. 7


116
AP
201
704
P2P Device
WLAN-STA
WLAN
BSS
702
P2P
Group(s)
P2P Device
197
P2P Device
195

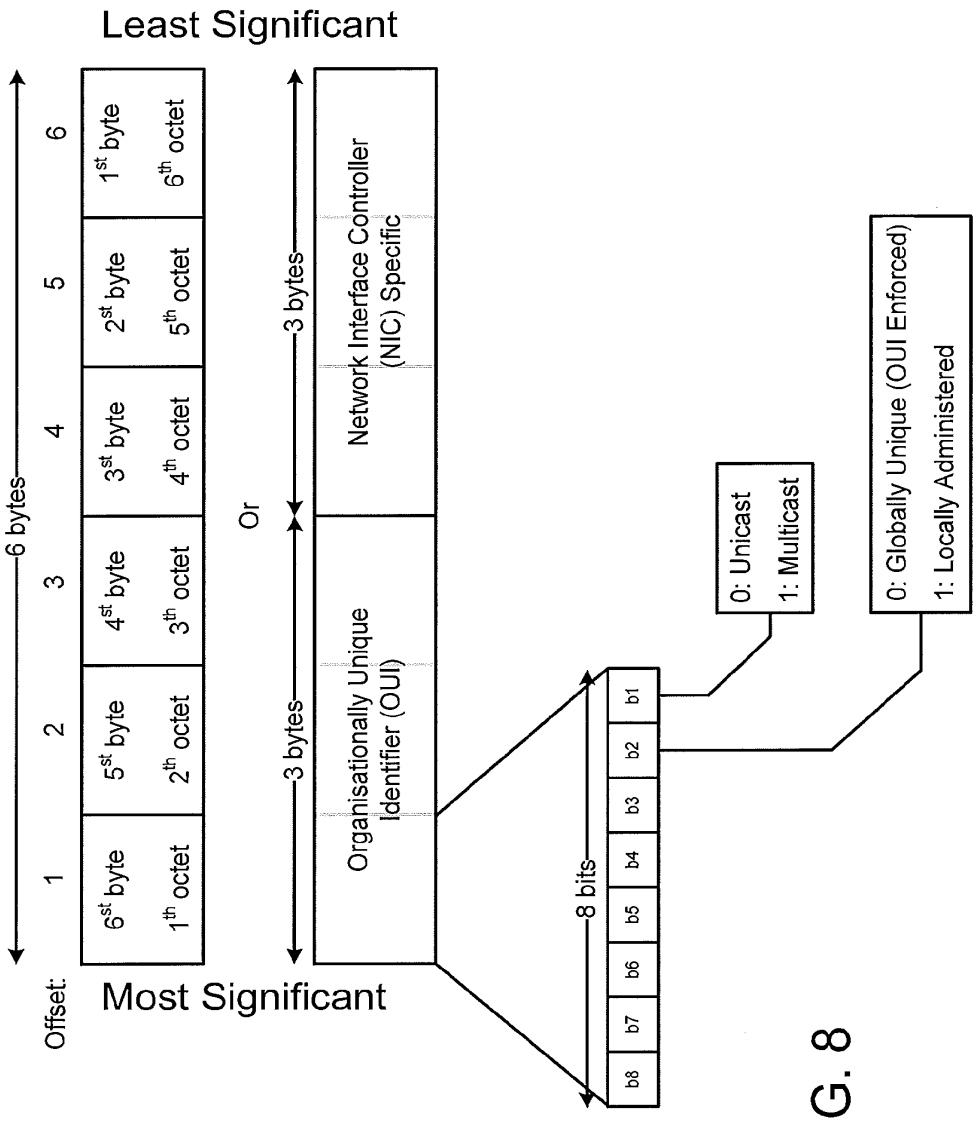
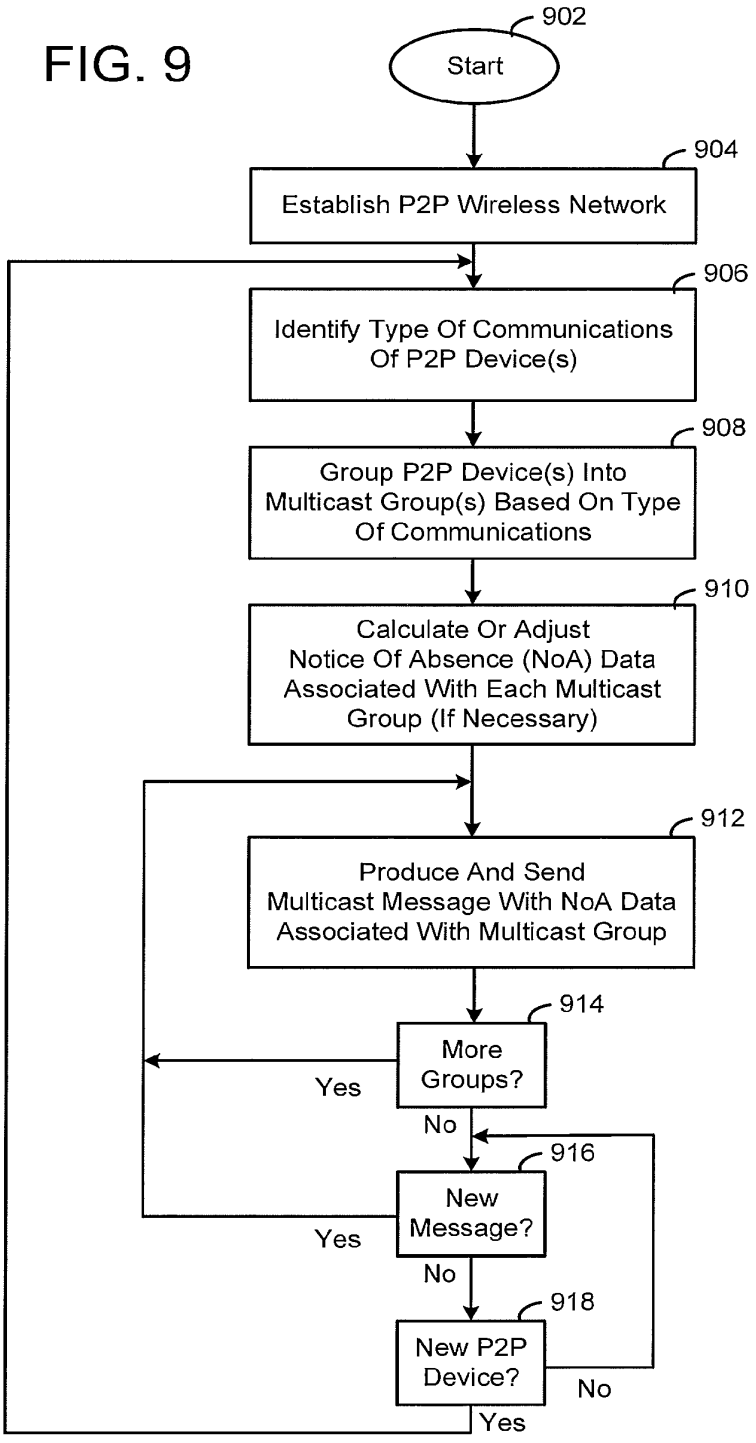

Least Significant
Most Significant
Offset:
1
2
3
4
5
6
6 bytes
6st byte
1th octet
5st byte
2th octet
4st byte
3th octet
3st byte
4th octet
2st byte
5th octet
1st byte
6th octet
Or
3 bytes
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b1
b2
b3
b4
b5
b6
b7
b8
0: Unicast
1: Multicast
0: Globally Unique (OUI Enforced)
1: Locally Administered
800

FIG. 8

FIG. 9


902
Start
904
Establish P2P Wireless Network
906
Identify Type Of Communications Of P2P Device(s)
908
Group P2P Device(s) Into Multicast Group(s) Based On Type Of Communications
910
Calculate Or Adjust Notice Of Absence (NoA) Data Associated With Each Multicast Group (If Necessary)
912
Produce And Send Multicast Message With NoA Data Associated With Multicast Group
914
More Groups?
Yes
No
916
New Message?
Yes
No
918
New P2P Device?
No
Yes

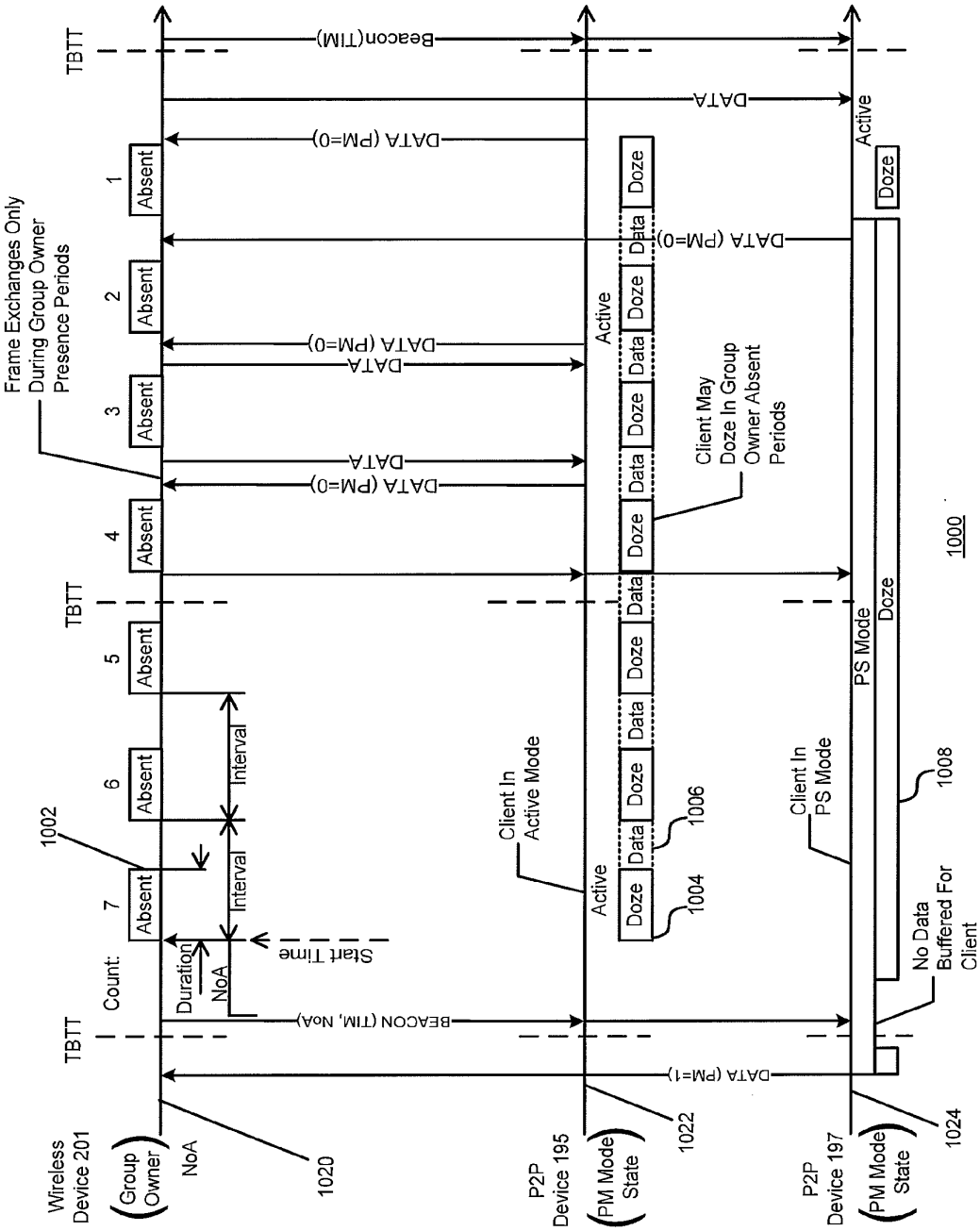

Wireless Device 201
(Group Owner)
NoA
1020
P2P Device 195
(PM Mode State)
1022
P2P Device 197
(PM Mode State)
1024
TBTT
Count:
Duration
NoA
Start Time
Interval
Interval
1002
Beacon(TIM)
BEACON (TIM, NoA)
DATA (PM=1)
DATA
DATA (PM=0)
Absent
Frame Exchanges Only During Group Owner Presence Periods
Active
Doze
Data
Client May Doze In Group Owner Absent Periods
Client In Active Mode
Client In PS Mode
PS Mode
No Data Buffered For Client
1004
1006
1008
1000

FIG. 10

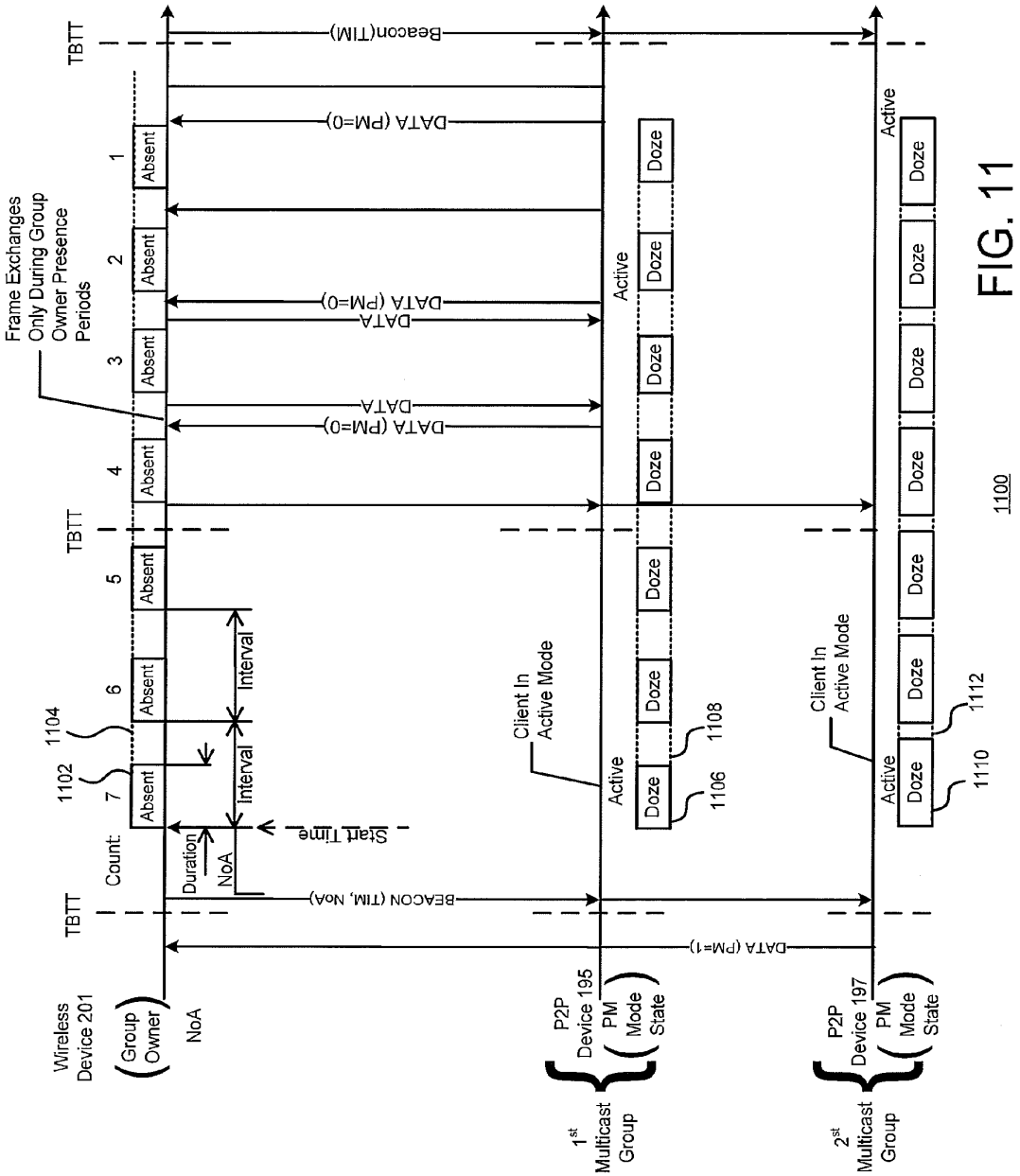
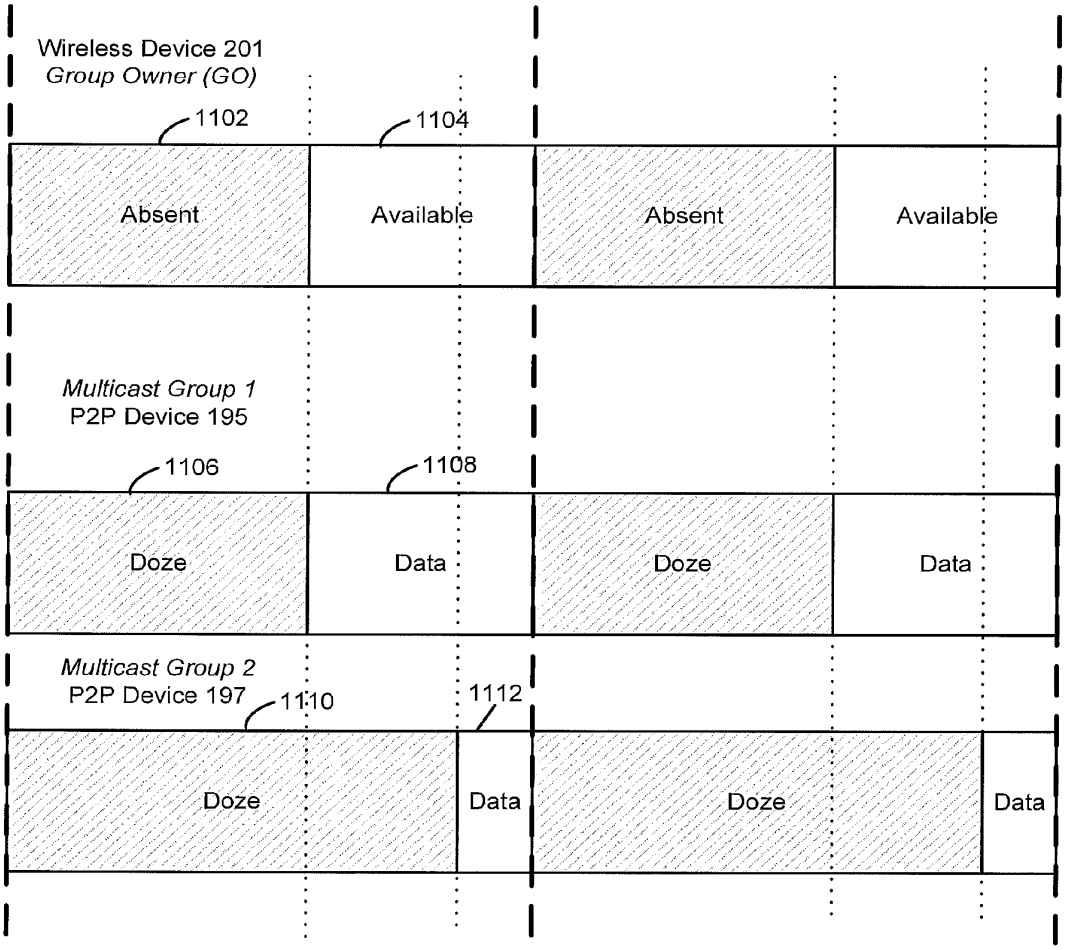

Wireless Device 201
(Group Owner)
NoA
P2P Device 195
PM Mode State
1st Multicast Group
P2P Device 197
PM Mode State
2nd Multicast Group
Frame Exchanges Only During Group Owner Presence Periods
TBTT
Beacon(TIM)
DATA (PM=0)
DATA
Absent
Doze
Active
Client In Active Mode
Count:
Duration
NoA
Interval
Start Time
BEACON (TIM, NoA)
DATA (PM=1)
1100
1102
1104
1106
1108
1110
1112

FIG. 11

FIG. 12


Wireless Device 201
Group Owner (GO)
1102
1104
Absent
Available
Absent
Available
Multicast Group 1
P2P Device 195
1106
1108
Doze
Data
Doze
Data
Multicast Group 2
P2P Device 197
1110
1112
Doze
Data
Doze
Data
1200

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 12 18 6237

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WI-FI ALLIANCE: "Wi-Fi Peer-to-Peer (P2P) Specification v1.1", WI-FI ALLIANCE SPECIFICATION,, 1 January 2010 (2010-01-01), pages 1-159, XP009163866,	10-12,14	INV. H04W76/00
Y	* sections 3.2.6, 3.3.3.2 *	1-9,13	
Y	US 2006/268873 A1 (TONJES RALF [DE] ET AL TOENJES RALF [DE] ET AL) 30 November 2006 (2006-11-30) * paragraphs [0011], [0035] - [0040], [0059] *	1-9,13	
A	Wi-Fi Alliance: "Wi-Fi CERTIFIED Wi-Fi Direct", , 1 October 2010 (2010-10-01), pages 1-14, XP055041124, Retrieved from the Internet: URL:http://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-direct%E2%84%A2-personal-portable-wi-fi%C2%AE-connect-devices [retrieved on 2012-10-16] * tables 1, 2 *	1-14	TECHNICAL FIELDS SEARCHED (IPC) H04W
A	WO 2011/046703 A2 (INTEL CORP [US]; YUAN HAO [CN]) 21 April 2011 (2011-04-21) * the whole document *	1-14	
A	US 2012/106381 A1 (VEDANTHAM RAMANUJA [US] ET AL) 3 May 2012 (2012-05-03) * the whole document *	1-14	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 February 2013	Saffell, Christine

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

3

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 18 6237

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-02-2013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006268873 A1	30-11-2006	AT 403994 T	15-08-2008
		AU 2002352185 A1	23-06-2004
		EP 1566013 A1	24-08-2005
		US 2006268873 A1	30-11-2006
		WO 2004051926 A1	17-06-2004
WO 2011046703 A2	21-04-2011	CN 102045842 A	04-05-2011
		EP 2489238 A2	22-08-2012
		US 2011090877 A1	21-04-2011
		WO 2011046703 A2	21-04-2011
US 2012106381 A1	03-05-2012	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Samsung Ex. 1004, Page 135 of 563

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 055 072 B1

(12) EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
17.04.2013 Patentblatt 2013/16

(21) Anmeldenummer: **07765292.3**

(22) Anmeldetag: **30.05.2007**

(51) Int Cl.:
H04L 29/12 *(2006.01)* ***H04W 8/26*** *(2009.01)*
H04W 84/18 *(2009.01)*

(86) Internationale Anmeldenummer:
PCT/EP2007/055231

(87) Internationale Veröffentlichungsnummer:
WO 2008/022821 (28.02.2008 Gazette 2008/09)

(54) Verfahren und Anordnung zum Bereitstellen eines drahtlosen Mesh-Netzwerks

Method and arrangement for provision of a wire-free mesh network

Procédé et structure pour mise à disposition d'un réseau maillé sans fil

(84) Benannte Vertragsstaaten:
DE FR GB IT SE

(30) Priorität: **24.08.2006 EP 06017663**

(43) Veröffentlichungstag der Anmeldung:
06.05.2009 Patentblatt 2009/19

(73) Patentinhaber: **Siemens Enterprise Communications GmbH & Co. KG**
81379 München (DE)

(72) Erfinder:
- **FALK, Rainer**
  85435 Erding (DE)
- **KOHLMAYER, Florian**
  82319 Starnberg (DE)

(74) Vertreter: **Fritzsche, Thomas et al**
Fritzsche Patent
Naupliastrasse 110
81545 München (DE)

(56) Entgegenhaltungen:
EP-A- 1 635 528
US-A1- 2004 141 468
US-A1- 2006 114 863

- **IEEE COMPUTER SOCIETY: "802.11i IEEE Standard for Information Technology - Telcommunications and information exchange between systems - Local and metropolitan area networks - specific requirements" IEEE STANDARDS, IEEE,, US, Bd. 802.11, 23. Juli 2004 (2004-07-23), Seiten 1-175, XP002402752**
- **FACCIN S M ET AL: "Mesh WLAN networks: concept and system design" IEEE WIRELESS COMMUNICATIONS, [Online] Bd. 13, Nr. 2, April 2006 (2006-04), Seiten 10-17, XP002415589 ISSN: 1536-1284 Gefunden im Internet: URL:http://ieeexplore.ieee.org/iel5/7742/34234/01632476.pdf?isnumber=34234&arnumber= 1632476> [gefunden am 2007-01-18]**
- **IEEE: 'IEEE P802.11s(TM)/D0.02 Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking' 01 Juni 2006, THREE PARK AVENUE NEW YORK, NEW YORK, Seiten I - 202, XP055021575**

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

Printed by Jouve, 75001 PARIS (FR)

EP 2 055 072 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Bereitstellen eines drahtlosen Mesh-Netzwerks gemäß Anspruch 1 sowie eine Anordnung zum Bereitstellen eines drahtlosen Mesh-Netzwerks gemäß Anspruch 23.

[0002] Ein drahtloses Maschen- bzw. Mesh-Netzwerk ist ein vermaschtes Netz, das beispielsweise in einem Wireless Local Area Network (WLAN) implementiert ist. Bei einem Mesh-Netzwerk kann ein mobiler Knoten Daten, die von einem anderen mobilen Knoten stammen, an einen weiteren mobilen Knoten weiterleiten oder an eine Basisstation übertragen. In einem Maschennetzwerk bzw. Mess-Netzwerk (Mesh-Network) können weite Distanzen überspannt werden, insbesondere in unebenen oder schwierigen Terrain. Maschennetze arbeiten zudem sehr zuverlässig, da jeder mobile Knoten mit einigen anderen Knoten verbunden ist. Wenn ein Knoten ausfällt, beispielsweise auf Grund eines Hardware-Defekts, suchen dessen Nachbarknoten eine alternative Datenübertragungsroute. Maschennetze bzw. Mesh-Networks können feste oder mobile Geräte mit einbeziehen.

[0003] In Figur 1 ist, wie oben erläutert, ein Mesh-Netzwerk MESH, welches mit einem Infrastrukturnetzwerk INFRASTRUCTURE NETWORK verbunden ist, dargestellt und weist neben Knoten MP, MAP des Mesh-Netzwerks auch nicht Mesh-Stationen, wie beispielsweise eine nach WLAN funktionierende Station STA auf. Diese nach WLAN funktionierende Station STA ist mit dem Mesh-Netzwerk MESH über einen Mesh-Netzwerk-Knoten MAP, der als WLAN-Zugangspunkt, d.h. WLAN Access Point, arbeitet, verbunden.

[0004] Dabei kann das Mesh-Netzwerk MESH der WLAN-Station STA auch Zugang zu einem Infrastrukturnetzwerk INFRASTRUCTURE NETWORK, wie beispielsweise einem Firmennetz oder dem Internet ermöglichen.

[0005] Dabei erfolgt eine Authentisierung von Mesh-Knoten MP und/oder WLAN-Stationen STA beispielsweise unter Verwendung eines Authentisierungsservers AAA-Server (AS), wobei das Mesh-Netzwerk MESH in dem dargestellten Beispiel über eine Gateway-Komponente GW mit dem Infrastrukturnetzwerk INFRASTRUCTURE NETWORK gekoppelt ist.

[0006] In Figur 2 ist ein eigenständiges Mesh-Netzwerk MESH, wie es aus dem Stand der Technik bekannt ist, dargestellt. Dabei bedeutet eigenständig, dass das Mesh-Netzwerk MESH ausschließlich aus Mesh-Knoten MP gebildet wird.

[0007] Dabei kann es sich sowohl um Infrastrukturknoten als auch um so genannte Endbenutzerknoten, wie beispielsweise einem Notebook oder PDA handeln.

[0008] Figur 3 hingegen zeigt ein eigenständiges Mesh-Netzwerk mit einem Zugangspunkt MAP, wie es aus dem Stand der Technik bekannt ist, welcher es den nicht-mesh-fähigen Geräten, wie beispielsweise den dargestellten WLAN-Stationen STA erlaubt, sich am Netzwerk MESH anzumelden. Die dargestellten WLAN-Stationen STA nehmen jedoch nicht selbst am Mesh-Routing teil.

[0009] In den dargestellten Anordnungen gemäß dem Stand der Technik ist es dabei üblich, dass sich die Geräte mit einer so genannten MAC-Adresse (Media Access Control Ethernet ID) im Netzwerk identifizieren. Eine MAC-Adresse ist dabei die Schicht-2-Adresse eines Knotens zur Kommunikation in Kommunikationsnetzen basierend auf den IEEE 802 Standards, wie beispielsweise bei WLAN nach IEEE 802.11 und den gezeigten Mesh-Netzwerken MESH nach IEEE 802.11S. In der Regel ist diese Adresse global eindeutig mit der jeweiligen Hardware in Verbindung zu bringen.

[0010] Es ist jedoch bekannt, dass nicht vertrauenswürdige Teilnehmer ATTACKER MP fälschlicher Weise oder mit voller Absicht die MAC-Adresse eines vertrauenswürdigen Teilnehmers GOOD MP verwenden. Durch eine solche Manipulation, die auch als MAC Address Spoofing bekannt ist, kommt es zu Störungen der befallenen Netzwerke, beispielsweise zu Denial of Service (DoS) Attacken, die dadurch entstehen, dass das Opfer GOOD MP nicht mehr kommunizieren kann, weil seine Drahtlosverbindung (Wireless Link) nicht mehr gültig ist. Ferner kann an einem WLAN-Hotspot mit rein http browserbasierter Anmeldung die Kommunikationssitzung des vertrauenswürdigen Teilnehmers GOOD MP übernommen werden.

[0011] Aus Joshua Right Detecting Wireless LAN MAC Address Spoofing, 21.01.2003, http://www.routesecure.net/content/downloads/pdf/wlan_mascpoo_f_detection.pdf sind Maßnahmen zum Erkennen dieses WLAN MAC Address Spoofings offenbart, bei denen zum einen eine Überprüfung erfolgt, ob eine den Herstellern exklusiv zugewiesene so genannte Organizationally Unique Identifier OUI (siehe http://standart.ieee.org/regauth/oui/oui.txt), die Teil der übermittelten MAC-Adresse ist, überhaupt einem Hersteller zugewiesen ist. Weiterhin können auch WLAN MAC-Sequenznummern eines Teilnehmers, die üblicherweise fortlaufend erhöht werden, ausgewertet werden, was derart erfolgt, dass sobald eine größere Lücke auftaucht, ein Indiz dafür besteht, dass der entsprechende MAC Frame von einer anderen Station (Angreifer) gesendet wurde.

[0012] Nachteilig hierbei ist, dass die Überprüfung der OUI nur greift, falls die MAC-Adresse zufällig generiert wird, aber nicht dann, wenn der Angreifer ATTACKER MP lediglich die MAC-Adresse eines anderen vertrauenswürdigen Teilnehmers GOOD MP verwendet. Ferner kann auch der Angreifer ATTACKER MP auch zufällig MAC-Adressen generieren, unter der Nebenbedingung, dass deren OUI zugewiesen ist.

[0013] EP 1635528 A1 offenbar ein Verfahren zur Gewährung eines Zugangs zu einem Datenkommunikationsnetzwerk sowie einen entsprechenden Authentifikationsserver. Ein Verfahren und ein System zum Mapping originaler Media Access Control (MAC) Adressen zu eindeutigen lokal verwaltenden virtuellen MAC-Adressen in

einem Ethernet Netzwerk wird in US 2004/0141468 A1 offenbart.

[0014] Weiterhin ist aus der Patentanmeldung US 2006/0114863 eine Methode zur Absicherung von IEEE 802.11 Datenverkehr gegen das MAC Address Spoofing bekannt, bei der ein Schutz vor dem MAC- Address Spoofing bei WLAN-Netzwerken derart erfolgt, dass eine Zuordnungstabelle von MAC-Adresse und einer bei der WLAN-Anmeldung verwendeten Benutzeridentität angelegt ist und bei nachfolgenden WLAN-Anmeldungen die verwendete MAC-Adresse sowie die Benutzeridentität mit dem in der Zuordnungstabelle vorhandenen Eintrag auf Übereinstimmung überprüft werden und im Negativfall die Anmeldung abgewiesen wird. IEEE P802.11s D0.02, Juni 2006, offenbart ein Meshnetzwerk an dem sich Nicht-Mesh-Teilnehmer anmelden können und in dem auf Basis von Mac Adressen ein Layer 2 Routing erfolgt, bei dem Route Request Nachriten mit einem Destination Only Flag verwendet werden können.

[0015] Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein verbessertes Verfahren sowie Anordnung zur Bereitstellung eines drahtlosen Mesh-Netzwerks anzugeben.

[0016] Diese Aufgabe wird durch das Verfahren nach Anspruch 1 sowie durch die entsprechende Anordnung nach Anspruch 23 gelöst.

[0017] Bei dem erfindungsgemäßen Verfahren zum Bereitstellen eines drahtlosen lokalen Netzwerks, bei dem nach dem IEEE 802.11 Standard und seinen Derivaten insbesondere IEEE 802.15 oder IEEE 802.16 ausgestaltete stationäre Kommunikationseinrichtungen sowie mobile Kommunikationseinrichtungen nach Art des Mesh als Subnetzwerk verbunden sind, wird seitens einer sich beim Subnetzwerk anmeldenden Kommunikationseinrichtung dem Subnetzwerk eine anmeldende MAC-Adresse übermittelt, ferner eine Überprüfung derart durchgeführt, dass die anmeldende MAC-Adresse mit den seitens des Subnetzwerks erreichbaren MAC-Adressen verglichen wird und im Fall, dass die anmeldende MAC-Adresse zu den erreichbaren MAC-Adressen disjunkt ist, die anmeldende Kommunikationseinrichtung als Station des Subnetzwerks verbunden wird, während für den Fall, dass die anmeldende MAC-Adresse im Subnetzwerk bereits erreichbar ist, eine Zulassungsprozedur derart durchgeführt wird, dass ein Verwenden der anmeldenden MAC-Adresse durch zwei unterschiedliche Kommunikationseinrichtungen innerhalb des Subnetzwerks unterbunden wird.

[0018] Ein Vorteil des erfindungsgemäßen Verfahrens ist die Immunisierung gegen Auswirkungen des MAC-Address-Spoofings, da diese erfindungsgemäße Vorgehensweise gezielt die Anmeldung unter einer MAC-Adresse, die bereits erreichbar ist, unterbindet, wobei dies im Vergleich zu aus dem Stand der Technik bekannten Ansätzen keine vorab zu speichernden Beziehungen zwischen Geräten und MAC-Adressen oder dergleichen notwendig ist.

[0019] Bei einer Weiterbildung der Erfindung wird dabei als Zulassungsprozedur eine Abweisung der anmeldenden Kommunikation durchgeführt. Hierbei handelt es sich um die einfachste Variante der Sicherstellung einer Vermeidung von MAC Address Spoofing, weil keinerlei zusätzliche Abfragen und Datenübermittlungen notwendig sind. Außerdem ist dies die schnellstmögliche Abwicklung einer Zulassungsprozedur.

[0020] Alternativ wird als Zulassungsprozedur eine Umsetzung der anmeldenden MAC-Adresse derart durchgeführt, dass innerhalb des Subnetzwerks der anmeldenden Kommunikationseinrichtung eine zu den erreichbaren MAC-Adressen disjunkte MAC-Adresse zugewiesen wird.

[0021] Hierdurch wird unabhängig von der jedem Gerät global eindeutig zugeordneten MAC-Adresse intern für die Subnetzwerke eine nur lokal für diese Subnetzwerke gültige MAC-Adresse zugewiesen und so das Spoofing vermieden, d.h. dass ein MAC-Address-Spoofing negative Auswirkungen auf die Funktion des Mesh-Subnetzwerks, insbesondere das Routing und Weiterleiten von Daten innerhalb des Mesh-Subnetzwerks, hat.

[0022] Vorzugsweise wird dabei die disjunkte MAC-Adresse seitens des Subnetzwerks generiert, da diese über die Information der vorhandenen MAC-Adressen verfügt bzw. der in dem lokalen Netzwerk geltenden Adressen. Dabei ist es auch von Vorteil, dass die disjunkte MAC-Adresse aufgrund einer Pseudo-Zufallsfolge insbesondere einer genau einmal erzeugten "Number Used Once, Nonce" generiert wird.

[0023] Ferner ist es von Vorteil, dass die disjunkte MAC-Adresse bei einer Weiterbildung zu global insbesondere seitens Organisationen wie gemäß der OUI zugewiesenen MAC-Adressen disjunkt gewählt wird. Hierdurch ist gewährleistet, dass es keine Kollisionen mit global zugeordneten MAC-Adressen gibt.

[0024] Vorzugsweise wird dabei das 41. Bit der disjunkten MAC-Adresse mit dem Wert 1 belegt, so dass die lokale Gültigkeit auf einfache Weise gekennzeichnet ist.

[0025] Eine weitere vorteilhafte Ausgestaltung der Erfindung besteht darin, als Zulassungsprozedur seitens der im Subnetzwerk eine Prüfung auf Identität der anmeldenden Kommunikationseinrichtung mit der über die der anmeldenden MAC-Adresse entsprechenden erreichbaren MAC-Adresse bestimmten ersten Kommunikationseinrichtung durchzuführen. Hierdurch kann ermittelt werden, ob die anmeldende Kommunikationseinrichtung eine bereits bekannte Kommunikationseinrichtung ist, die lediglich einen weiteren Link im Mesh-Netzwerk aufbauen will, was gemäß Mesh-Architektur auch gewährleistet werden soll und somit kein Fall von Spoofing, sondern ein legitimer Anmeldeversuch ist und daher zuzulassen wäre.

[0026] Dabei ist bei einer Weiterbildung die Identitätsprüfung derart durchzuführen, dass seitens des Subnetzwerkes eine erste Prüfinformation über eine zu der der anmeldenden MAC-Adresse entsprechenden erreichbaren MAC-Adresse bestimmten Kommunikationseinrich-

Samsung Ex. 1004, Page 138 of 563

tung etablierten Route des Subnetzwerks an die erste Kommunikationseinrichtung übermittelt wird, ferner das Subnutzwerk an die erste Kommunikationseinrichtung eine Aufforderung zur Rücksendung der ersten Prüfinformation übermittelt sowie das Subnetzwerk das Rücksenden der ersten Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Station etablierten Route, d.h. über den aufzubauenden Link, des Subnetzwerks erwartet, im Anschluss hieran infolge eines Ausbleibens des Rücksendens ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt bzw. bei Eintreten des Rücksendens die Korrelation der ersten Prüfinformation mit der zurückgesandten Prüfinformation überprüft wird und im Falle des Erreichens eines festgelegten Korrelationsgrades insbesondere bei Identität von erster Prüfinformation zurückgesandter Prüfinformation die anmeldende Kommunikationseinrichtung als Station des Subnetzwerks verbunden wird, andernfalls ebenfalls ein Abweisen der anmeldenden Kommunikationseinrichtung eingeleitet wird.

[0027] Hierdurch wird also ein Senden eines Prüfparameters vom Netzwerk an die bereits angemeldete Station über die schon vorhandene Route durchgeführt und ein Erwarten, dass dieser Prüfparameter über die neu aufzubauende Route zurückgesendet wird, realisiert, was nur dann erfolgreich abgeschlossen wird, wenn es sich bei dem Gerät, das sich anmeldet, um das gleiche Gerät handelt, welches bereits unter der erreichbaren MAC-Adresse im Netz eingebunden ist.

[0028] Eine weitere Variante der Identitätsprüfung erfolgt derart, dass seitens des Subnetzwerks eine erste Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Station etablierte Route des Subnetzwerks an die erste Kommunikationseinrichtung übermittelt wird, das Subnetzwerk an die erste Kommunikationseinrichtung eine Aufforderung zur Rücksendung der ersten Prüfinformation übermittelt, das Subnetzwerk das Rücksenden der ersten Prüfinformation über eine zu der anmeldenden MAC-Adresse entsprechenden erreichbaren MAC-Adresse bestimmten Kommunikationseinrichtung etablierten Route des Subnetzwerks erwartet, ferner bei Ausbleiben des Rücksendens ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt, während bei Eintreten des Rücksendens im Falle die Korrelation der ersten Prüfinformation mit der zurückgesandten Prüfinformation überprüft wird, so dass im Fall des Erreichens eines festgelegten Korrelationsgrades, insbesondere bei Identität von erster Prüfinformation zu zurückgesandter Prüfinformation die anmeldende Kommunikationseinrichtung als Station des Subnetzwerks verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt. Hierbei handelt es sich um eine Variante, bei der der Prüfparameter vom Netzwerk an die sich gerade anmeldende Station gesandt wird, wobei die neu aufzubauende Route hierfür genutzt wird und im Anschluss hieran, das Netzwerk erwartet, dass der Prüfparameter über die bereits vorhandene Route zurückgesandt wird. Auch dies kann nur erfolgen, wenn anmeldendes Gerät und bereits erreichbares Gerät identisch sind und somit beide Routen zu ihm führen, so dass auch hier eine sichere Verifikation der Identität von anmeldender und bereits erreichbarer Station gewährleistet ist.

[0029] Vorzugsweise initiiert das Subnetzwerk die Übertragung der zweiten und/oder dritten Prüfinformation oder alternativ hierzu erfolgt die Übertragung der zweiten und/oder dritten Prüfinformation seitens der anmeldenden Kommunikationseinrichtung automatisch.

[0030] Eine weitere Variante zur Identitätsprüfung besteht darin, dass eine seitens der durch die anmeldende MAC-Adresse entsprechende erreichbare MAC-Adresse bestimmten ersten Kommunikationseinrichtung authentisierenden kryptographischen Schlüssels insbesondere eines aus einer gemäß dem so genannten "Extensible Authentication Protocol EAP"-Protokoll Netzanmeldung resultierenden der anmeldenden Kommunikationseinrichtung verfügbaren ersten Sitzungsschlüssels berechnete vierte Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Station etablierte Route des Subnetzwerks an das Subnetzwerk übermittelt wird, ferner seitens des Subnetzwerks unter Zuhilfenahme eines auf Grundlage eines zweiten durch die der anmeldenden MAC-Adresse entsprechenden erreichbaren MAC-Adresse bestimmten Kommunikationseinrichtung authentisierenden kryptographischen Schlüssels insbesondere eines aus einer gemäß dem "Extensible Autentication Protocol EAP"-Protokoll Netzanmeldung resultierenden dem Subnetzwerk verfügbaren zweiten Sitzungsschlüssels die Gültigkeit der vierten Prüfinformation ermittelt wird, bei gegebener Gültigkeit die anmeldende Kommunikationseinrichtung als Station des Subnetzwerks verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

[0031] Alternativ erfolgt die Identitätsprüfung derart, dass seitens der anmeldenden Kommunikationseinrichtung auf Grundlage eines ersten die anmeldende Kommunikationseinrichtung authentisierenden kryptographischen Schlüssels insbesondere eines aus einer gemäß dem so genannten "Extensible Authentication Protocol EAP"-Protokoll Netzanmeldung resultierenden der anmeldenden Kommunikationseinrichtung verfügbaren ersten Sitzungsschlüssels berechnete fünfte Prüfinformation über eine zu der der anmeldenden MAC-Adresse entsprechenden erreichbaren MAC-Adresse bestimmten Kommunikationseinrichtung etablierten Route an das Subnetzwerk übermittelt, ferner seitens des Subnetzwerks unter Zuhilfenahme eines auf Grundlage eines zweiten die anmeldende Kommunikationseinrichtung authentisierenden kryptographischen Schlüssels ist insbesondere eines aus gemäß dem "Extensible Authentication Protocol EAP"-Protokoll Netzanmeldung resultierenden dem Subnetzwerk verfügbaren zweiten Sitzungsschlüssels die Gültigkeit der Prüfinformation ermittelt wird, bei gegebener Gültigkeit die anmeldende Kommunikationseinrichtung als Station des Subnetzwerks ver-

Samsung Ex. 1004, Page 139 of 563

bunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

[0032] Durch diese beiden Varianten ist eine besonders sichere Verifikation der Identität möglich, da dies auf den jeweiligen Kommunikationseinrichtungen bzw. den zu ihnen bestehenden und respektive neu aufzubauenden Links zugeordneten Verschlüsselungsinformationen erfolgt.

[0033] Dabei wird vorzugsweise der erste und/oder der zweite Sitzungsschlüssel als gemäß dem "Extensible Authentication Protocol EAP"-Protokoll gebildeten Master Session Key, MSK erzeugt, so dass das erfindungsgemäße Verfahren in übliche EAP Umgebungen bzw. auf diese basierend implementiert werden kann.

[0034] Alternativ bzw. ergänzend hierzu können auch der erste und/oder der zweite Sitzungsschlüssel als gemäß dem "Extensible Authentication Protocol EAP"-Protokoll gebildeten "Extended Master Session Key, EMSK" Schlüssel erzeugt werden.

[0035] Zur Berechnung der ersten, zweiten, dritten, vierten und/oder fünften Prüfinformation eignet sich dabei eine Funktion gemäß einer kryptographischen Hash-Funktion, insbesondere der SHA-1, SHA-256 oder MD5 Hash-Funktion, da hier auf bekannte Routinen zurückgegriffen werden kann.

[0036] Alternativ bzw. ergänzend ist es von Vorteil, wenn zur Berechnung der ersten, zweiten, dritten, vierten und/oder fünften Prüfinformation "Keyed Hash-Funktionen", wie insbesondere die EAS-CBC-MAC, HMAC-SHA1, HMAC-SHC256, HMAC-MD5 verwendet wird, wobei die HMAC-Funktionen nach RFC2104 definiert sind.

[0037] Bei einer vorteilhaften Ausgestaltung wird die Zulassungsprozedur initiiert, wenn die anmeldende Kommunikationseinrichtung sich als Teilnehmer nach Art des Mesh beim Subnetzwerk anmeldet, so dass zwischen Mesh-Teilnehmern und Nicht-Mesh-Teilnehmern unterschieden und entsprechende Varianten des erfindungsgemäßen Verfahrens eingesetzt werden können.

[0038] Bei einer weiteren vorteilhaften Ausgestaltung wird die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation als ein insbesondere als Pseudo-Zufallscode, wie beispielsweise ein Nonce-Wert erzeugt.

[0039] Alternativ oder ergänzend hierzu wird bei einer weiteren vorteilhaften Ausgestaltung die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation als ein aus einem insbesondere als Pseudo-Zufallscode, wie beispielsweise ein Nonce erzeugten Wert generierter Hash-Code übermittelt. Hierdurch werden eine zusätzliche Sicherung sowie ein erhöhter Verifikationsgrad erreicht.

[0040] Bei einer weiteren alternativen bzw. ergänzenden Ausgestaltung wird als die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation ein aus einem Betriebsparameter der anmeldenden Kommunikationseinrichtung und/oder ersten Kommunikationseinrichtung generierter Hash-Code übermittelt. Vorteilhaft dabei ist, dass auf bekannte Parameter zurückgegriffen werden kann, so dass kein Parameter generiert werden muss und zugleich besteht aufgrund der engen Kopplung dieser Parameter mit dem Endgerät eine einfache Identifikationsmöglichkeit desselben.

[0041] Die der Erfindung zugrunde liegende Aufgabe wird ferner durch die Anordnung zum Bereitstellen des drahtlosen lokalen Netzwerks gelöst, welches sich durch Mittel zur Durchführung des Verfahrens auszeichnet.

[0042] Weitere Einzelheiten und Vorteile der Erfindung sollen ausgehend vom in den Figuren 1 bis 4 dargestellten Stand der Technik anhand von in den Figuren 5 bis 12 dargestellten Ausführungsbeispielen näher erläutert werden. Dabei zeigt

- Figur 1 ein Mesh-Netzwerk Szenario nach dem Stand der Technik,
- Figur 2 ein eigenständiges Mesh-Netzwerk nach dem Stand der Technik,
- Figur 3 ein Mesh-Netzwerk nach dem Stand der Technik mit einem Zugangspunkt für Nicht-Mesh-Teilnehmerstationen,
- Figur 4 ein Szenario einer Mesh-Ownership-Überprüfung gemäß dem Stand der Technik,
- Figur 5 ein Ablaufdiagramm eines Ausführungsbeispiels der Erfindung,
- Figur 6 ein Nachrichtenflussdiagramm zu einer ersten Variante zur erfindungsgemäßen Mesh-Ownership-Überprüfung,
- Figur 7 ein Nachrichtenflussdiagramm zu einer zweiten Variante zur erfindungsgemäßen Mesh-Ownership-Überprüfung,
- Figur 8 ein Nachrichtenflussdiagramm zu einer dritten Variante zur erfindungsgemäßen Mesh-Ownership-Überprüfung,
- Figur 9 ein Szenario mit über Mesh-Zugangspunkte angeschlossenen Nicht-Mesh-Teilnehmerstationen nach dem Stand der Technik,
- Figur 10 ein MAC-Datenframe gemäß dem Stand der Technik,
- Figur 11 ein Ablaufdiagramm einer Weiterleitung von Mesh-Datenframes gemäß dem Stand der Technik,
- Figur 12 ein Ablaufdiagramm mit erfindungsgemäßer Adressumsetzung ausgehend von den Szenarien gemäß dem Stand der Technik.

[0043] Ausgehend von den in den Figuren 1 bis 4 dargestellten Szenarien und den sich ergebenden Problemen greift die Erfindung vorteilhaft ein und löst die genannten Probleme für ein Mesh-Netzwerk, wie in dem Ausführungsbeispiel gemäß Figur 5 anhand eines das Ausführungsbeispiel aufzeigenden Ablaufdiagramms dargestellt.

[0044] Dabei geht die erfindungsgemäß ausgestaltete Verfahrensweise ausgehend von einem ersten Schritt S1, welcher einen Ausgangszustand START wiedergibt, nach Erhalt eines Ereignisses, nämlich dem Empfang einer Anmeldeaufforderung einer Teilnehmerstation unter Verwendung der MAC-Adresse MA an einem Mesh-

Samsung Ex. 1004, Page 140 of 563

Netzwerk in einem zweiten Schritt S2 über in einen dritten Schritt S3, bei dem geprüft wird, ob bereits eine Station mit der übertragenen MAC-Adresse MA bereits in dem Mesh-Netzwerk angemeldet ist.

[0045] Diese in einem vierten Schritt S4 durchgeführte Überprüfung führt, falls es sich um eine bereits angemeldete erreichbare MAC-Adresse MA handelt, in eine weitere Abfrage in einem fünften Schritt S5, bei dem geprüft wird, ob die anmeldende Teilnehmerstation ein Mesh-Knoten, d.h. ein Mesh-Teilnehmer oder eine Nicht-Mesh-Station ist. Dabei erfolgt in einem sechsten Schritt S6 eine Zurückweisung der Anmeldeanforderung, soweit es sich um eine Nicht-Mesh-Station handelt. Anderenfalls, d.h. im Falle, dass es ein Mesh-Knoten ist, erfolgt in einem achten Schritt S8 eine Überprüfung im Sinne einer MAC Address Ownership-Überprüfung für anmeldende Teilnehmerstation und MAC-Adresse MA. Bei dieser MAC Address Ownership-Überprüfung wird überprüft, ob die Teilnehmerstation berechtigt ist, die übertragene MAC-Adresse MA zu verwenden.

[0046] Ergibt die Abfrage, dass das Ergebnis der MAC Address Ownership-Überprüfung OK ist, d.h., wenn es sich um eine bereits angemeldete Teilnehmerstation handelt, erfolgt in einem zehnten Schritt S10 ein Akzeptieren der Anmeldeaufforderung und die Teilnehmerstation kann diesen Link aufbauen. Anderenfalls erfolgt wiederum eine gemäß dem sechsten Schritt S6 durchgeführte Zurückweisung der Anmeldeaufforderung, so dass das erfindungsgemäße Verfahren in einem siebten Schritt S7 in einen Endzustand kehrt.

[0047] Ein Kern der Erfindung ist also, dass bei einem Netzwerkzugang eines Teilnehmers unter Verwendung einer MAC-Adresse zu einem Mesh-Netzwerk durch das Mesh-Netzwerk überprüft wird, ob bereits ein Teilnehmerknoten mit der von dem anmeldenden Teilnehmer verwendeten MAC-Adresse angemeldet ist und somit in diesem Netz erreichbar ist, wobei für den Fall, dass die MAC-Adresse in diesem Netzwerk noch nicht erreichbar ist, der anmeldende Teilnehmer akzeptiert wird, jedoch im Fall, dass ein Teilnehmer mit der MAC-Adresse erreichbar ist, in der oben beschriebenen Art reagiert wird.

[0048] Dabei existieren auch Alternativen zu der oben beschriebenen Zulassungsprozedur. Eine wäre beispielsweise, dass bei Detektion im vierten Schritt S4, dass es sich um eine bereits erreichbare MAC-Adresse handelt, sofort eine Abweisung des anmeldenden Teilnehmers erfolgt.

[0049] Eine weitere Alternative bzw. Ergänzung zu dem erläuterten Vorgehen im Rahmen der Zulassungsprozedur besteht darin, eine MAC Address Translation, d.h. eine Ersetzung von MAC-Adressen, durchzuführen, ähnlich wie sie beispielsweise auch bei der so genannten Network Address Translation von IP Adressen zur Umsetzung privater IP Adressen in öffentliche IP Adressen bekannt ist. Dabei wird jedoch jeweils eine erste MAC-Adresse in eine ihr zugeordnete zweite MAC-Adresse umgesetzt, wogegen bei einer Network Address Translation eine Umsetzung mehrerer privater IP Adressen auf die gleiche öffentliche IP-Adresse umgesetzt werden.

[0050] Erfindungsgemäß würde dabei die von der anmeldenden Teilnehmerstation angegebene MAC-Adresse bezüglich der Kommunikation innerhalb des Netzwerks durch eine freie MAC-Adresse ersetzt werden, wobei freie MAC-Adresse bedeutet, dass es sich um eine aktuell innerhalb des betreffenden Netzes nicht verwendeten MAC-Adresse handelt, sie also disjunkt ist zu den erreichbaren MAC-Adressen.

[0051] Dabei kann die ersetzende Adresse durch Pseudo-Zufallscodes generiert werden, wobei dies vorzugsweise auf einem MAC-Adressbereich beschränkt ist, bei welchem es sich nicht um einen gemäß OUI bestimmten Organisationen zugewiesenen Adressen handelt.

[0052] Dies lässt sich beispielsweise dadurch sicherstellen, dass das 41. Bit, das so genannte "U/L" für Universal/Local Bit der MAC-Adresse den Wert 1 hat, so dass diese MAC-Adresse eben nicht global eindeutig ist, sondern lokal administriert wird und somit auch nur dort eindeutig ist. Der Effekt ist dann der, dass einem anmeldenden Teilnehmer mit einer externen mehrdeutigen MAC-Adresse dadurch eindeutig eine intern eindeutige zugewiesen wird.

[0053] Für die in dem Ablaufdiagramm genannte Überprüfung des MAC Address Ownership bestehen einige Implementierungsvarianten, die im Folgenden näher erläutert werden sollen.

[0054] Der grundsätzliche Kerngedanke der MAC Address Ownership-Überprüfung ist, dass die sich anmeldende Station die Kenntnis eines MAC Ownership-Prüfparameters bei der Anmeldung nachweisen muss. Die Bedingung, die dabei eine Identitätsüberprüfung ermöglicht, ist, dass der Prüfparameter nur derselben Station bekannt ist, die bereits angemeldet und erreichbar ist.

[0055] Dabei kann dieser Prüfparameter eine pseudo-zufällig generierte Zahl sein, eine so genannte Nonce oder ein kryptographischer Wert, d.h. ein Wert, der mit Hilfe kryptographischer Verfahren und eines Schlüssels berechnet wurde oder ein anderer bekannter Parameter, wie beispielsweise eine Seriennummer oder ein Zählerwert sein.

[0056] Wenn nun die anmeldende Station die Kenntnis dieses Prüfparameters nachweist, wird sie akzeptiert. Dabei wird vorzugsweise dieser Nachweis durch Übertragung des Prüfparameters auf mindestens zwei verschiedenen Routen geführt. Eine Route ist dabei immer die gerade neu aufzubauende, während die andere aus den schon vorhandenen frei wählbar ist.

[0057] Implementierungsvarianten ergeben sich dabei aus unterschiedlichen Abläufen des Nachweises, die möglich sind.

[0058] Beispielsweise kann ein Ablauf derart erfolgen, dass der Prüfparameter vom Netzwerk an die bereits angemeldete Station über die schon vorhandene Route gesendet wird und im Anschluss hieran vom Netzwerk erwartet wird, dass der Prüfparameter über die neu aufzu-

Samsung Ex. 1004, Page 141 of 563

bauende Route zurückgesandt wird. Hierdurch ist also sichergestellt, dass anmeldende und bereits angemeldete Stationen identisch sind und lediglich die anmeldende Station eine weitere Route aufbauen will, wie es gemäß Mesh-Architektur grundsätzlich möglich ist, denn nur, wenn es sich um ein und dieselbe Station handelt, ist ein Rücksenden des Prüfparameters über die neu aufzubauende Route möglich. Ein Angreifer würde diese Information nicht besitzen.

[0059] Eine Variante hierzu besteht darin, dass der Prüfparameter vom Netzwerk an die sich gerade anmeldende Station über die neu aufzubauende Route gesandt wird und im Anschluss hieran, das Rücksenden des Prüfparameters über die bereits vorhandene Route erwartet wird. Dies ist also im Grunde lediglich eine Umkehrung der Übertragungsrichtungen.

[0060] Eine weitere Variante besteht darin, dass der Prüfparameter, wie z.B. die oben genannte pseudo-zufällig generierte Zufallszahl bzw. Nonce von der Station, die sich anmeldet, an das Netzwerk über die genannten zwei Routen, nämlich zum einen die neu aufzubauende und zum anderen die über eine schon vorher vorhandene Route an das Netzwerk übertragen wird. Das Netzwerk muss dann lediglich die Gleichheit der beiden über die verschiedenen Routen eingegangenen Parameter prüfen und im einfachsten Fall bei Identität bzw. bei einem hohen Maß an Korrelation der Prüfparameter entsprechend die anmeldende Station zulassen und bei Ungleichheit abweisen. Initiiert werden kann dabei das Senden durch die beteiligten Stationen ausgelöst werden oder aber es erfolgt ein Abfragen des Prüfparameters initiiert von der Netzwerkseite über die genannten zwei verschiedenen Routen.

[0061] Eine weitere Möglichkeit besteht darin, dass ein Prüfparameter unter Verwendung eines kryptographischen Schlüssels durch die sich gerade anmeldende Station erfolgt. Dies kann beispielsweise auf Grundlage eines aus einer EAP basierten Netzanmeldung resultierenden Master Session Key MSK erfolgen. Nach Berechnen erfolgt dann ein Senden des Prüfparameters über die bereits vorhandene Route an das Netzwerk, welches zum Quercheck unter Nutzung desselben Schlüssels eigens einen Prüfparameter berechnet und ihn mit dem empfangenen auf Identität prüft.

[0062] Analog hierzu kann die angemeldete Station Prüfparameter auf Grundlage des ihm zugeordneten kryptographischen Schlüssels berechnen und ihn über die gerade aufzubauende Route an das Netzwerk senden.

[0063] Kern der Ownership-Überprüfung ist daher

- Senden des Prüfparameters,
- Senden eines aus dem Prüfparameter abgeleiteten Werts, wie beispielsweise den Hash-Wert des Prüfparameters oder des Eingabewertes einer Hash-Funktion, die den Prüfparameter als Resultat liefert, wie beispielsweise SHA-1, SHA-256 oder MD5,
- Verwenden des Prüfparameters als Input zur Berechnung einer kryptographischen Prüfsumme, dem so genannten Message Authentication Code, wie beispielsweise HMAC-SHA1, HMAC-SHA256, HMAC-MD5 oder AES-CPC-MAC, und Senden des Resultats.

[0064] Die beiden ersten Varianten der Nachweisabläufe, d.h. ein Abweisen bzw. eine MAC-Adressumsetzung sind dabei dann von Vorteil, wenn bekannt ist, dass sich ein Teilnehmer nur einmal an diesem Netzwerk anmelden kann bzw. soll, wie beispielsweise es bei herkömmlichen WLAN-Stationen der Fall ist, während die dritte Variante, also die Ownership-Überprüfung dann sinnvoll eingesetzt werden kann, wenn ein Teilnehmer legitim mehrere Zugangslinks zu diesem Netzwerk aufrechterhalten kann, wie es beispielsweise für Mesh-Knoten innerhalb eines Mesh-Netzwerkes zugelassen ist.

[0065] Daher sieht auch eine Weiterbildung vor, dass unterschiedliche Arten von Teilnehmern unterschieden werden, für oben genannten Fall beispielsweise konkret zwischen Mesh-Teilnehmern und Nicht-Mesh-Teilnehmern, wobei einer Teilnehmerstation freigestellt ist, sich als Mesh-Teilnehmer oder Nicht-Mesh-Teilnehmer am Netzwerk anzumelden und wobei die Überprüfung dann derart durchgeführt wird, dass für den Fall, dass er sich als Nicht-Mesh-Teilnehmer anmeldet, erfindungsgemäß überprüft wird, dass auch kein anderer Teilnehmer mit der gleichen MAC-Adresse als Mesh-Teilnehmer am Netzwerk angemeldet ist. Auch kann überprüft werden, dass kein anderer Teilnehmer mit der gleichen MAC-Adresse als Nicht-Mesh-Teilnehmer am Netzwerk bereits angemeldet ist.

[0066] In Figur 6 ist eine detailliertere Darstellung einer ersten Variante der Ownership-Überprüfung in Form eines Nachrichtenflussdiagramms dargestellt.

[0067] Zu erkennen ist der Nachrichtenfluss zwischen einer sich anmeldenden Station MP-A, welche die MAC-Adresse MACA aufweist, an einem Mesh-Netzwerk, welches zumindest aus den Mesh-Knoten MP-1 und MP-2 besteht, wobei eine erste Station MP-1 eine erste MAC-Adresse MAC1 aufweist und die zweite Station MP-2 eine zweite MAC-Adresse MAC2 zu eigen hat.

[0068] Ein gemäß der Erfindung ergebender möglicher Nachrichtenablauf sich wie folgt darstellt.

[0069] Zu einem ersten Zeitpunkt T1.1 sendet die anmeldende Station MP-A eine Anmeldeanforderung zum Aufbau eines Links an einen Mesh-Knoten des Mesh-Netzwerks, in dem gewählten Beispiel eine zweite Station MP-2.

[0070] Hierauf wird zu einem Zeitpunkt T1.2 durch MP-2 geprüft, ob die MAC-Adresse der anmeldenden Station MACA bereits im Mesh-Netzwerk erreichbar ist, d.h. ob bereits ein Knoten mit dieser Adresse angemeldet ist. Bei dem dargestellten Beispiel soll angenommen werden, dass dies der Fall ist. Dabei könnte eine Überprüfung auf Vorhandensein einer bereits bestehenden erreichbaren Adresse dadurch erfolgen, dass die zweite

Samsung Ex. 1004, Page 142 of 563

Station MP-2 seine Routingtabellen nach einem Eintrag für die Anmelde-MAC-Adresse MACA durchsucht, oder es erfolgt durch eine so genannte Route Request Nachricht, die vorzugsweise mit einem Destination Only "Flag" für den Knoten mit der anmeldenden MAC-Adresse MACA ausgesendet wird, um eine eventuell vorhandene Route durch das Mesh-Netzwerk zu ermitteln.

[0071] Da hier im vorliegenden Fall die Anmelde-MAC-Adresse MACA bereits eine im Mesh-Netzwerk erreichbare Adresse darstellt, sendet die zweite Kommunikationseinrichtung MP-2 zu einem Zeitpunkt T1.3 eine Fehlernachricht an die anmeldende Station MP-A zurück, welche angibt, dass ein MAC Address Ownership-Nachweis MAO erforderlich ist, wobei diese Nachricht optional ist.

[0072] Ferner wird zu einem vierten Zeitpunkt T1.4 seitens der zweiten Kommunikationseinrichtung MP-2 ein Prüfparameter N, beispielsweise eine Pseudo-Zufallszahl erzeugt und gespeichert optional mit weiteren Daten, insbesondere der MAC-Adresse MACA der anmeldenden Station MP-A, um diese dann anschließend für den Ownership-Nachweis derart zu verwenden, dass die zweite Kommunikationseinrichtung MP-2 über eine erste Kommunikationseinrichtung MP-1 an die anmeldende Station MP-A diesen Prüfparameter als Nachricht sendet, wobei diese Nachricht zuerst an die erste Kommunikationseinrichtung MP-1 gesandt wird, welche sie dann an die anmeldende Station MP-A weiterleitet.

[0073] Neben dem Prüfparameter N enthält diese Nachricht dabei auch als Adressinformation die MAC-Adressen von der zweiten Kommunikationseinrichtung MP-2 und der anmeldenden Station MP-A, damit auch, falls die Nachricht über mehrere Zwischenknoten weitergeleitet wird, dennoch erfolgreich bei der anmeldenden Station MP-A eintrifft.

[0074] Nach Erhalt dieser Nachricht wird zu einem fünften Zeitpunkt T1.5 seitens der anmeldenden Kommunikationseinrichtung MP-A erneut eine Anmeldeanforderung zum Aufbau eines Links an die zweite Kommunikationseinrichtung MP-2 versandt, wobei diese im Gegensatz zu der zum ersten Zeitpunkt T1.1 versandten Aufforderung auch den Prüfparameter N enthält.

[0075] Hierauf kann dann zu einem sechsten Zeitpunkt T1.6 durch die zweite Kommunikationseinrichtung MP-2 der von der anmeldenden Station MP-A gesendete Prüfparameter N dahingehend überprüft werden, ob er mit dem gespeicherten übereinstimmt, welches in dem dargestellten Szenario der Fall sein soll, so dass zu einem siebten Zeitpunkt T1.7 die zweite Kommunikationseinrichtung MP-2 an die anmeldende Kommunikationseinrichtung MP-A eine OK-Nachricht zur Bestätigung sendet und somit die anmeldende Station MP-A als Teilnehmerstation des Netzwerks zugelassen wird.

[0076] In Figur 7 ist nun eine weitere Variante dargestellt, bei der die alternative Realisierung des Nachweisablaufs darin besteht, dass die anmeldende Station MP-A selbst einen Prüfparameter N generiert, der von der zweiten Kommunikationseinrichtung MP-2 über den vorhandenen Link über die erste Kommunikationseinrichtung MP-1 abgefragt wird. Bei dem dargestellten Nachrichtenablaufdiagramm startet zu einem ersten Zeitpunkt T2.1 der Nachweisablauf derart, dass die anmeldende Station MP-A zunächst wie üblich eine Anmeldeanforderung zum Aufbau eines Links an die zweite Kommunikationseinrichtung MP-2 sendet.

[0077] Daraufhin prüft zu einem zweiten Zeitpunkt T2.2 die zweite Kommunikationseinrichtung MP-2, ob die MAC-Adresse, welche seitens der anmeldenden Kommunikationseinrichtung MP-A übertragen worden ist, d.h. die Anmeldeadresse MACA bereits im Mesh-Netzwerk erreichbar ist, d.h. ein Knoten mit dieser MAC-Adresse angemeldet ist. Auch in diesem Beispiel soll dies angenommen werden, wobei die Überprüfung, wie unter Figur 6 beschrieben, erfolgen könnte. Auch bei dieser Variante wird zu einem dritten Zeitpunkt T2.3 seitens der zweiten Kommunikationseinrichtung MP-2 eine Fehlernachricht an die anmeldende Kommunikationseinrichtung MP-A zurückgesandt, welche angibt, dass ein MAC Address Ownership-Nachweis MAO erforderlich ist, so dann in Abweichung zu der oben beschriebenen Variante die anmeldende Station MP-A selbst einen Prüfparameter N erzeugt, wie beispielsweise eine Pseudo-Zufallszahl und diese speichert. Um nun der zweiten Kommunikationseinrichtung MP-2 die Überprüfung zu ermöglichen, sendet die anmeldende Station MP-A über die erste Kommunikationseinrichtung MP-1 an die zweite Kommunikationseinrichtung MP-2 eine Nachricht, wobei diese zuerst an die erste Kommunikationseinrichtung MP-1 gesendet wird, welche sie dann an die zweite Kommunikationseinrichtung MP-2 weiterleitet und den Prüfparameter N, welcher durch die anmeldende Kommunikationseinrichtung MP-A erzeugt worden ist, enthält. Die Kommunikationseinrichtung speichert den empfangenen Prüfparameter N und optional weitere Daten, insbesondere die MAC-Adresse MACA der anmeldenden Station MP-A.

[0078] Zu einem fünften Zeitpunkt T2.5 sendet die anmeldende Kommunikationseinrichtung daraufhin erneut eine Anmeldeanforderung zum Aufbau eines Links an die zweite Kommunikationseinrichtung MP-2, wobei diese im Gegensatz zu der zum ersten Zeitpunkt T2.1 versandten Nachricht auch den Prüfparameter N enthält.

[0079] Daraufhin erfolgt zu einem sechsten Zeitpunkt T2.6, nachdem die zweite Kommunikationseinrichtung MP-2 die Nachricht von der anmeldenden Kommunikationseinrichtung MP-A erhalten hat, eine Überprüfung durch die zweite Kommunikationseinrichtung MP-2 dahingehend, ob der von der anmeldenden Kommunikationseinrichtung MP-A gesendete Prüfparameter mit dem über die erste Kommunikationseinrichtung MP-1 empfangenen Prüfparameter übereinstimmt, was in diesem Beispiel angenommen wird, so dass zu einem siebten Zeitpunkt T2.7 die zweite Kommunikationseinrichtung MP-2 an die anmeldende Kommunikationseinrichtung MP-A eine OK-Nachricht zur Bestätigung sendet und diese Teilnehmerstation dem Netzwerk zulässt.

Samsung Ex. 1004, Page 143 of 563

[0080] Eine Alternative hierzu wäre seitens der anmeldenden Kommunikationseinrichtung MP-A bereits bei der ersten Anmeldung einen Prüfparameter in die Nachricht einzufügen, was zu einem fast identischen Ablauf führen würde, der sich nur dahingehend unterscheidet, dass die ersten beiden Nachrichten entfallen.

[0081] Bei den Prüfparametern kann es sich dabei insbesondere um pseudo-zufällig generierte Zufallszahlen (Nonce) handeln.

[0082] In Figur 8 ist eine weitere Variante dargestellt und am Beispiel eines Nachrichtenflussdiagramms erläutert, bei dem auf das Erzeugen eines Prüfparameters verzichtet wird und stattdessen auf einen seitens der anmeldenden Station MP-A vorhandenen Information, d.h. Parameter, zurückgegriffen wird, welcher seitens der zweiten Kommunikationseinrichtung MP-2 über beide Routen, d.h. einmal über die neu aufzubauende Route sowie über die bereits bestehende abgefragt wird.

[0083] Dabei ist ein Vorteil dieser Variante, dass beliebige Parameter abgefragt werden können, so dass dadurch eine Überprüfung ermöglicht wird, bei der die übliche Anmeldeprozedur selbst nicht geändert werden muss. Es genügt lediglich, wenn der anmeldenden Kommunikationseinrichtung MP-A zugeordnete Parameterwerte abfragbar sind.

[0084] Dabei kann es sich bei diesen Parametern insbesondere um Seriennummern der anmeldenden Kommunikationseinrichtung MP-A, den Typ, das Modell, die Softwareversion der genannten Kommunikationseinrichtung handeln, ferner kann es sich auch um Zählerwerte der anmeldenden Kommunikationseinrichtung MP-A handeln, wie beispielsweise Paketzähler, Sequenznummernzähler von Routing-Nachrichten, die spezielle Route Request Sequence Number der anmeldenden Kommunikationseinrichtung MP-A, d.h. es werden an ihm zwei Route Request-Anfragen über die beiden genannten Routen gestellt, auf die er mit der jeweils passenden, d.h. eng beieinander liegenden Sequenznummer antworten muss, wobei darauf zu achten wäre, dass bei der über den neu aufzubauenden Link bzw. die Route übertragene Route Request, d.h. derjenige keine Angaben über die "Destination Sequence Number" erfolgen, da ansonsten ein eventueller Angreifer-Knoten den aktuellen und damit erwarteten Wert lernen würde.

[0085] Bei der anschließenden Überprüfung würde dann getestet, ob die Werte identisch sind bzw. ob die Zählerwerte, welche unterschiedlich sein können, da die Abfragen ja auch zu unterschiedlichen Zeitpunkten stattfinden, hinreichend nah beieinander liegen. Hierzu wäre beispielsweise ein Schwellwertvergleich zu bevorzugen.

[0086] Die Nachrichten fließen dabei wie folgt.

[0087] Zu einem ersten Zeitpunkt T3.1 wird die bekannte Anmeldeanforderung seitens der anmeldenden Kommunikationseinrichtung MP-A, welche die Anmeldeadresse MACA enthält, an die zweite Kommunikationseinrichtung MP-2 gesandt, worauf diese prüft, ob die übertragene Anmeldeadresse MACA bereits im Mesh-Netzwerk erreichbar ist und zu einem dritten Zeitpunkt T3.3 eine Anfrage nach beliebigen Parametern an die anmeldende Station MP-A versendet, worauf die anmeldende Station MP-A hierauf die entsprechenden Parameter an die zweite Kommunikationseinrichtung MP-2 sendet, welche diese dann zu einem fünften Zeitpunkt T3.5 speichert und zu einem sechsten Zeitpunkt T3.6 eine Abfrage der gleichen Parameter über die erste Kommunikationseinrichtung MP-1 an die anmeldende Kommunikationseinrichtung MP-A versendet, woraufhin die anmeldende Kommunikationseinrichtung MP-A die geforderten Parameter über die erste Kommunikationseinrichtung MP-1 an die zweite Kommunikationseinrichtung MP-2 überträgt, so dass zu einem achten Zeitpunkt T3.8 die zweite Kommunikationseinrichtung MP-2 eine OK-Nachricht an die anmeldende Station MP-A übertragen kann und somit eine Zulassung dieser Station zum Netzwerk erfolgt.

[0088] Eine Alternative hierzu besteht darin, den Link gewissermaßen unter Vorbehalt aufzubauen. D.h. die OK-Nachricht würde direkt nach der Anmeldeanforderung gesendet und danach in einer Vorbehaltsphase die Prüfungen, wie oben dargestellt, durchgeführt, so dass, falls die Überprüfung negativ ausfällt, der direkte Link wieder abgebaut wird. Dabei wird vorzugsweise der direkte Link zwischen der anmeldenden Station MP-A und der zweiten Kommunikationseinrichtung MP-2 von der zweiten Kommunikationseinrichtung MP-2 für das Routing erst dann als Vorhanden behandelt, wenn die Überprüfung erfolgreich durchgeführt ist, d.h. nach der Vorbehaltsphase.

[0089] In Figur 9 ist nun ein Szenario dargestellt, bei dem durch das Mesh-Netzwerk, d.h. durch einen der Mesh Access Points MAP bei der Anmeldung eines Knotens als Nicht-Teilnehmer, d.h. beispielsweise als eine WLAN-Station STA an einem Mesh Access Point MAP geprüft wird, ob bereits innerhalb des Mesh-Netzes ein Mesh-Knoten angemeldet ist, der die gleiche MAC-Adresse verwendet, wie die anmeldende Station, welcher sich als Nicht-Mesh-Teilnehmer anmeldet.

[0090] Das besondere an diesem dargestellten Beispiel ist, dass nur die MAC-Adresse eines Knotens bei einer Anmeldung einer Station als Nicht-Mesh-Teilnehmer geprüft wird und nur eine Prüfung gegenüber denjenigen MAC-Adressen stattfindet, die zu einem Mesh-Knoten gehören, also einem Teilnehmer, der als Mesh-Teilnehmer angemeldet ist.

[0091] Hierdurch wird gewährleistet, dass kein Nicht-Mesh-Teilnehmer die MAC-Adresse eines Mesh-Knotens verwendet bzw. mit dieser MAC-Adresse innerhalb des Mesh-Netzwerkes sichtbar ist. Dabei ist erkennbar, dass ein Knoten kein Mesh-Teilnehmer ist, durch einen Eintrag in einer Tabelle mit einem gesetzten Flag, welches als "isProxied" (s. IEEE 802.11s D0.02 Abschnitt 11A.3.5.2 MP Proxy Table) bekannt ist, wogegen ein Mesh-Knoten, welcher zu einem Mesh-Teilnehmer gehört, in der Tabelle mit einem entsprechend nicht gesetzten Flag erfasst wäre.

[0092] Erfindungsgemäß könnten dabei folgende

Samsung Ex. 1004, Page 144 of 563

Maßnahmen ergriffen werden, wenn die Nicht-Mesh-Teilnehmerstation eine Adresse aufweist, welche gleich ist zu einer Mesh-Teilnehmerstation und zwar würde entweder die Anmeldung der entsprechenden Nicht-Mesh-Station abgewiesen oder die von der Nicht-Mesh-Station verwendete MAC-Adresse wird in eine freie MAC-Adresse übersetzt MAC Address Translation.

[0093] Dabei könnte in einer Variante die Prüfung derart erfolgen, dass ermittelt wird, ob die MAC-Adresse bereits in Benutzung ist, sowohl gegenüber Mesh-Teilnehmern wie gegenüber Nicht-Mesh-Teilnehmern, d.h. es wird geprüft, ob irgendein Knoten MP, MAP, STA unter dieser MAC-Adresse erreichbar ist.

[0094] Diese Variante ist insbesondere dann vorteilhaft, wenn keine Information verfügbar ist, ob ein Knoten mit einer bestimmten MAC-Adresse am Mesh-Routing selbst teilnimmt.

[0095] Die MAC-Adressumsetzung MAC Address Translation soll ausgehend von der Figur 10 und 11 näher erläutert werden.

[0096] Dabei zeigt Figur 10 den Aufbau eines nach IEEE 802.11 definierten MAC Frames, der gemäß dem Standard bis zu vier Adressfelder, so genannte MAC-Adressen, enthalten kann (vgl. auch IEEE 802.11 Abschnitt 7.2).

[0097] Dabei kann es sich um die

- so genannte Source Address SA,
- Destination Address DA,
- Transmitting Station Address TA
- oder so genannte Receiving Station Address RA

handeln.

[0098] Source Address SA bezeichnet dabei die Adresse des ursprünglichen Senders, während die Destination Address DA die Adresse des endgültigen Empfängerknotens angibt.

[0099] Im Allgemeinen werden jedoch innerhalb eines Mesh-Netzwerks Frames über mehrere Zwischenknoten weitergeleitet, so dass dafür die Adressfelder Transmitting Station Address TA und Receiving Station Address RA verwendet werden.

[0100] Dabei ist die Transmitting Station Address TA und die Receiving Station Address RA immer in diesem Frame enthalten, während die Source Address SA und die Destination Address DA nur dann befüllt sind, wenn sie benötigt werden, d.h. unterschiedlich zu der Transmitting Station Address TA oder der Receiving Station Address RA sind.

[0101] Daneben enthält das Data Frame prinzipiell auch noch ein Feld für Nutzdaten DATA sowie ein Feld mit der Prüfsumme FCS.

[0102] Weitere für die Erläuterung nicht relevante Header-Felder, wie Frame Control, Duration/ID oder Sequence Control sind dabei zur Vereinfachung nicht dargestellt worden.

[0103] Figur 11 verdeutlicht dabei den Einsatz dieser MAC Frames, wobei die jeweilige Befüllung selbst erklärend ist.

[0104] In Figur 12 ist schließlich, von diesem Stand der Technik ausgehend, die erfindungsgemäße Umsetzung der MAC-Adresse für den Fall einer bereits verwendeten bzw. erreichbaren Adresse dargestellt.

[0105] Zu erkennen ist, dass seitens eines MAC Access Points MAP-1 eine Umsetzung der MAC-Adresse M-S einer Nicht-Mesh-Teilnehmerstation STA in eine innerhalb des Mesh-Netzes nicht verwendete, z.B. pseudo-zufällig erzeugte MAC-Adresse M-R, mit "R" wie Random.

[0106] Die Umsetzung ist daher auch als Ersetzen der von der Nicht-Mesh-Teilnehmerstation STA angegebenen MAC-Adresse M-S zu werten, wobei von den Nicht-Mesh-Teilnehmerknoten STA kommenden MAC Frames die Umsetzung lediglich die Transmitter Address TA, welche identisch zur Source Address SA ist, betrifft und bei an den Nicht-Mesh-Teilnehmerknoten STA gerichteten MAC Frames die Receiver Address RA, welche identisch zur Destination Address DA ist.

[0107] Dargestellt ist auch die Zuordnungstabelle in dem Mesh Access Point, über welchen die Nicht-Mesh-Teilnehmerstation STA sich anmeldet. Zu erkennen ist dabei, dass diese Einträge enthält, mit der jeweils aufeinander abzubildende Mesh-Netz-externe MAC-Adressen (MAC EXT) zugeordnet zu den Mesh-Netz-internen MAC-Adressen (MAC INT) gespeichert sind.

[0108] Eine Variante hierbei ist, dass die genannte MAC-Adressumsetzung bzw. Translation stets stattfindet, d.h. unabhängig davon, ob die angegebene MAC-Adresse schon erreichbar ist oder nicht.

Patentansprüche

1. Verfahren zum Bereitstellen eines drahtlosen lokalen Netzwerks, bei dem nach dem IEEE 802.11 Standard und seinen Derivaten, insbesondere IEEE 802.15 oder IEEE 802-16, ausgestaltete stationäre Kommunikationseinrichtungen, AP, sowie mobile Kommunikationseinrichtungen (MAP, MP) nach Art des Mesh als Subnetzwerk verbunden sind, wobei alle mobilen Kommunikationseinrichtungen (MAP, MP), die zu einem aus MESH-Knoten (MAP, MP) gebildeten Subnetzwerk (MESH) gehören, die MESH-Teilnehmer bilden und wobei eine nicht-MESH-fähige mobile Kanmunikatior-seinrichtung (STA), wie beispielsweise eine WLAN-Station, als Nicht-MESH-Teilnehmer sich an diesem SubNetzwerk (MESH) anmelden kann, wobei

   a) seitens einer sich als Nicht-MESH-Teilnehmer bei diesem Subnetzwerk (MESH) anmeldenden nicht-MESH-fähigen mobilen Kommunikationseinrichtung (MP-A) dem Subnetzwerk (MESH) eine anmeldenden MAC-Adresse (MA-

Samsung Ex. 1004, Page 145 of 563

CA) übermittelt wird,
b) eine Überprüfung derart durchgeführt wird, dass die anmeldende MAC-Adresse (MAC-A) mit den innerhalb des Subnetzwerks (MESH) erreichbaren MAC-Adressen (MAC1, MAC2) verglichen wird, wobei in der Überprüfung eine Route Request Nachricht mit einem Destination Only Flag für die Kommunikationseinrichtung mit der anmeldenden MAC-Adresse ausgesendet wird,
c) im Fall, dass die anmeldende MAC-Adresse (MACA) zu den innerhalb des Subnetzwerks (MESH) erreichbaren MAC-Adressen (MAC1, MAC2) disjunkt ist, die anmeldenden Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird,
d) im Fall, dass die anmeldende MAC-Adresse (MACA) im Subnetzwerk (MESH) bereits erreichbar ist, eine Zulassungsprozedur derart durchgeführt wird, dass ein Verwenden der anmeldenden MAC-Adresse (MACA) durch zwei unterschiedliche Kommunikationseinrichtungen innerhalb des Subnetzwerks (MESH) unterbunden wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** als Zulassungsprozeciur eine Abweisung der anmeldenden Kommunikationseinrichtung (MP-A) erfolgt.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** als Zulassungsprozedur eine Umsetzung der anmeldenden HMAC-Adresse (MACA) derart erfolgt, dass innerhalb des Subnetzwerks (MESH) der anmeldenden Kommunikationseinrichtung (MP-A) eine zu den erreichbaren MAC-Adressen (MAC1, MAC2) disjunkte MAC-Adresse zugewiesen wird.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, dass** die disjunkte MAC-Adresse seitens des Subnetzwerkes (MESH) generiert wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** die disjunkte MAC-Adresse auf Grundlage einer Pseudo-Zufallsfolge - insbesondere einer genau einmal erzeugten "Number Used Once, Nonce" - generiert wird.

6. Verfahren nach einem der Ansprüche 3 bis 5, **dadurch gekennzeichnet, dass** die disjunkte MAC-Adresse auch zu global - insbesondere seitens Organisationen wie gemäß dem OUI, Organizationally Unique Identifier - zugewiesenen MAC-Adressen disjunkt gewählt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** Bit 41 der disjunkten MAC-Adresse mit dem Wert "1" belegt wird.

8. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** als Zulassungsprozedur seitens des Subnetzwerks (MESH) eine Prüfung auf Identität der anmeldende Kommunikationseinrichtung (MP-A) mit der - über die der anmeldenden MAC-Adresse (MACA) - entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) bestimmten ersten Kommunikationseinrichtung (MP-1, MP-2) erfolgt.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** zur Identitätsprüfung

a) seitens des Subnetzwerks (MESH) eine erste Prüfinformation über eine zu der - der anmeldenden MAC-Adresse (MACA) entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) - bestimmten Kommunikationseinrichtung (MP-1, MP-2) etablierten Route des Subnetzwerks (MESH) an die erste Kommunikationseinrichtung (MP-1, MP-2) übermittelt wird,
b) das Subnetzwerk (MESH) an die erste Kommunikationseinrichtung (MP-1, MP-2) eine Aufforderung zur Rücksendung der ersten Prüfinformation übermittelt,
c) das Subnetzwerk (MESH) das Rücksendens der ersten Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Kommunikationseinrichtung (MP-A) etablierte Route des Subnetzwerks (MESH) erwartet,
d) bei Ausbleiben des Rücksendens ein Abweisen der anmeldenden Kommunikationseinrichtung (MP-A) erfolgt,
e) bei Eintreten des Rücksendens die Korrelation der ersten Prüfinformation mit der rückgesandten Prüfinformation überprüft wird,
f) im Falle des Erreichens eines festgelegten Korrelationsgrades - insbesondere bei Identität - von erster Prüfinformation zu rückgesandter Prüfinformation die anmeldende Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

10. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** zur Identitätsprüfung

a) seitens des Subnetzwerks (MESH) eine erste Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Kommunikationseinrichtung (MP-A) etablierte Route des Subnetzwerks (MESH) an die erste Kommunikationseinrichtung (MP-1, MP-2) übermittelt wird,
b) das Subnetzwerk (MESH) an die erste Kommunikationseinrichtung (MP-1, MP-2) eine Auf-

Samsung Ex. 1004, Page 146 of 563

forderung zur Rücksendung der ersten Prüfinformation übermittelt,
c) das Subnetzwerk (MESH) das Rücksenden der ersten Prüfinformation über eine zu der - der anmeldenden MAC-Adresse (MACA) entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) - bestimmten Kommunikationseinrichtung (MP-1, MP-2) etablierten Route des Subnetzwerks (MESH) erwartet,
d) bei Ausbleiben des Rücksendens ein Abweisen der anmeldenden Kommunikationseinrichtung (MP-A) erfolgt,
e) bei Eintreten des Rücksendens im Falle die Korrelation der ersten Prüfinformation mit der rückgesandten Prüfinformation überprüft wird,
f) im Falle des Erreichens eines festgelegten Korrelationsgrades - insbesondere bei Identität - von erster Prüfinformation zu rückgesandter Prüfinformation die anmeldende Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

11. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** zur Identitätsprüfung

a) seitens des Subnetzwerks (MESH) eine zweite Prüfinformation über eine zu der - der anmeldenden MAC-Adresse (MACA) entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) - bestimmten Kommunikationseinrichtung (MP-1, MP-2) etablierten Route des Subnetzwerks (MESH) sowie eine dritte Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Station etablierte Route des Subnetzwerks (MESH) an die erste Kommunikationseinrichtung (MP-1, MP-2) erwartet wird,
b) bei Ausbleiben der zweiten und/oder dritten Prüfinformation ein Abweisen der anmeldenden Kommunikationseinrichtung (MP-A) erfolgt,
c) im Falle bei Eintreffen der zweiten und dritten Prüfinformation die Korrelation der zweiten Prüfinformation mit der dritten Prüfinformation überprüft wird,
d) im Falle des Erreichens eines festgelegten Korrelationsgrades - insbesondere bei Identität - von zweiter Prüfinformation zu dritter Prüfinformation die anmeldende Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

12. Verfahren nach Anspruch 11, **dadurch gekennzeichnet, dass** die Übertragung der zweiten und/oder dritten Prüfinformation seitens des Subnetzwerks (MESH) initiiert wird.

13. Verfahren nach Anspruch 11, **dadurch gekennzeichnet, dass** die Übertragung der zweiten und/oder dritten Prüfinformation seitens der anmeldenden Kommunikationseinrichtung (MP-A) initiiert wird.

14. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** zur Identitätsprüfung

a) eine seitens der anmeldenden Kommunikationseinrichtung (MP-A) auf Grundlage eines ersten die anmeldende Kommunikationseinrichtung (MP-A) authentisierenden kryptografischen Schlüssels - insbesondere eines aus einer gemäß dem so genannten "Extensible Authentication Protocol, EAP"-Protokoll Netzanmeldung resultierenden, der anmeldenden Kommunikationseinrichtung (MP-A) verfügbaren ersten Sitzungsschlüssels - berechnete vierte Prüfinformation über eine im Rahmen des Anmeldeversuchs der anmeldenden Station etablierte Route des Subnetzwerks (MESH) an das Subnetzwerk (MESH) übermittelt wird,
b) seitens des Subnetzwerks (MESH) unter Zuhilfenahme eines auf Grundlage eines zweiten - durch die der anmeldenden MAC-Adresse (MACA) entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) bestimmten Kommunikationseinrichtung (MP-1, MP-2) - authentisierenden kryptografischen Schlüssels - insbesondere eines aus einer gemäß dem "Extensible Authentication Protocol, EAP"-Protokoll Netzanmeldung resultierenden, dem Subnetzwerk (MESH) verfügbaren zweiten Sitzungsschlüssels - ein Entschlüsselungsversuch durchgeführt wird,
c) bei erfolgreicher Entschlüsselung die anmeldenden Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

15. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, dass** zur Identitätsprüfung

a) eine seitens eines der durch die anmeldende MAC-Adresse (MACA) entsprechenden erreichbaren MAC-Adresse (MAC1, MAC2) bestimmten ersten Kommunikationseinrichtung (MP-1, MP-2) authentisierenden kryptografischen Schlüssels - insbesondere eines aus einer gemäß dem so genannten "Extensible Authentication Protocol, EAP"-Protokoll Netzanmeldung resultierenden, der anmeldenden Kommunikationseinrichtung (MP-A) verfügbaren ersten Sitzungsschlüssels - berechnete fünfte Prüfinformation über eine etablierte Route der anmeldenden Kommunikationseinrichtung

Samsung Ex. 1004, Page 147 of 563

(MP-A) an das Subnetzwerk (MESH) übermittelt,
b) seitens des Subnetzwerks (MESH) unter Zuhilfenahme eines auf Grundlage eines zweiten die anmeldende Kommunikationseinrichtung (MP-A) authentisierenden kryptografischen Schlüssels - insbesondere eines aus einer gemäß dem "Extensible Authentication Protocol, EAP"-Protokoll Netzanmeldung resultierenden, dem Subnetzwerk (MESH) verfügbaren zweiten Sitzungsschlüssels - ein Entschlüsselungsversuch durchgeführt wird, c) bei erfolgreicher Entschlüsselung die anmeldende Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird, andernfalls ein Abweisen der anmeldenden Kommunikationseinrichtung erfolgt.

16. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der erste und/oder der zweite Sitzungsschlüssel als gemäß dem "Extensible Authentication Protocol, EAP"-Protokoll gebildeten "Master Session Key, MSK" Schlüssels erzeugt wird.

17. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der erste und/oder der zweite Sitzungsschlüssel als gemäß dem "Extensible Authentication Protocol, EAP"-Protokoll gebildeten "Extended Master Session Key, EMSK" Schlüssels erzeugt wird.

18. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** zur Berechnung der ersten, zweiten, dritten, vierten und/oder fünften Prüfinformation eine Funktion gemäß einer kryptographischen - insbesondere SHA-1, SHA256 oder MD5 - Hash-Funktion verwendet wird.

19. Verfahren nach Anspruch 18, **dadurch gekennzeichnet, dass** zur Berechnung der ersten, zweiten, dritten, vierten und/oder fünften Prüfinformation "Keyed-Hash-Funktionen" - insbesondere AES-CBC-MAC, HMAC-SHA1, HMAC-SHA256 oder HMAC-MD5, wobei die HMAC-Funktion nach RFC2104 definiert ist, - verwendet werden.

20. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation als ein - insbesondere als Pseudo-Zufallscode, wie beispielsweise ein "Nonce", - Wert erzeugt wird.

21. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** als die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation ein aus einem - insbesondere als Pseudo-Zufallstode, wie beispielsweise ein "Nonce", - erzeugtem Wert generierter Hash-Code übermittelt wird.

22. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** als die erste, zweite, dritte, vierte und/oder fünfte Prüfinformation ein aus einem Betriebsparameter der anmeldenden Kommunikationseinrichtung (MP-A) und/oder ersten Kommunikationseinrichtung generierter Hash-Code übermittelt wird.

23. Anordnung zum Bereitstellen eines drahtlosen lokalen Netzwerks, bei dem nach dem IEEE 802.15 Standard und seinen Derivaten, insbesondere IEEE 802.15 oder IEEE 802.16, ausgestaltete stationäre Kommunikationseinrichtungen, AE, sowie mobile Kommunikationseinrichtungen (MAP, MP) nach Art des Mesh als Subnetzwerk verbunden sind, wobei alle mobilen Kommunikationseinrichtungen (MAP, MP), die zu einem aus MESH-Knoten (MAP, MP) gebildeten Subnetzwerk (MESH) gehören, die MESH-Teilnehmer bilden und wobei eine nicht-MESH-fähige mobile Kommunikationseinrichtung (STA), wie beispielsweise eine WLAN-Station, als Nicht-MESH-Teilnehmer sich an diesem Subnetzwerk (MESH) anmelden kann, wobei

a) eine Übermittlungsvorrichtung vorhanden ist, durch die seitens einer sich als Nicht-MESH-Teilnehmer bei diesem Subnetzwerk (MESH) anmeldenden nicht-MESH-fähigen mobilen Kommunikationseinrichtung (MP-A) dem Subnetzwerk (MESH) eine anmeldende MAC-Adresse (MACA) übermittelt wird,
b) eine Überprüfungseinrichtung vorhanden ist, durch die eine Überprüfung derart durchgefürt wird, dass die anmeldende MAC-Adresse (MACA) mit den innerhalb des Subnetzwerks (MESH) erreichbaren MAC-Adressen (MAC1, MAC2) verglichen wird, wobei in der Überprüfung eine Route Request Nachricht mit einem Destination Only Flag für die Kommunikationseinrichtung mit der anmeldende MAC-Adresse ausgesendet wird, wobei durch die Überprüfungseinrichtung.
c) im Fall, dass die anmeldende MAC-Adresse (MACA) zu den innerhalb des Subnetzwerks (MESH) erreichbaren MAC-Adressen (HMAC1, MAC2) disjunkt ist, die anmeldende Kommunikationseinrichtung (MP-A) als Station des Subnetzwerks (MESH) verbunden wird,
d) im Fall, dass die anmeldende MAC-Adresse (MACA) im Subnetzwerk (MESH) bereits erreichbar ist, eine Zulassungsprozedur derart durchgeführt wird, dass ein Verwenden der anmeldenden MAC-Adresse (MACA) durch zwei unterschiedliche Kommunikationseinrichtungen innerhalb des Subnetzwerks (MESH) unterbunden wird.

Samsung Ex. 1004, Page 148 of 563

Claims

1. Method for provision of a wireless local network in which stationary communication devices (AP) designed according to standard IEEE 802.11 and its derivatives, in particular IEEE 802.15 or IEEE 802.16, and mobile communication devices (MAP, MP) are connected together in the manner of a mesh as a subnetwork, wherein all mobile communication devices (MAP, MP) which belong to a subnetwork (MESH) formed from MESH nodes (MAP, MP) constitute the MESH subscribers, and wherein a non-MESH capable mobile communication device (STA), such as for example a WLAN station, can register on this subnetwork (MESH) as a non-MESH subscriber, wherein

   a) a registering MAC address (MACA) is transmitted to the subnetwork (MESH) by a non-MESH capable mobile communication device (MP-A) registering on this subnetwork (MESH) as a non-MESH subscriber,
   b) a check is carried out such that the registering MAC address (MACA) is compared with the MAC addresses (MAC1, MAC2) accessible within the subnetwork (MESH), wherein during the check a route request message is emitted with a destination-only flag for the communication device with the registering MAC address,
   c) in the case that the registering MAC address (MACA) is disjunct to the MAC addresses (MAC1, MAC2) accessible within the subnetwork (MESH), the registering communication device (MP-A) is connected as a station of the subnetwork (MESH),
   d) in the case that the registering MAC address (MACA) is already accessible in the subnetwork (MESH), an approval procedure is performed such that use of the registering MAC address (MACA) by two different communication devices within the subnetwork (MESH) is prohibited.

2. Method according to claim 1, **characterised in that** as an approval procedure, the registering communication device (MP-A) is rejected.

3. Method according to claim 1, **characterised in that** as an approval procedure, the registering MAC address (MACA) is converted such that within the subnetwork (MESH), a MAC address disjunct to the accessible MAC address (MAC1, MAC2) is allocated to the registering communication device (MP-A).

4. Method according to claim 3, **characterised in that** the disjunct MAC address is generated by the subnetwork MESH.

5. Method according to claim 4, **characterised in that** the disjunct MAC address is generated on the basis of a pseudo-random sequence, in particular a "Number used once, nonce" generated precisely once.

6. Method according to any one of claims 3 to 5, **characterised in that** the disjunct MAC address is also selected disjunct to MAC addresses allocated globally, in particular by organisations such as in accordance with OUI (organisationally unique identifier).

7. Method according to any one of the preceding claims, **characterised in that** bit 41 of the disjunct MAC address is filled with the value "1".

8. Method according to claim 1, **characterised in that** as an approval procedure, the subnetwork MESH performs a check of the identity of the registering communication device (MP-A) with the specific first communication device (MP-1, MP-2) via the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA).

9. Method according to claim 8, **characterised in that** for the identity check:

   a) the subnetwork MESH transmits a first check information to the first communication device (MP-1, MP2) via a route of the subnetwork (MESH) established for the specific communication device (MP-1, MP-2) for the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA),
   b) the subnetwork (MESH) transmits a request for return of the first check information to the first communication device (MP1, MP2),
   c) the subnetwork (MESH) awaits the return of the first check information via a route of the subnetwork (MESH) established during the registration attempt of the registering communication device (MP-A),
   d) in the absence of the return, the registering communication device (MP-A) is rejected,
   e) on reception of the return, the correlation of the first check information with the returned check information is checked,
   f) in the case of reaching an established correlation degree, in particular on identity, of the first check information with the returned check information, the registering communication device (MP-A) is connected as a station of the subnetwork (MESH), otherwise the registering communication device is rejected.

10. Method according to claim 8, **characterised in that** for the identity check

Samsung Ex. 1004, Page 149 of 563

a) the subnetwork (MESH) transmits a first check information to the first communication device (MP-1, MP-2) via a route of the subnetwork (MESH) established during the registration attempt by the registering communication device (MP-A),
b) the subnetwork (MESH) transmits a request for return of the first check information to the first communication device (MP-1, MP-2),
c) the subnetwork (MESH) awaits the return of the first test information via route of the subnetwork (MESH) established for the specific communication device (MP-1, MP-2) for the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA),
d) in the absence of the return, the registering communication device (MP-A) is rejected,
e) on reception of the return, in this case the correlation of the first check information with the returned check information is checked,
f) in the case of reaching an established correlation degree, in particular on identity, of the first check information with the returned check information, the registering communication device (MP-A) is connected as a station of the subnetwork (MESH), otherwise the registering communication device is rejected.

11. Method according to claim 8, **characterised in that** for the identity check

a) the subnetwork (MESH) awaits a second test information via a route of the subnetwork (MESH) established for the specific communication device (MP-1, MP-2) for the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA), and a third test information via a route of the subnetwork (MESH) established during the registration attempt by the registering station at the first communication device (MP-1, MP-2),
b) in the absence of the second and/or third check information, the registering communication device (MP-A) is rejected,
c) in the case of reception of the second and third check information, the correlation of the second check information with the third check information is checked,
d) in the case of reaching an established correlation degree, in particular on identity, of the second check information with the third check information, the registering communication device (MP-A) is connected as the station of the subnetwork (MESH), otherwise the registering communication device is rejected.

12. Method according to claim 11, **characterised in that** the transmission of the second and/or third check information is initiated by the subnetwork (MESH).

13. Method according to claim 11, **characterised in that** the transmission of the second and/or third check information is initiated by the registering communication device (MP-A).

14. Method according to claim 8, **characterised in that** for the identity check

a) a fourth check information calculated by the registering communication device (MP-A) on the basis of a first cryptographic key authenticating the registering communication device (MP-A), in particular a first session key available to the registering communication device (MP-A) and resulting from a network registration according to the so-called extensible authentication protocol EAP, is transmitted to the subnetwork (MESH) via a route of the subnetwork (MESH) established during the registration attempt of the registering station,
b) the subnetwork (MESH) makes a decryption attempt using a second cryptographic key authenticating this specific communication device (MP-1, MP-2) by the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA), in particular a second session key available to the subnetwork (MESH) and resulting from a network registration according to the "Extensible authentication protocol EAP".
c) on successful decryption, the registering communication device (MP-A) is connected as a station of the subnetwork (MESH), otherwise the registering communication device is rejected.

15. Method according to claim 8, **characterised in that** for the identity check

a) a fifth check information calculated by a cryptographic key authenticating the specific first communication device (MP-1, MP-2) by the accessible MAC address (MAC1, MAC2) corresponding to the registering MAC address (MACA), in particular a first session key available to the registering communication device (MP-A) and resulting from a network registration according to the so-called "Extensible authentication protocol EAP", is transmitted to the subnetwork (MESH) via an established route of the registering communication device (MP-A),
b) the subnetwork (MESH) makes a decryption attempt using a second cryptographic key authenticating the registering communication device (MP-A), in particular a second session key available to the subnetwork (MESH) and resulting from a network registration according to the

Samsung Ex. 1004, Page 150 of 563

"Extensible authentication protocol EAP".
c) on successful decryption, the registering communication device (MP-A) is connected as a station of the subnetwork (MESH), otherwise the registering communication device is rejected.

16. Method according to any one of the preceding claims, **characterised in that** the first and/or second session key is generated as a "Master session key MSK" for according to the "Extensible authentication protocol EAP".

17. Method according to any one of the preceding claims, **characterised in that** the first and/or second session key is generated as an "Extended master session key EMSK" formed according to the "Extensible authentication protocol EAP".

18. Method according to any one of the preceding claims, **characterised in that** to calculate the first, second, third, fourth, and/or fifth check information, a function is used according to a cryptographic hash function, in particular SHA-1, SHA256 or MD5.

19. Method according to claim 18, **characterised in that** calculate the first, second, third, fourth and/or fifth check information, "Keyed hash functions" are used, in particular AES-CBC-MAC, HMAC-SHA1, HMAC-SHA256 or HMAC-MD5, wherein the HMAC function is defined according to RFC2104.

20. Method according to any one of the preceding claims, **characterised in that** the first, second, third, fourth and/or fifth check information is generated as a value, in particular as a pseudo-random code such as for example a "nonce".

21. Method according to any one of the preceding claims, **characterised in that** as the first, second, third, fourth and/or fifth check information, a hash code is transmitted which is produced from a value generated in particular as a pseudo-random code, such as for example a "nonce".

22. Method according to any one of the preceding claims, **characterised in that** as the first, second, third, fourth and/or fifth check information, a hash code is transmitted which is generated from an operating parameter of the registering communication device (MP-A) and/or first communication device.

23. Arrangement for provision of a wireless local network in which stationary communication devices (AP) designed according to standard IEEE 802.11 and its derivatives, in particular IEEE 802.15 or IEEE 802.16, and mobile communication devices (MAP, MP) are connected together in the manner of the mesh as a subnetwork, wherein all mobile communication devices (MAP, MP) which belong to a subnetwork (MESH) formed from MESH nodes (MAP, MP) constitute the MESH subscribers, and wherein a non-MESH capable mobile communication device (STA), such as for example a WLAN station, can register on this subnetwork (MESH) as a non-MESH subscriber, wherein

a) a transmission device is present by means of which a registering MAC address (MACA) is transmitted to the subnetwork (MESH) by a non-MESH capable mobile communication device (MP-A) registering on this subnetwork (MESH) as a non-MESH subscriber,
b) a check device is present, by means of which a check is carried out such that the registering MAC address (MACA) is compared with the MAC addresses (MAC1, MAC2) accessible within the subnetwork (MESH), wherein during the check a route request message is emitted with a destination-only flag for the communication device with the registering MAC address,
c) in the case that the registering MAC address (MACA) is disjunct to the MAC addresses (MAC1, MAC2) accessible within the subnetwork (MESH), the registering communication device (MP-A) is connected as a station of the subnetwork (MESH),
d) in the case that the registering MAC address (MACA) is already accessible in the subnetwork (MESH), an approval procedure is performed such that use of the registering MAC address (MACA) by two different communication devices within the subnetwork (MESH) is prohibited.

Revendications

1. Procédé de mise à disposition d'un réseau local sans fil, dans lequel des installations de communication stationnaires, AP, ainsi que des installations de communication mobiles (MAP, MP), équipées selon la norme IEEE 802.11 et ses dérivées, en particulier IEEE 802.15 ou IEEE 802.16, sont connectées sous forme d'un sous-réseau de type maillé, toutes les installations de communication mobiles (MAP, MP), qui font partie d'un sous-réseau (MESH) formé par des noeuds de réseau maillé (MAP, MP), formant les participants du réseau maillé (MESH) et une installation de communication mobile (STA) non compatible avec un réseau maillé, par exemple une station WLAN, pouvant s'inscrire à ce sous-réseau (MESH) en tant que non-participant du réseau maillé,

a) une adresse MAC d'inscription (MACA) étant communiquée au sous-réseau (MESH) de la part d'une installation de communication mobile

Samsung Ex. 1004, Page 151 of 563

(MP-A), non compatible avec un réseau maillé, s'inscrivant auprès de ce sous-réseau (MESH) en tant que non-participant du réseau maillé,
b) une vérification étant effectuée de sorte que l'adresse MAC d'inscription (MACA) soit comparée avec les adresses MAC (MAC1, MAC2) accessibles à l'intérieur du sous-réseau (MESH) ; lors de la vérification, un message de demande de route avec un drapeau « Uniquement destination » étant envoyé à l'installation de communication ayant l'adresse MAC d'inscription,
c) dans le cas où l'adresse MAC d'inscription (MACA) est disjointe des adresses MAC (MAC1, MAC2) accessibles à l'intérieur du sous-réseau (MESH), l'installation de communication s'inscrivant (MP-A) étant connectée en tant que station du sous-réseau (MESH),
d) dans le cas où l'adresse MAC d'inscription (MAC-A) est déjà accessible dans le sous-réseau (MESH), une procédure d'autorisation étant effectuée de manière telle qu'une utilisation de l'adresse MAC d'inscription (MACA) par deux installations de communication différentes à l'intérieur du sous-réseau (MESH) soit empêchée.

2. Procédé selon la revendication 1, **caractérisé en ce qu'**un rejet de l'installation de communication s'inscrivant (MP-A) a lieu en tant que procédure d'autorisation.

3. Procédé selon la revendication 1, **caractérisé en ce que**, en tant que procédure d'autorisation, a lieu une conversion de l'adresse MAC d'inscription (MACA) de manière telle que, à l'intérieur du sous-réseau (MESH), une adresse MAC disjointe des adresses MAC accessibles (MAC1, MAC2) soit attribuée à l'installation de communication s'inscrivant (MP-A).

4. Procédé selon la revendication 3, **caractérisé en ce que** l'adresse MAC disjointe est générée du côté du sous-réseau (MESH).

5. Procédé selon la revendication 4, **caractérisé en ce que** l'adresse MAC disjointe est générée sur la base d'une suite pseudo aléatoire - en particulier d'un nombre généré précisément une seule et unique fois (« Number Used Once, Nonce »).

6. Procédé selon l'une quelconque des revendications 3 à 5, **caractérisé en ce que** l'adresse MAC disjointe est sélectionnée également disjointe d'adresses MAC attribuées mondialement - en particulier de la part d'organisations telles que OUI (« Organizationally Unique Identifier »).

7. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le bit 41 de l'adresse MAC disjointe est occupé par la valeur « 1 ».

8. Procédé selon la revendication 1, **caractérisé en ce que**, en tant que procédure d'autorisation, a lieu du côté du sous-réseau (MESH) un contrôle de l'identité de l'installation de communication s'inscrivant (MP-A) avec la première installation de communication (MP-1, MP-2) déterminée - par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA).

9. Procédé selon la revendication 8, **caractérisé en ce que**, pour le contrôle d'identité,

a) du côté du sous-réseau (MESH) est communiquée à la première installation de communication (MP-1, MP-2) une première information de contrôle sur une route du sous-réseau (MESH) établie vers l'installation de communication (MP-1, MP-2) déterminée - par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA),
b) le sous-réseau (MESH) communique à la première installation de communication (MP-1, MP-2) une demande de renvoi de la première information de contrôle,
c) le sous-réseau (MESH) attend le renvoi de la première information de contrôle sur une route du sous-réseau (MESH) établie dans le cadre de la tentative d'inscription de l'installation de communication s'inscrivant (MP-A),
d) en cas d'absence du renvoi a lieu un rejet de l'installation de communication s'inscrivant (MP-A),
e) en cas d'arrivée du renvoi, la corrélation de la première information de contrôle avec l'information de contrôle renvoyée est vérifiée,
f) dans le cas de l'obtention d'un degré de corrélation défini - en particulier lors de l'identité - de la première information de contrôle par rapport à l'information de contrôle renvoyée, l'installation de communication s'inscrivant (MP-A) est connectée en tant que station du sous-réseau (MESH), sinon a lieu un rejet de l'installation de communication s'inscrivant.

10. Procédé selon la revendication 8, **caractérisé en ce que**, pour le contrôle d'identité,

a) du côté du sous-réseau (MESH) est communiquée à la première installation de communication (MP-1, MP-2) une première information de contrôle sur une route du sous-réseau (MESH) établie dans le cadre de la tentative d'inscription de l'installation de communication s'inscrivant (MP-A),

Samsung Ex. 1004, Page 152 of 563

b) le sous-réseau (MESH) communique à la première installation de communication (MP-1, MP-2) une demande de renvoi de la première information de contrôle,
c) le sous-réseau (MESH) attend le renvoi de la première information de contrôle sur une route du sous-réseau (MESH) établie vers l'installation de communication (MP-1, MP-2) déterminée - par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA),
d) en cas d'absence du renvoi a lieu un rejet de l'installation de communication s'inscrivant (MP-A),
e) en cas d'arrivée du renvoi, la corrélation de la première information de contrôle avec l'information de contrôle renvoyée est vérifiée,
f) dans le cas de l'obtention d'un degré de corrélation défini - en particulier lors de l'identité - de la première information de contrôle par rapport à l'information de contrôle renvoyée, l'installation de communication s'inscrivant (MP-A) est connectée en tant que station du sous-réseau (MESH), sinon a lieu un rejet de l'installation de communication s'inscrivant.

11. Procédé selon la revendication 8, **caractérisé en ce que**, pour le contrôle d'identité,

a) du côté du sous-réseau (MESH), une deuxième information de contrôle sur une route du sous-réseau (MESH) établie vers l'installation de communication (MP-1, MP-2) déterminée - par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA) - ainsi qu'une troisième information de contrôle sur une route du sous-réseau (MESH) établie dans le cadre de la tentative d'inscription de la station s'inscrivant sont attendues à la première installation de communication (MP-1, MP-2),
b) en cas d'absence de la deuxième et/ou de la troisième information de contrôle a lieu un rejet de l'installation de communication s'inscrivant (MP-A),
c) dans le cas de l'arrivée de la deuxième et de la troisième information de contrôle, la corrélation de la deuxième information de contrôle avec la troisième information de contrôle est vérifiée,
d) dans le cas de l'obtention d'un degré de corrélation défini - en particulier lors de l'identité - de la deuxième information de contrôle par rapport à la troisième information de contrôle, l'installation de communication s'inscrivant (MP-A) est connectée en tant que station du sous-réseau (MESH), sinon a lieu un rejet de l'installation de communication s'inscrivant.

12. Procédé selon la revendication 11, **caractérisé en ce que** la transmission de la deuxième et/ou de la troisième information de contrôle est lancée du côté du sous-réseau (MESH).

13. Procédé selon la revendication 11, **caractérisé en ce que** la transmission de la deuxième et/ou de la troisième information de contrôle est lancée du côté de l'installation de communication s'inscrivant (MP-A).

14. Procédé selon la revendication 8, **caractérisé en ce que**, pour le contrôle d'identité,

a) une quatrième information de contrôle sur une route du sous-réseau (MESH) établie dans le cadre de la tentative d'inscription de la station s'inscrivant, calculée du côté de l'installation de communication s'inscrivant (MP-A) sur la base d'une première clé cryptographique authentifiant l'installation de communication s'inscrivant (MP-A) - en particulier d'une première clé de session disponible à l'installation de communication s'inscrivant (MP-A) et résultant d'une inscription au réseau selon le protocole dit EAP (« Extensible Authentication Protocol ») - est transmise au sous-réseau (MESH),
b) un essai de déchiffrage est effectué du côté du sous-réseau (MESH) à l'aide d'une clé sur la base d'une deuxième clé cryptographique - en particulier d'une deuxième clé de session disponible à l'installation de communication s'inscrivant (MP-A) et résultant d'une inscription au réseau selon le protocole dit EAP (« Extensible Authentication Protocol ») - authentifiant - l'installation de communication (MP-1, MP-2) déterminée par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA),
c) en cas de déchiffrage réussi, l'installation de communication s'inscrivant (MP-A) est connectée en tant que station du sous-réseau (MESH), sinon a lieu un rejet de l'installation de communication s'inscrivant.

15. Procédé selon la revendication 8, **caractérisé en ce que**, pour le contrôle d'identité,

a) une cinquième information de contrôle sur une route établie de l'installation de communication s'inscrivant (MP-A) est communiquée au sous-réseau (MESH) de la part d'une clé cryptographique - en particulier d'une première clé de session disponible à l'installation de communication s'inscrivant (MP-A), résultant d'une inscription au réseau selon le protocole dit EAP (« Extensible Authentication Protocol ») - authentifiant la première installation de commu-

Samsung Ex. 1004, Page 153 of 563

nication (MP-1, MP-2) déterminée par les adresses MAC (MAC1, MAC2) accessibles correspondant à l'adresse MAC d'inscription (MACA),
b) un essai de déchiffrement est effectué du côté du sous-réseau (MESH) à l'aide d'une clé sur la base d'une deuxième clé de chiffrement - en particulier d'une deuxième clé de session disponible à l'installation de communication s'inscrivant (MP-A), résultant d'une inscription au réseau selon le protocole d'authentification extensible dit EAP (de l'anglais « Extensible Authentication Protocol ») - authentifiant l'installation de communication s'inscrivant (MP-A),
c) en cas de déchiffrement réussi, l'installation de communication s'inscrivant (MP-A) est connectée en tant que station du sous-réseau (MESH), sinon a lieu un rejet de l'installation de communication s'inscrivant.

16. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** la première et/ou la deuxième clé de session est générée en tant que clé de session maître (MSK, « Master Session Key ») selon le protocole EPA (protocole d'authentification extensible, de l'anglais « Extensible Authentication Protocol »).

17. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** la première et/ou la deuxième clé de session est générée en tant que clé de session maître étendue (EMSK, « Extended Master Session Key ») selon le protocole EPA (protocole d'authentification extensible, de l'anglais « Extensible Authentication Protocol »).

18. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que**, pour le calcul des première, deuxième, troisième, quatrième et/ou cinquième informations de contrôle, on emploie une fonction conforme à une fonction de hachage cryptographique - en particulier SHA1, SHA256 ou MD5.

19. Procédé selon la revendication 18, **caractérisé en ce que**, pour le calcul des première, deuxième, troisième, quatrième et/ou cinquième informations de contrôle, on emploie des fonctions de hachage codées (« Keyed-Hash ») - en particulier AES-CBC-MAC, HMAC-SHA1, HMAC-SHA256 ou HMAC-MD5, la fonction HMAC étant définie selon RFC2104.

20. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les première, deuxième, troisième, quatrième et/ou cinquième informations de contrôle sont générées sous forme d'une valeur - en particulier sous forme d'un code pseudo aléatoire, par exemple « Nonce ».

21. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que**, en tant que première, deuxième, troisième, quatrième et/ou cinquième informations de contrôle, on transmet un code de hachage généré d'après une valeur générée - en particulier en tant que code pseudo aléatoire, par exemple « Nonce ».

22. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que**, en tant que première, deuxième, troisième, quatrième et/ou cinquième informations de contrôle, on communique un code de hachage généré d'après un paramètre de fonctionnement de l'installation de communication s'inscrivant (MP-A) et/ou de la première installation de communication.

23. Structure de mise à disposition d'un réseau local sans fil, dans laquelle des installations de communication stationnaires, AP, ainsi que des installations de communication mobiles (MAP, MP), équipées selon la norme IEEE 802.11 et ses dérivées, en particulier IEEE 802.15 ou IEEE 802.16, sont connectées sous forme d'un sous-réseau de type maillé, toutes les installations de communication mobiles (MAP, MP), qui font partie d'un sous-réseau (MESH) formé par des noeuds de réseau maillé (MAP, MP), formant les participants du réseau maillé et une installation de communication mobile (STA) non compatible avec un réseau maillé, par exemple une station WLAN, pouvant s'inscrire à ce sous-réseau (MESH) en tant que non-participant du réseau maillé,
dans laquelle

a) est présent un dispositif de transmission par le biais duquel une adresse MAC d'inscription (MACA) est transmise au sous-réseau (MESH) de la part d'une installation de communication mobile (MP-A), non compatible avec le réseau maillé, s'inscrivant auprès de ce sous-réseau (MESH) en tant que non-participant du réseau maillé,
b) est présent un dispositif de vérification par le biais duquel une vérification est effectuée de manière telle que l'adresse MAC d'inscription (MACA) soit comparée avec les adresses MAC (MAC1, MAC2) accessibles à l'intérieur du sous-réseau (MESH), sachant qu'au cours de la vérification est envoyé un message de demande de route avec un drapeau « Uniquement destination » pour l'installation de communication ayant l'adresse MAC d'inscription,
sachant que par le dispositif de vérification,
c) dans le cas où l'adresse MAC d'inscription (MACA) est disjointe des adresses MAC (MAC1, MAC2) accessibles à l'intérieur du sous-réseau (MESH), l'installation de communication s'inscrivant (MP-A) est connectée en

Samsung Ex. 1004, Page 154 of 563

tant que station du sous-réseau (MESH),
d) dans le cas où l'adresse MAC d'inscription (MACA) est déjà accessible dans le sous-réseau (MESH), une procédure d'autorisation est effectuée de manière telle qu'une utilisation de l'adresse MAC d'inscription (MACA) par deux installations de communication différentes soit empêchée à l'intérieur du sous-réseau (MESH).

Samsung Ex. 1004, Page 155 of 563

FIG 1

Stand der Technik

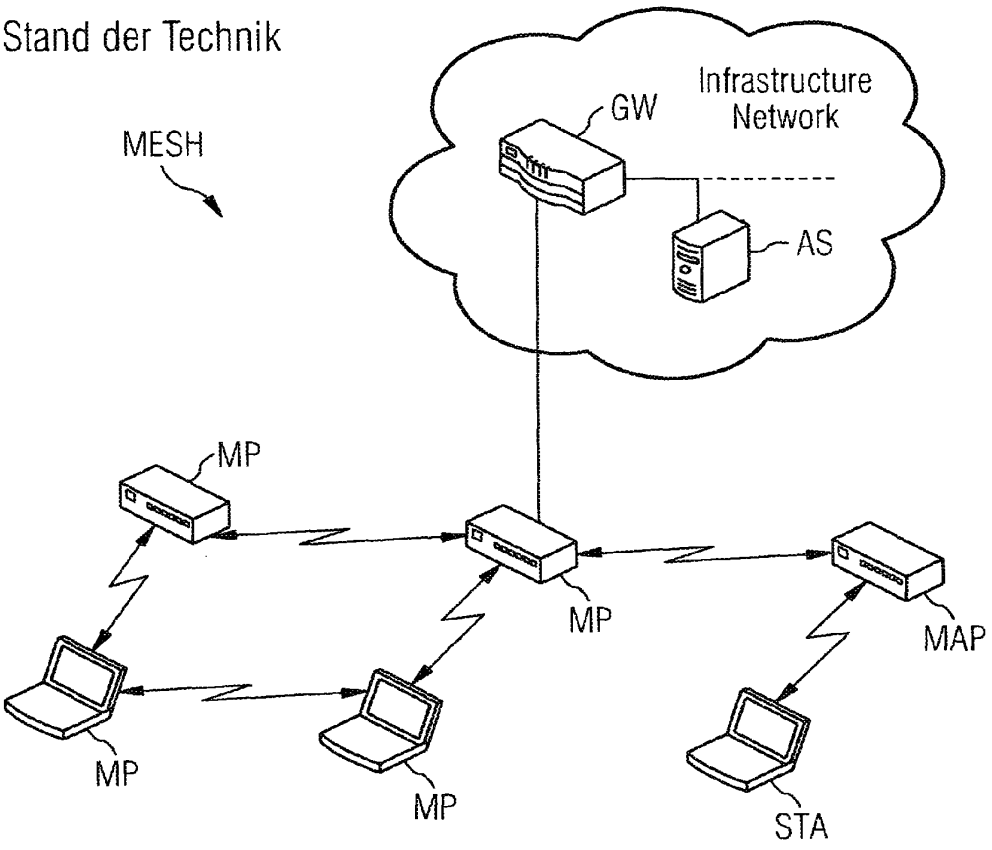


FIG 2
Stand der Technik

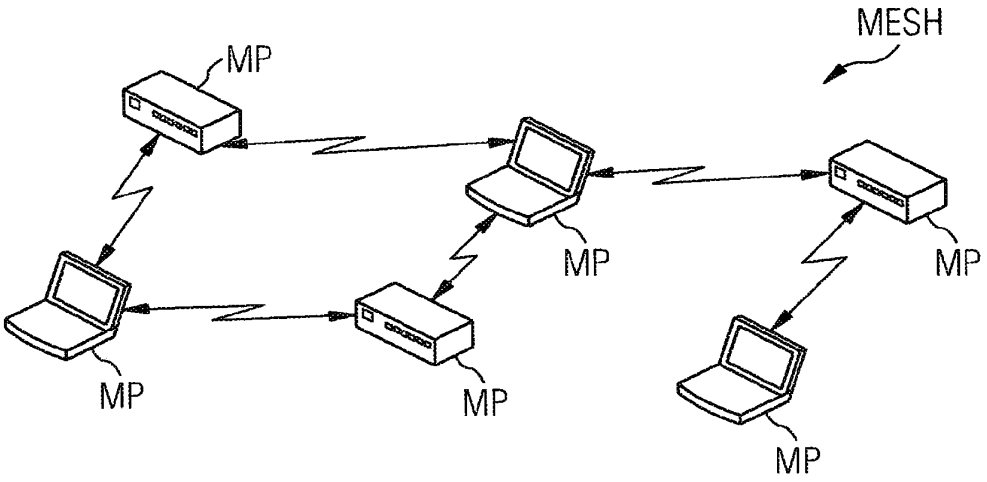


FIG 3
Stand der Technik

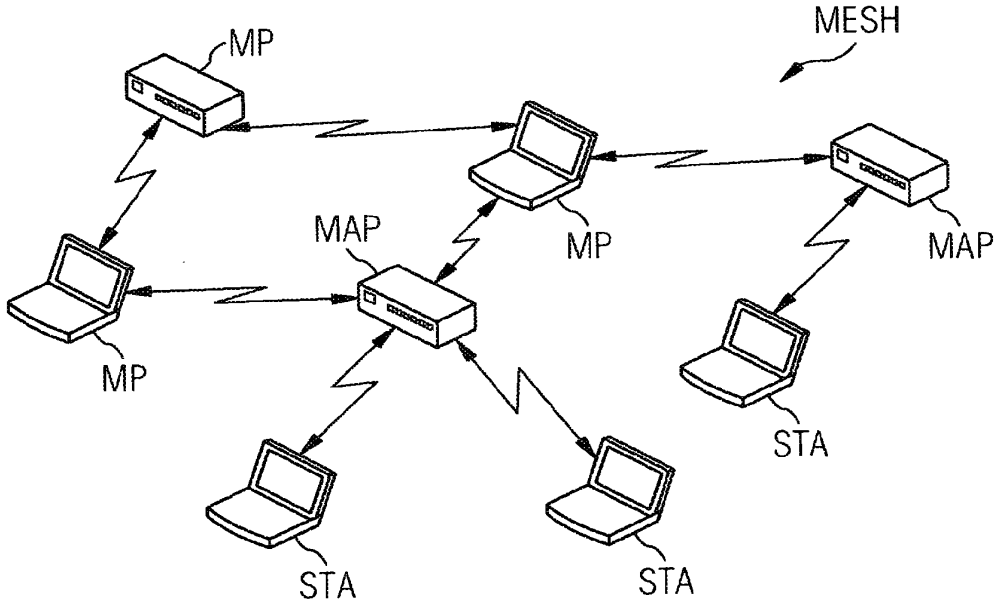


FIG 4
Stand der Technik

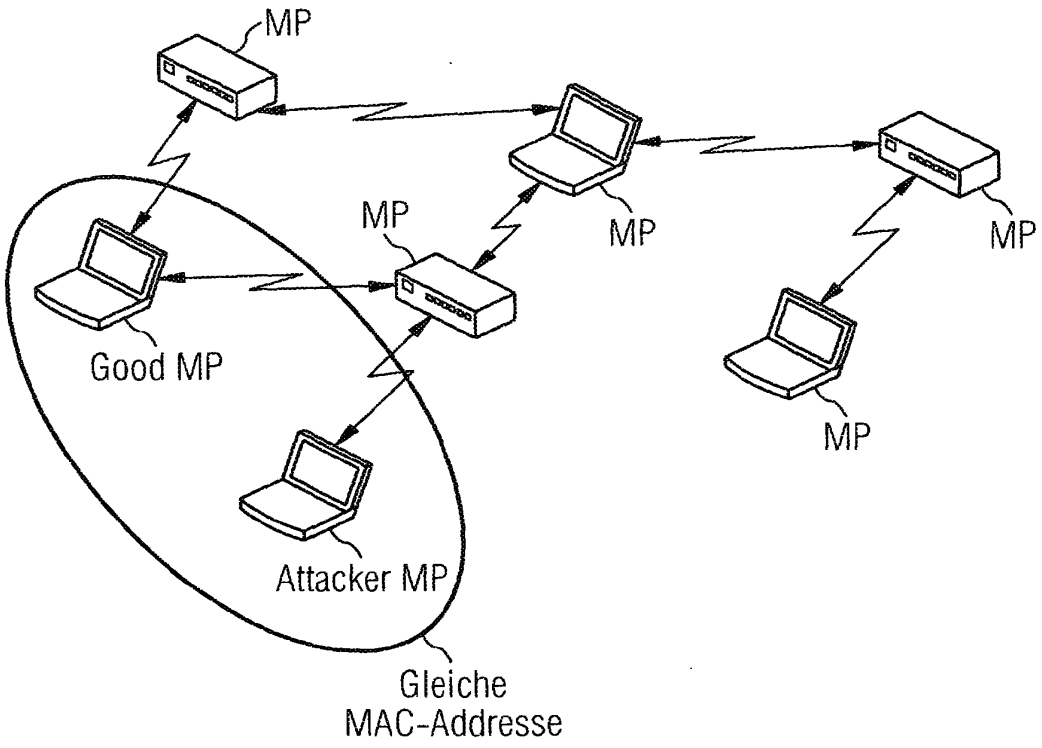


FIG 5

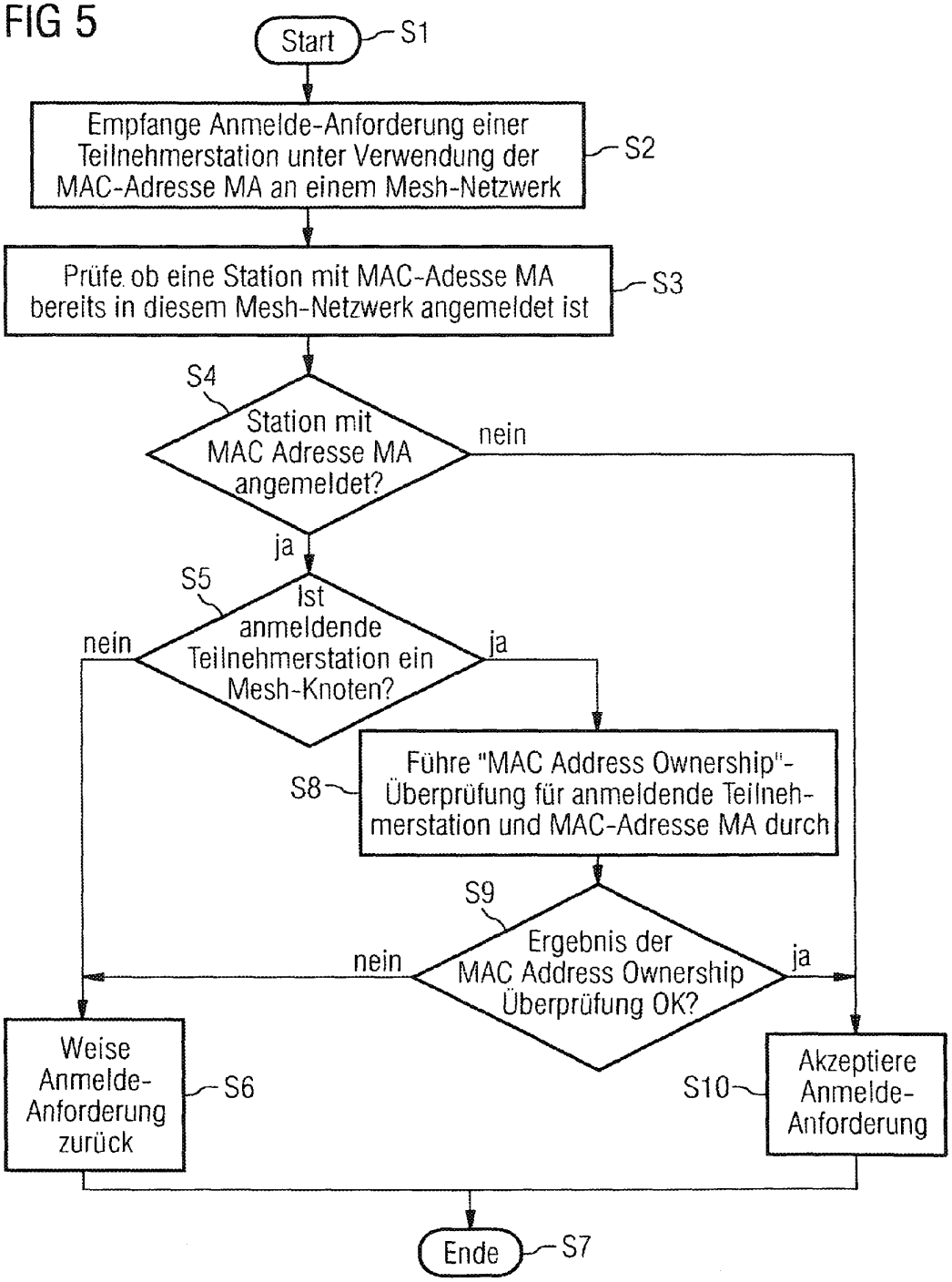

Start
S1
Empfange Anmelde-Anforderung einer Teilnehmerstation unter Verwendung der MAC-Adresse MA an einem Mesh-Netzwerk
S2
Prüfe ob eine Station mit MAC-Adesse MA bereits in diesem Mesh-Netzwerk angemeldet ist
S3
S4
Station mit MAC Adresse MA angemeldet?
nein
ja
S5
Ist anmeldende Teilnehmerstation ein Mesh-Knoten?
nein
ja
S8
Führe "MAC Address Ownership"-Überprüfung für anmeldende Teilnehmerstation und MAC-Adresse MA durch
S9
Ergebnis der MAC Address Ownership Überprüfung OK?
nein
ja
Weise Anmelde-Anforderung zurück
S6
S10
Akzeptiere Anmelde-Anforderung
Ende
S7

FIG 6

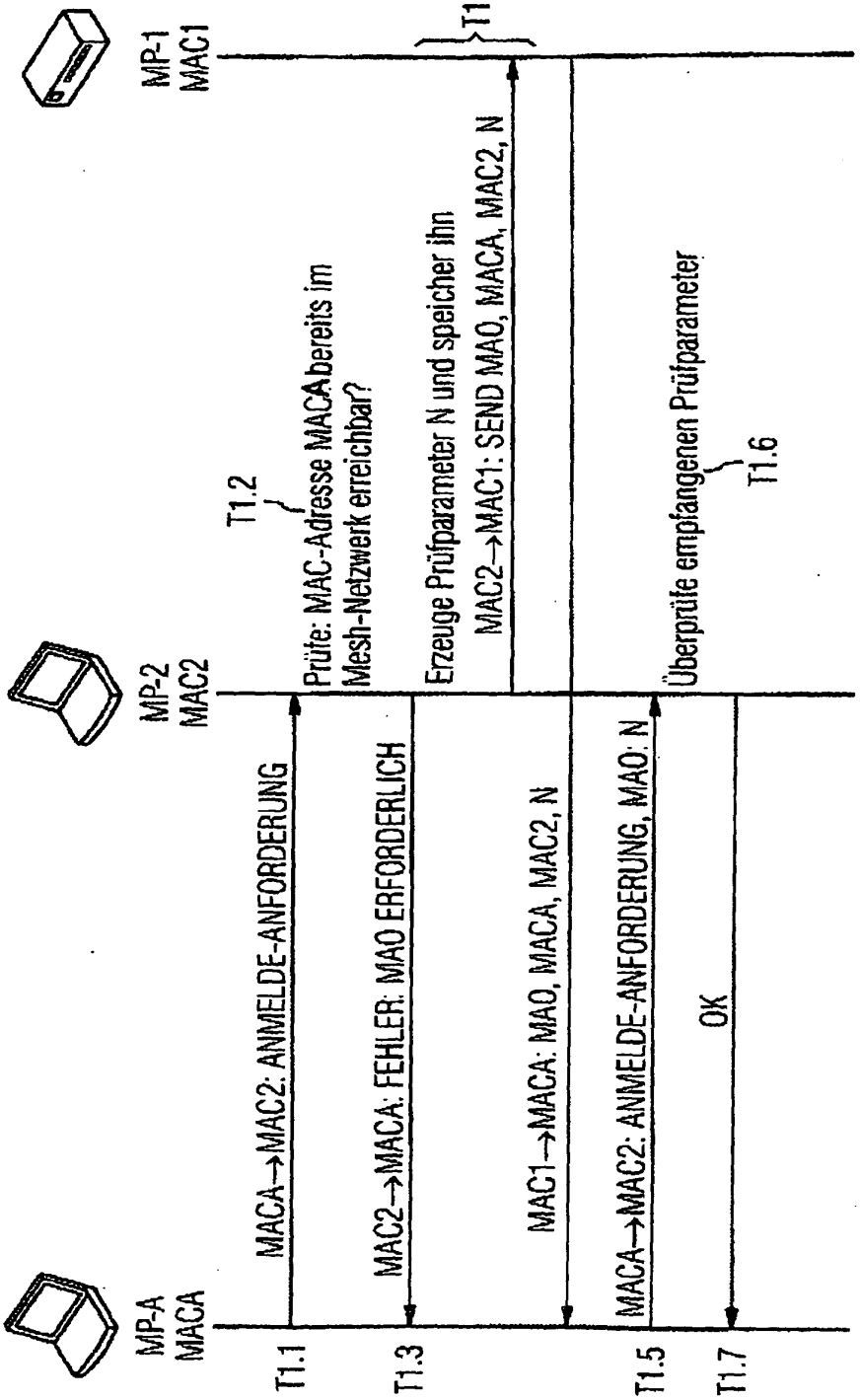
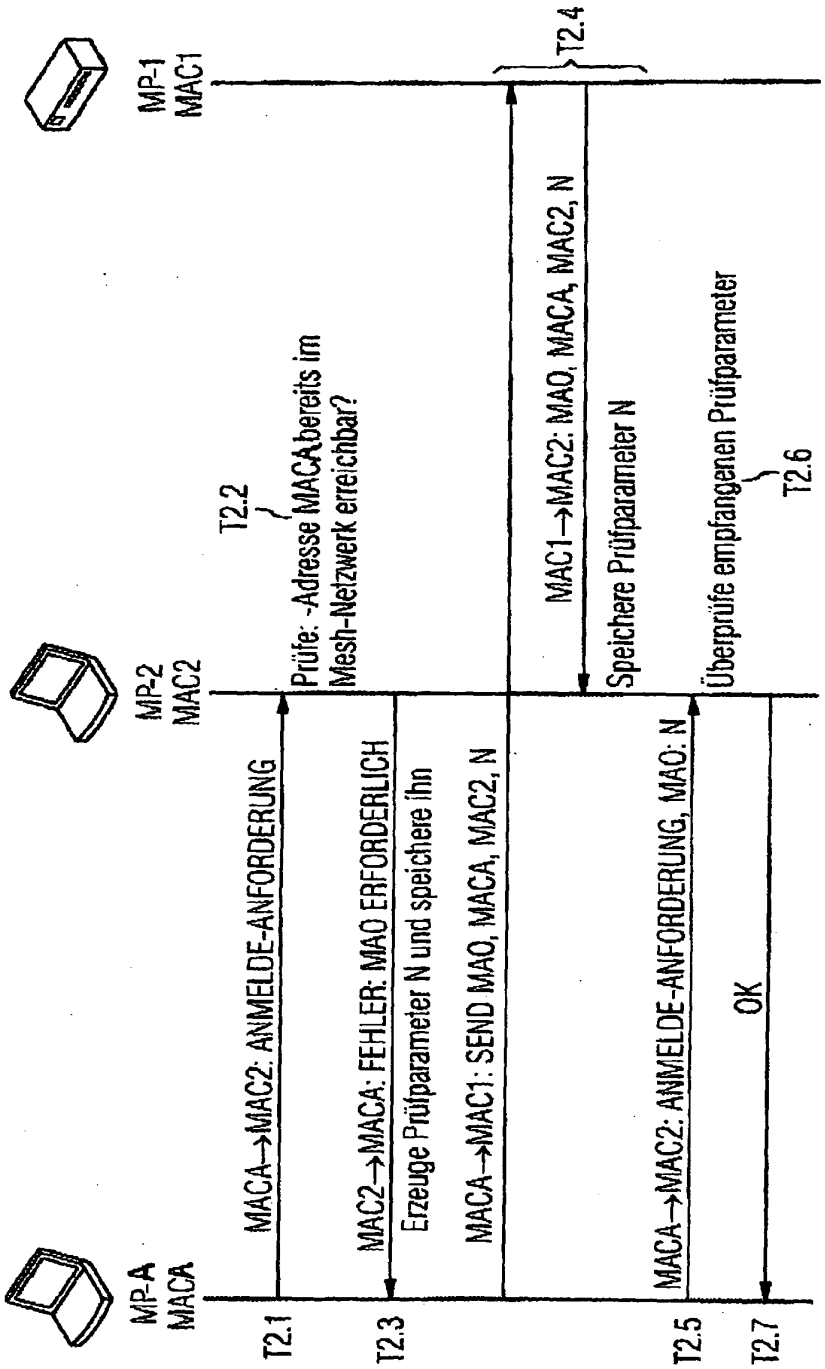
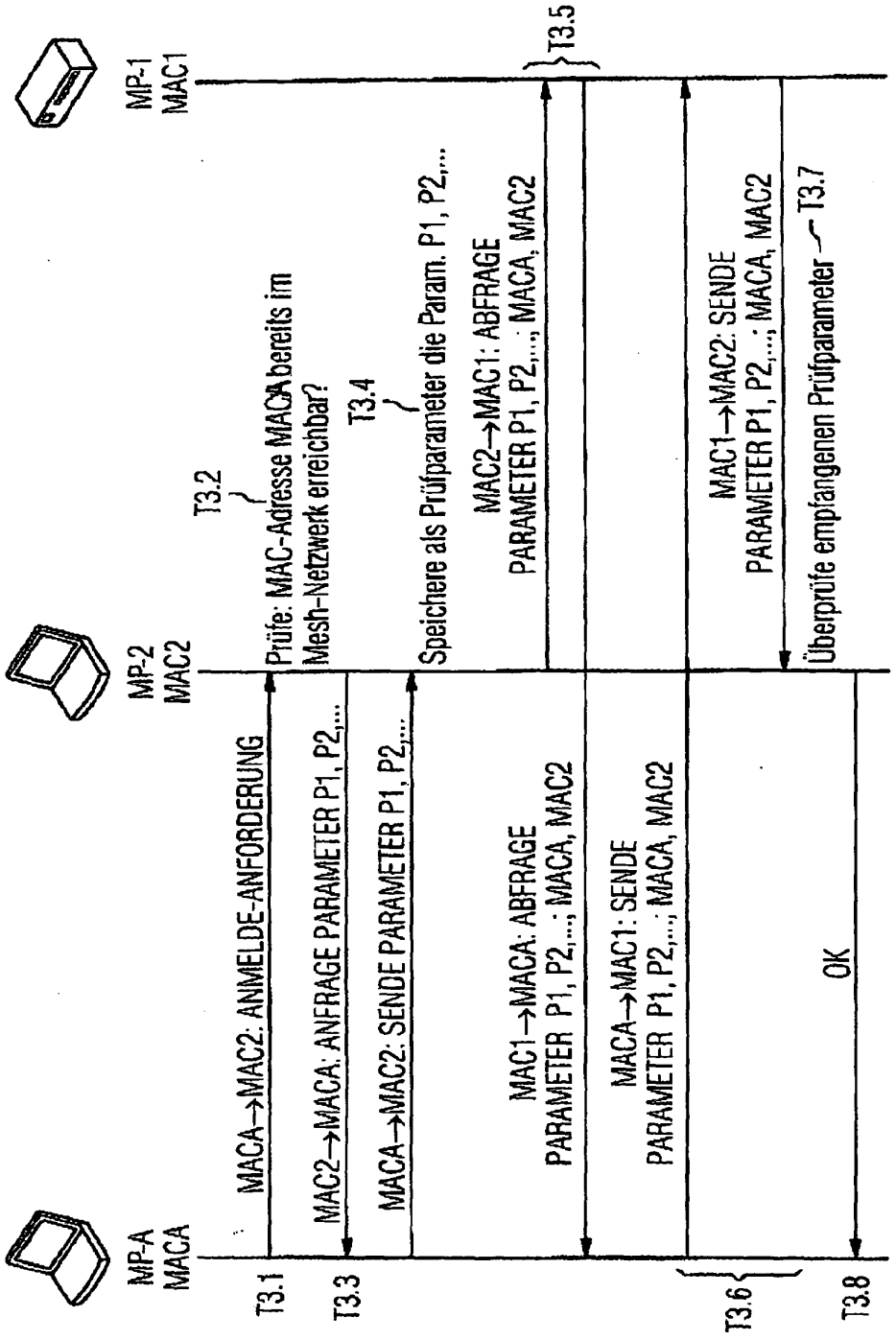

MP-A
MACA
MP-2
MAC2
MP-1
MAC1
T1.1
MACA→MAC2: ANMELDE-ANFORDERUNG
T1.2
Prüfe: MAC-Adresse MACA bereits im Mesh-Netzwerk erreichbar?
T1.3
MAC2→MACA: FEHLER: MAO ERFORDERLICH
Erzeuge Prüfparameter N und speicher ihn
T1.4
MAC2→MAC1: SEND MAO, MACA, MAC2, N
MAC1→MACA: MAO, MACA, MAC2, N
T1.5
MACA→MAC2: ANMELDE-ANFORDERUNG, MAO: N
Überprüfe empfangenen Prüfparameter
T1.6
OK
T1.7

FIG 7



Samsung Ex. 1004, Page 161 of 563

FIG 8



Samsung Ex. 1004, Page 162 of 563

FIG 9

Stand der Technik

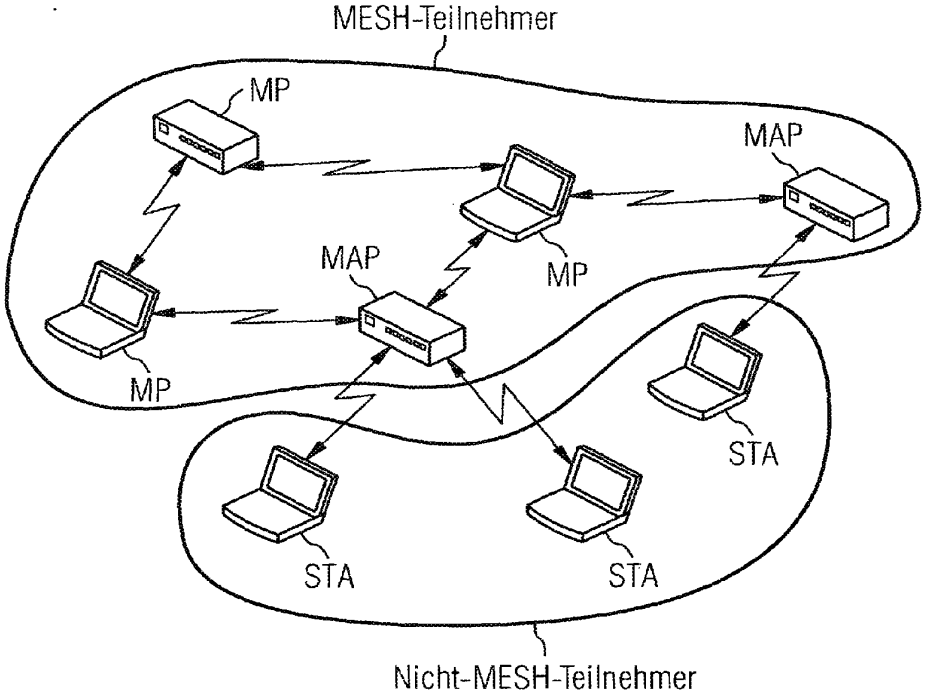


FIG 10

Stand der Technik

RA	TA	DA	SA	DATA	FCS

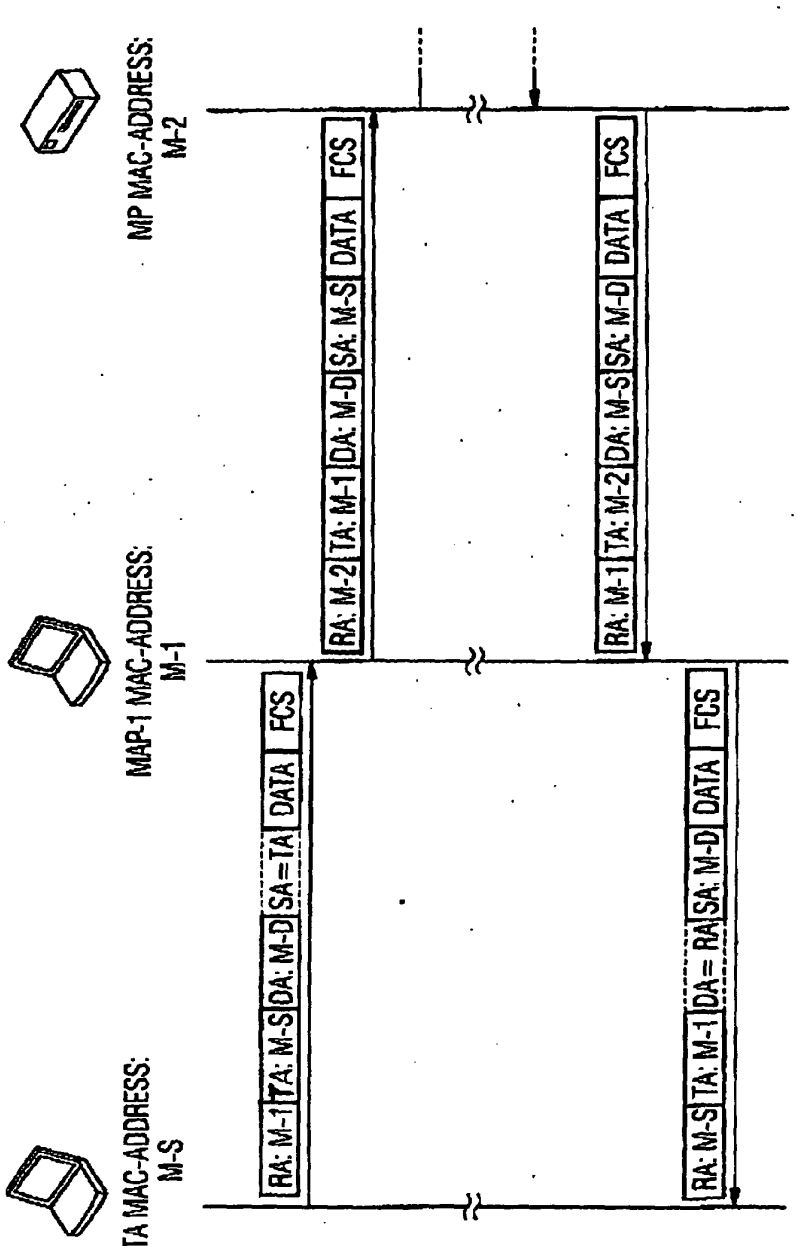
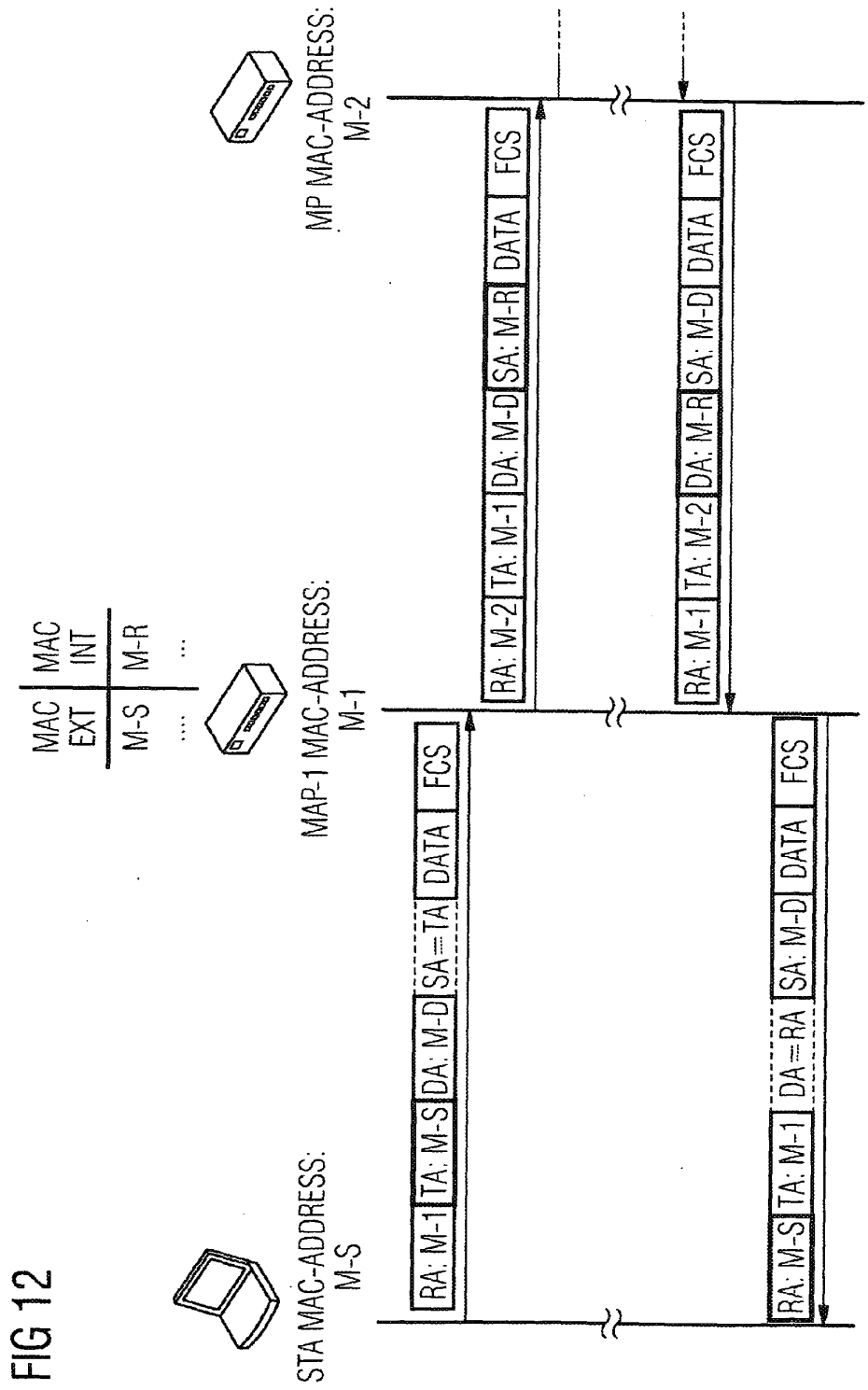


FIG 11 Stand der Technik

FIG 12


STA MAC-ADDRESS: M-S
MAP-1 MAC-ADDRESS: M-1
MP MAC-ADDRESS: M-2
MAC EXT
MAC INT
M-S
M-R
RA: M-1
TA: M-S
DA: M-D
SA=TA
DATA
FCS
RA: M-2
TA: M-1
DA: M-D
SA: M-R
DATA
FCS
RA: M-1
TA: M-2
DA: M-R
SA: M-D
DATA
FCS
RA: M-S
TA: M-1
DA=RA
SA: M-D
DATA
FCS

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- EP 1635528 A1 **[0013]**
- US 20040141468 A1 **[0013]**
- US 20060114863 A **[0014]**

Samsung Ex. 1004, Page 166 of 563

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 February 2014 (06.02.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/020407 A1

(51) International Patent Classification:
H04L 29/12 (2006.01) *H04W 76/02* (2009.01)

(21) International Application Number:
PCT/IB2013/001660

(22) International Filing Date:
30 July 2013 (30.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/677,079 30 July 2012 (30.07.2012) US

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **HUANG, Kaiyuan**; 603 March Road, Kanata, Ontario K2K 2M5 (CA). **RAYMENT, Stephen**; 1604-95 Bronson Avenue, Ottawa, Ontario K1R 1E2 (CA). **ROELAND, Dinand**; Skinnarasvagen 39, S-19275 Sollentuna (SE). **ROMMER, Stefan**; Skogsrydsgatan 7, S-42674 Vastra Frolunda (CA).

(74) Agent: **BAUER, Richard, P.**; Katten Muchin Rosenman LLP, 2900 K Street NW, Suite 200, North Tower, Washington, DC 20007-5118 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PROVIDING MULTIPLE SERVICES OVER WLAN

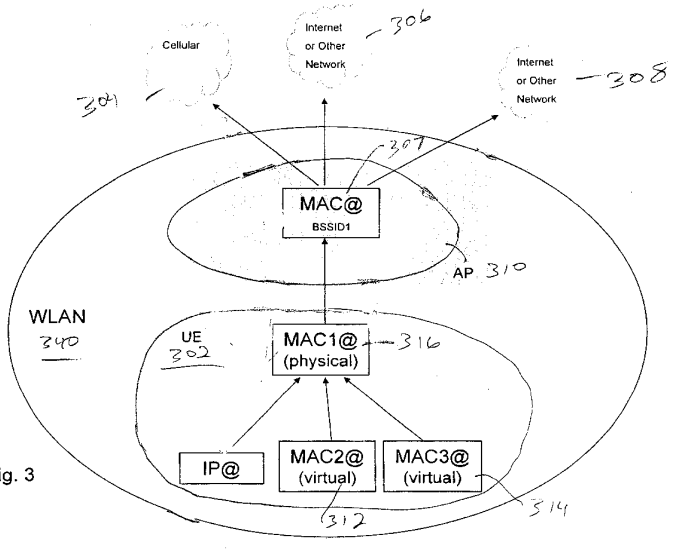


Fig. 3

(57) Abstract: A system and method of providing, to a client, access to multiple packet data networks (PDNs), each PDN providing a dedicated PDN connection is disclosed. The client is provided with a number of virtual MAC addresses. Each of the virtual MAC addresses is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the packet data networks. One of the virtual MAC addresses is then delivered via a 4 address MAC frame when the client is communicating with the associated data service. The client may be a Wi-Fi client communicating with the associated data service over a cellular data network.

WO 2014/020407 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND SYSTEM FOR PROVIDING MULTIPLE SERVICES OVER WLAN

[0001] This application claims priority to U.S. Provisional Patent Appln. No. 61/677,079, filed July 30, 2012, the contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present application relates generally to WLAN access to a cellular network, more specifically, to providing multiple virtual services over a WLAN interface.

BACKGROUND OF THE INVENTION

[0003] A need exists to provide multiple concurrent services over WLAN (Wireless Local Area Network). For example when WLAN is used to provide access to cellular data networks, it is desirable to provide access to multiple PDNs (Packet Data Networks). This capability is currently done on 3G/4G networks where, e.g., IMS (IP Multimedia Subsystem) and Internet access can be simultaneously provided. Each of these services is identified via their APNs (Access Point Name). It is the name of a network, where a network in 3GPP terminology is called Packet Data Network (PDN). In the 3GPP core network, there is a gateway called PGW (Packet Data Network Gateway). This is a PDN GW; i.e. a gateway towards one or more PDNs. Between the UE (User Equipment; e.g., Wi-Fi client) and PGW(s) one or more "PDN connections" are setup. Each PDN connection is a virtual point-to-point link from a UE to a PDN. A UE initiates the setup of a PDN connection. When it does that, it may include an APN. Each PDN connection has one IP address. As each PDN may have its own IP address range, it can occur that two PDN connections to different PDNs get the same IP address. Herein, the term "PDN" may be used for a "PDN connection." Thus, the IP address spaces for each of the different services may overlap, making IP address resolution of the services impossible. What is needed is a means to provide multiple virtual point-to-point links between the device and one or more PDNs.

[0004] Other approaches have been proposed to solve this problem, including running VLANs (Virtual Local Area Networks, e.g., IEEE 802.1Q) over WLAN, and performing tunneling over WLAN (using e.g. GRE - Generic Routing Encapsulation). The approach described below is potentially simpler to implement than the alternatives, reducing device cost and power consumption and the basic frame structure is already implemented in some existing devices.

SUMMARY OF THE INVENTION

[0005] The present invention is directed to alleviating the problems of the prior art. In particular, the present invention proposes to use the IEEE 802.11 WDS (Wireless Distribution System) four-address frame format to segregate multiple virtual services over a single WLAN interface.

[0006] According to one aspect of the present invention, a method provides to a client access to multiple packet data network (PDN) connections – preferably over WLAN, each PDN providing a dedicated PDN connection (e.g., Skype, Netflix, etc.), a single PDN capable of providing multiple services. The client (e.g., User Equipment (UE) such as a cell phone) is provided with a number of virtual MAC (Media Access Control) addresses. Each of the virtual MAC addresses is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the PDNs. One of the virtual MAC addresses is then provided via a 4 address MAC frame for the client to communicate with the associated data service. When communicating with a data service via a PDN connection, the virtual MAC address associated with the PDN connection is then included in a 4 address MAC frame.

[0007] In a preferred embodiment, the client is a Wi-Fi client, and the Wi-Fi client is communicating with the associated data service over a cellular data network.

[0008] According to another aspect of the present invention, apparatus providing to a client, access to a plurality of PDNs, each PDN providing a dedicated PDN connection, includes an

Access Point (AP) configured to communicate with (i) the client and (ii) the plurality of PDNs. The AP may be configured to provide the client a plurality of virtual MAC addresses, and to assign each of the virtual MAC addresses to a dedicated PDN connection, where each dedicated PDN connection is associated with one of the PDNs. The AP is further configured to provide one of the virtual MAC addresses via a 4 address MAC frame for the client to communicate with the associated data service. In alternative embodiments, the virtual MAC addresses may be (i) pre-loaded onto the UE (User Equipment, e.g., a cell phone) as pre-configured global MACs (e.g., for each data service), (ii) administered by the network (fixed or 3GPP (3rd Generation Partnership Project) AAA (Authentication, Authorization and Accounting protocol)) and sent to UE at authentication, and/or (iii) negotiated dynamically when the UE needs it (e.g. based on ARP (Address Resolution Protocol)). In alternatives (ii) and (iii), the virtual MAC addresses may be supplied to the UE through the AP.

[0009] According to a further aspect of the present invention, at least one computer-readable, non-transitory medium is provided, which contains program code which, when loaded into one or more processors of an AP, causes the one or more processors to provide to a client access to a plurality of PDNs, where each PDN provides a dedicated PDN connection. The program code causes the one or more processors to provide the client a plurality of virtual Media Access Control (MAC) addresses; where each of the virtual MAC addresses corresponds to a dedicated PDN connection, each dedicated PDN connection being associated with one of the PDNs; and deliver one of the virtual MAC addresses via a 4 address MAC frame for the client to use when the client is communicating with the associated data service.

[0010] Other aspects and features of the present invention will become apparent to those of ordinary skill in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1a is a diagram illustrating the general 802.11 frame format;

[0012] Fig. 1b is a diagram illustrating the 802.11 frame format in accordance with the preferred embodiments;

[0013] Fig. 2 is a diagram illustrating a typical use of the known 802.11 address format frame in a wireless bridge;

[0014] Fig. 3 is a block diagram illustrating links between a UE and a Trusted WLAN Access Gateway (TWAG) according to an embodiment of the invention;

[0015] Fig. 4 is a is a schematic block diagram of the structure according to the preferred embodiments;

[0016] Fig. 5 is a functional flow chart illustrating how the four-address MAC header is used for communication between a UE and a PDN;

[0017] Fig. 6 is a flow chart of a preferred process according to the present invention;

[0018] Fig. 7 is a process diagram of an initial attachment in WLAN on GTP (GPRS Tunneling Protocol) S2a;

[0019] Fig. 8 is a process diagram of UE-Initiated connectivity to additional PDN in WLAN on GTP S2a;

[0020] Fig. 9 is a process diagram of a handover procedure between 3GPP access and WLAN on S2a;

[0021] Fig. 10 is a process diagram of a handover from WLAN on GTP S2a to 3GPP access;

[0022] Fig. 11 is a process diagram of a UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN;

[0023] Fig. 12 is a process diagram of a PDN GW Initiated Bearer Deactivation with GTP on S2a.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0024] In order to lighten the following description, the following acronyms will be used herein:

Table 1

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting protocol
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AP	Access Point
APN	Access Point Network
ARP	Address Resolution Protocol
BNG	Broadband Network Gateway
BSSID	Basic Service Set Identifier
DA	Destination Address
DHCP	Dynamic Host Control Protocol
EAP	Extendible Authentication Protocol

EPC	Evolved Packet Core
EPS	Evolved Packet System
FFS	For Further Study
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
hPCRF	Home network Policy Control and Charging Rules Function
HPLMN	Home Public Land Mobile Network
IMSI	International Mobile Subscriber Identity
IP-CAN	IP Connectivity Access Network
LBO	Local Breakout
MAC	Media Access Control
NSWO	Non Seamless WLAN Offload
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PMIPv6	Proxy Mobile IP version 6
QoS	Quality of Service
RA	Receiver Address
S2a	Trusted non-3GPP interface to EPC
SA	Source Address
SaMOG	S2a-based Mobility over GTP

SDO	Standard Development Organization
TA	Transmitter Address
TEID	Tunnel Endpoint ID
TWAG	Trusted WLAN Access Gateway
UE	User Equipment
vPCRF	Visited network Policy Control and Charging Rules Function
VPLMN	Visited Public Land Mobile Network
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network
WLCP	WLAN Control Protocol

[0025] In overview, the present invention proposes a solution for SaMOG (S2a-based Mobility over GTP) phase 2. For the first PDN connection, additional information elements are proposed to be added to EAP-AKA (Extendible Authentication Protocol - Authentication and Key Agreement). These information elements may carry e.g. handover indicator or APN. For additional PDN connections, traffic may be separated on a per-PDN connection basis using four MAC addresses in the 802.11 frame. A control protocol may be used to setup and teardown additional PDN connections.

[0026] Typically, the first PDN/NSWO (Non Seamless WLAN Offload) connection over WLAN uses the per-UE point-to-point link as defined in TS 23.402 clause 16. Standard IEEE 802.11 messaging is used over the Wi-Fi air link. As defined in IEEE 802.11-2007 section 7.2.2, a normal data frame uses three address fields. E.g. for an uplink frame (To DS=1 and From DS=0 in table 7-7 of IEEE 802.11-2007):

Address #1 is the receiving address (RA) and equals the BSSID of the AP;

Address #2 is the transmitting address (TA) and equals the source address (SA) which equals the MAC address of the UE;

Address #3 is the destination address (DA) and equals the MAC address of the TWAG (Trusted WLAN Access Gateway).

The MAC header also defines an address #4 which is normally not used.

[0027] To achieve a per-UE-and-PDN point-to-point link for additional PDN/NSWO connections, all four address fields in the MAC data frame header are used in accordance with the present invention. Frames are sent/received with header fields To DS=1 and From DS=1 as defined in table 7-7 of IEEE 802.11-2007. E.g. for an uplink frame:

Address #1 is RA and equals the BSSID of the AP;

Address #2 is TA and equals the physical MAC address of the UE;

Address #3 is DA and equals the MAC address of the TWAG;

Address #4 is SA and equals a virtual MAC address of the UE.

[0028] In the present invention, for each additional PDN connection, there is a virtual MAC address on the UE. This address is preferably unique within the scope of the UE. A virtual MAC address combined with the physical MAC address of the UE provides a globally unique identification for a PDN/NSWO connection. The TWAG and the UE can use this identification to correlate a packet to the correct PDN/NSWO connection.

[0029] Preferably, the 4-address MAC frame is used only over the Wi-Fi air link. Between the access point and TWAG, standard (wired) Ethernet frames are used. For an additional PDN connection, the UE virtual MAC address may be used between the access point and TWAG. The solution may be: (1) In the downlink, the AP preferably is able to know which physical MAC belongs to a virtual MAC. This may be a new AP requirement. It may learn this from uplink packets, though. (2) If we the physical MAC is not used between AP and TWAG, but only use the virtual MAC, then the virtual MAC should be unique within the scope of a TWAG. So, some kind of MAC negotiation mechanism can be used. This could be

done with the control protocol in the next section. Alternatively, some other mechanism e.g. VLANs between AP and TWAG may be used.

[0030] WLCP (WLAN Control Protocol) is a new protocol (related to SaMOG). The details are to be defined in Wi-Fi Alliance or 3GPP. WLCP could use the 4-address field as well; e.g. a dedicated virtual MAC is used to denote WLCP packets. The WLCP packets may be defined by Wi-Fi Alliance or stage 3 in 3GPP. A WLCP packet may e.g. indicate "attach" including APN and handover indicator.

[0031] Fig. 1a, is a diagram which illustrates the general format of the 802.11 MAC frame format. The MAC frame format comprises a set of fields that occur in a fixed order in all frames. There are three address fields in the MAC frame format, four when the ad hoc or the Wireless Distribution System (WDS) mode is being used. These fields are used to indicate the basic service set identifier (BSSID), source address, destination address, transmitting station address, and receiving station address. The usage of the four address fields in each frame type is indicated by the abbreviations BSSID, Destination Address (DA), Source Address (SA), Receiver Address (RA), and Transmitter Address (TA).

[0032] Fig. 1b, is a diagram which illustrates the format of the 802.11 4-address MAC frame format according to the preferred embodiments. It is similar to Fig. 1a, but specifies that the fourth MAC address is a virtual MAC address.

[0033] In Fig. 2, a LAN 1 (200) has a Station 1 (202), a Station 2 (204), an AP 1 (206), and UE (208), which communicates with at least one of antennas (210) and (212). A second LAN 2 (220) has a Station 3 (222), a Station 4 (224), an AP 2 (226), and antennas (230) and (232). LAN 1 communicates with LAN 2 over WDS link (240), using an 802.11 4-address format frame (280) according to the ad hoc or WDS modes. LAN1 and LAN 2 operate with 802.3 Ethernet Frames (250) and (252), respectively. LAN 1 can communicate with a cellular network (260) and/or an Internet or other network (270). Each of the Stations, APs, and UEs includes one or more processors, ROM storing program code for carrying out the

functions described herein, RAM, typical interfaces, transmitters/receivers, antennas, power supplies, etc. The UE may, for example, be a hand-held portable device such as a cellular telephone, smart phone, pad device, Personal Data Assistant, laptop computer, etc.

[0034] In Fig. 2, the four-address format frame (280) may be used to direct information over the WDS link (240). In this case, the four-address format frame (280) comprises the MAC address of Station 1 (202), the MAC address of Access Point 1 (206), the MAC address of Access Point 2 (226), and the MAC address of Station 3 (222). These are included in the 802.11 frame header. The frame data of (280) is the same as the original Ethernet frame (250). Based on information in this four-address format frame (280), the original Ethernet frame (250) will be reconstructed.

[0035] In the prior art, the UE typically can have only a single connection over the WLAN. The UE will not be able to concurrently access more than one PDN connection. As indicated earlier, when the WLAN is used to provide access to cellular data networks, it is desirable to provide access to multiple PDNs (packet data networks). As will be described further below, in the preferred embodiments, the IEEE 802.11 WDS (Wireless Distribution System) four-address frame format (280) is used to segregate multiple virtual services over a single WLAN interface. A four-address format currently may be used to create wireless repeater products, where one pair of addresses defines the ultimate source and destination address, and the other pair defines the next hop address. In the preferred embodiments on the other hand, the format is modified to enable multiple virtual services to be associated with multiple virtual addresses.

[0036] Fig. 3 shows the basic architecture of a wireless distribution system that illustrates how a UE can access multiple services according to the preferred embodiments of the present invention. In Fig. 3, MAC2@ and MAC3@ each are associated with an IP@. Thus, there are a total of three IP addresses in Fig. 3. The figure illustrates how a Wi-Fi client, such as a mobile device UE (302) can connect to a Trusted WLAN Access Gateway Cellular Network

(304), or Internet or other network (306) and/or (308), via an Access Point (310) in order to obtain access to additional services through the WLAN 340.

[0037] The Wi-Fi client (302) is provided access to multiple packet data networks (PDNs) via a cellular data network (304), where each PDN provides a dedicated PDN connection. More specifically, the Wi-Fi client (302) is provided with a number of virtual MAC addresses (312) and (314). Each virtual MAC address (312) and (314) is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the packet data networks. The Wi-Fi client's virtual MAC address for the requested data service is then delivered via a 4 address MAC frame (inner address) when the Wi-Fi client (302) is communicating with the associated data service over the cellular data network (304).

[0038] For an upstream frame (device to network), the receiver address is the wireless access point (310) address MAC BSSAD1 (307; outer address), and the destination address is the wireless access gateway address, while the transmitter address is the device (302) physical address (316) and the source address is the device (302) virtual address (312; inner address) and/or (314; inner address). For a downstream frame (network to device), the transmitter address is the access point (310) address and the source address is the wireless access gateway, while the receiver address is the device (302) physical address (316) and the destination address is the device (302) virtual address (312) and/or (314).

[0039] Fig. 4 is a is a schematic block diagram of the structure according to the preferred embodiments. The UE may comprise a cellular telephone (402) having an antenna (404) which wirelessly communicates with a first antenna (454) of an AP (450). The cellular telephone (402) also has one or more CPUs (406), a ROM (408), a RAM (410), a bus (412), an antenna interface (414), a transmitter/receiver (416; which may be separate or combined circuitry), and a power supply (418). The AP has a one or more CPUs (456), a ROM (458), a RAM (460), a bus (462), a first antenna interface (456), a first transmitter/receiver (462; which may be separate or combined circuitry), and a power supply (458). The AP (450) also has a second antenna (470) for communicating with one or more dedicated Networks (480)

and (482). A second interface (472) is coupled the second antenna (470), and a second transceiver (474) is coupled to the second interface (472). A third interface (490) may, for example, be coupled to a wired network via wiring (492).

[0040] For single APN connections, only the transmitter address and the receiver address will be used on the upstream and downstream respectively. The need to use multiple PDN connections is indicated when the device initially connects to the network, or when an additional APN is needed, by using, e.g. extensions to EAP (Extensible Authentication Protocol) or DHCP (Dynamic Host Control Protocol). In this case the source and destination address fields will be used instead of transmitter and receiver.

[0041] For a first PDN connection, the normal Wi-Fi MAC address format is used. No change is necessary compared to unmodified UE. The 4-MAC address MAC format is then used between UE and AP for additional PDN connections. The 4-MAC frame in the upstream, i.e. between UE and AP will comprise:

RA (Receiver Address) = AP BSSID
TA (Transmitter Address) = UE MAC@1 (physical)
DA (Destination Address) = TWAG
SA (Source Address) = UE MAC@2 (virtual; for 2nd PDN connection).

[0042] On the downstream side, that is between the AP and UE, the 4-MAC frame format will comprise:

RA (Receiver Address) = UE MAC@1 (physical)
TA (Transmitter Address) = AP BSSID
DA (Destination Address) = UE MAC@2 (virtual)
SA (Source Address) = TWAG.
Where, e.g., MAC@1 is an abbreviation for MAC Address 1.

[0043] Now, between the AP and the TWAG, normal addressing is used; e.g. using UE MAC@2 for the 2nd PDN connection. The virtual MAC addresses may assigned to the UE by:

-Pre-configured global MACs loaded into the UE at the factory or a UE provisioning facility (e.g., wireless provider store);
-Administered by a network (fixed or 3GPP (AAA) and sent to the UE at authentication (perhaps limited to a max number of PDN connections); and/or
-Negotiated dynamically when the UE needs it (e.g. by means of the previously mentioned WLCP, or based on ARP (Address Resolution Protocol)).

[0044] Fig. 5, is a functional flow diagram illustrating how the 4-address MAC header is used in the establishment of an additional PDN connection in the preferred embodiments.

[0045] For authentication (EAP and 802.1X) and for the first PDN connection, the UE uses its first MAC address and normal Wi-Fi MAC frame for addressing. This way, an easier UE implementation can be achieved when only a single PDN connection is used.

[0046] For an additional PDN connection, the UE uses another virtual MAC address. All signaling over Wi-Fi is done using the 4-address MAC frame. For PDN connections, DHCP extensions may be used (when DCHP is the control plane protocol) to indicate handover and a non-default APN. Downlink frames are always sent L2 (Layer 2) unicast (including e.g. RA and IP multicast). The 4-address MAC frames use the same encryption over Wi-Fi as the normal MAC frames.

[0047] Fig. 6 is a flow chart of a preferred process according to the present invention. These functions are preferably carried out in the AP, using one or more processors therein, together with memory storing program code to carry out the described functions. The process provides the UE access to a plural PDNs, where each PDN provides a dedicated PDN

connection. The process begins at step (602), and at step (604) the AP allocates the UE a plurality of virtual MAC addresses. At step (606), the AP assigns each of the virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of the PDNs. At step (608), the AP delivers one of the virtual MAC addresses via a 4 address MAC frame when the UE is communicating with the associated data service.

[0048] Fig. 7 is a process diagram of an initial attachment in WLAN on GTP (GPRS Tunneling Protocol) S2a for roaming, LBO (Local Breakout), and non-roaming scenarios. The procedure is as in 3GPP TS (Technical Specification) 23.402 clause 16.2.1 with the following additions:

Step 1. Optionally, in order optimize network selection, the network may indicate its capabilities (support for handover, support for attach to non-default APN, support for non-seamless WLAN offload, support for EPC-routed traffic, support for attach to multiple PDN connections). Preferably, it is FFS if these capabilities are specified by 3GPP or by another SDO.

Step 2. The UE indicates initial attach in EAP to the 3GPP AAA. The UE preferably indicates whether it requests EPC (Evolved Packet Core) access or non-seamless WLAN offload in EAP to the 3GPP AAA. If the UE requests EPC access, it may indicate APN. As part of step 2, the 3GPP AAA sends these indicators to the TWAN. If the UE indicates EPC access without indicating APN, then the EAP reply indicates the selected default APN. As part of step 2, the UE indicates its capabilities (support for handover, support for attach to non-default APN, support for attach to multiple PDN connections). The network indicates its capabilities (support for handover, support for attach to non-default APN, support for non-seamless WLAN offload, support for EPC-routed traffic, support for attach to multiple PDN connections) to the UE.

Step 3. If the UE indicated an APN in the previous step, the TWAN verifies that it is allowed by subscription, selects the PDN GW for the APN correspondingly, and includes the APN in the Create Session Request.

[0049] Fig. 8 is a process diagram of UE-Initiated connectivity to an additional PDN in WLAN on GTP S2a. Establishment of an additional PDN/NSWO connection over WLAN with GTP S2a is supported only for the accesses that support such feature and for the UEs that have such capability.

[0050] This procedure is related to the case when the UE has an established a PDN/NSWO connection over WLAN and wishes to establish one or more additional PDN/NSWO connections over such access. This procedure is also used to request for connectivity to an additional PDN/NSWO connection over WLAN when the UE is simultaneously connected to such access and a 3GPP access, and the UE already has active PDN/NSWO connections over both the accesses. The UE establishes a separate point-to-point link to the TWAG for each additional PDN/NSWO connection.

[0051] There can be more than one PDN connection per APN when GTP is used between the TWAN and the PDN GW. During the establishment of a new PDN connection, the TWAN allocates and sends a default S2a bearer ID to the PDN GW. The default S2a bearer ID is unique in the scope of the UE within a TWAG, i.e. the IMSI (International Mobile Subscriber Identity) and the default S2a bearer ID together identify a PDN connection within a TWAG. In order to be able to identify a specific established PDN connection, both the TWAG and the PDN GW preferably store the default S2a bearer ID. The establishment of an additional PDN/NSWO connection should not impact the first PDN/NSWO connection. As a separate point-to-point link is used for each additional PDN/NSWO connection, traffic separation can be achieved between all PDN/NSWO connections including the first.

Step 1. The UE triggers the establishment of a new PDN/NSWO connection by means of WLCP. This step establishes the setup of a new per-UE-and-PDN-connection point-to-point link to the TWAG. The UE preferably indicates whether it requests EPC access or non-seamless WLAN offload. If the UE requests EPC access, it may indicate APN. The UE preferably triggers the re-establishment of an existing PDN/NSWO connectivity by providing a handover indicator.

Step 2. Upon establishment of an additional PDN/NSWO connection, steps 9-15 as described in clause 8.2.x.2.1.1 are performed. As part of these steps, the TWAN performs PDN GW selection as described in TS 23.402. Steps 9-15 are preferably executed with PDN GW2 instead of PDN GW1. Unless non-seamless WLAN offload was selected in step 1, steps 10-14 in clause 8.2.x.2.1.1 are preferably always performed.

[0052] Fig. 9 is a process diagram of a handover procedure between 3GPP access and WLAN on S2a. The home routed roaming, LBO and non-roaming scenarios are depicted in Fig. 9. In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN (Home Public Land Mobile Network) to the PDN GW in the VPLMN (Visited Public Land Mobile Network) and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy preferably are not involved, except for the authentication and authorization in step 2.

[0053] For connectivity to multiple PDNs the following preferably applies:

If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 15 are preferably skipped and the UE preferably only perform step 16 for each PDN connection that is being transferred from 3GPP access.

If the UE is connected only to 3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 15 are preferably performed. In these steps the UE preferably provides an APN corresponding to one of the PDN connections that are being transferred from 3GPP access. The UE preferably then repeats step 16 for each of the remaining PDN connections that are being transferred from 3GPP access.

Step 17 is preferably repeated for each PDN connection that is being transferred from 3GPP access.

Step 16 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in TS 23.402 clause 8.1.

[0054] The steps in Fig. 9 are based on Fig. 8, with the following changes:

Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.

Step 2. As step 2 in Fig. 8 with the following addition: The UE preferably indicates handover via EAP to 3GPP AAA.

Steps 3 and 10. As step 2 in Fig. 8 with the following addition: The handover indication is preferably set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF (Policy and Charging Enforcement Function)-Initiated IP-CAN (IP Connectivity Access Network) Session Modification Procedure with the PCRF (Policy and Charging Rules Function).

Step 4 and 11. The PDN GW preferably executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [xx]. The Event Report indicates the change in Access Type. If the PDN GW decided to allocate a new IP address/prefix instead of preserving the old IP address/prefix, as described in TS 23.402 clause 4.1.3.2.3, the PDN GW executes an IP-CAN session Establishment Procedure with the PCRF instead of a PCEF-Initiated IP-CAN Session Modification Procedure.

Step 6 and 13. The PDN GW preferably responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID (Tunnel Endpoint ID) of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS (Evolved Packet System) Bearer Identity, EPS Bearer QoS (Quality of Service), APN-AMBR (Aggregate Maximum Bit Rate), Charging ID, Cause). The Create Session Response preferably contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access. The Charging Id provided by the PGW is preferably the Charging ID previously assigned to the default bearer of the PDN connection in the 3GPP access.

Step 16. For connectivity to multiple PDNs simultaneously or nearly-simultaneously, the UE preferably establishes connectivity to each PDN that is being transferred from 3GPP access, besides the PDN connection that was established in the

previous steps, by executing the UE-initiated Connectivity to Additional PDN procedure specified above.

Step 17. The PDN GW preferably initiates the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [xx], clause 5.4.4.1.

[0055] Fig. 10 is a process diagram of a handover from WLAN on GTP S2a to 3GPP access for roaming, LBO and non-roaming scenarios, according to the present invention. This procedure is preferably as in TS 23.402 clause 8.2.1.1/8.2.1.2 with the following differences:

Step 1. There is preferably a GTP tunnel between TWAN and PGW.

Step 18. The PDN GW preferably initiates resource allocation deactivation procedure in the TWAN as discussed above.

[0056] Fig. 11 is a process diagram of a UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN. If the UE has a single PDN/NSWO connection established over WLAN, this procedure is preferably the same as TS 23.402 clause 16.3.1.1. If the UE has multiple PDN/NSWO connections established over WLAN, this clause preferably applies to UE/TWAN-requested PDN disconnection procedure. For multiple PDN/NSWO connectivity, this disconnection procedure is preferably repeated for each PDN/NSWO connection.

[0057] The procedure outlined in Fig. 11 preferably applies to the Non-Roaming, Home Routed Roaming, and Local Breakout cases. In the Local Breakout case, the vPCRF preferably forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy preferably serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is preferably not involved.

[0058] If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF preferably do not occur. Instead, the PDN GW may employ static configured policies.

Step 1. The UE may initiate disconnection of the PDN/NSWO connection by means of WLCP.

Step 2. The TWAN preferably releases the PDN connection and sends a Delete Session Request (Linked EPS Bearer ID) message for this PDN connection to the PDN GW. In case of a NSWO connection, the TWAN preferably releases this connection and the subsequent steps preferably do not apply.

Step 3. The PDN GW preferably informs the 3GPP AAA Server of the PDN disconnection.

Step 4. The PDN GW preferably deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [x].

Step 5. The PDN GW preferably acknowledges with a Delete Session Response (Cause) message.

[0059] Fig. 12 is a process diagram of a PDN GW Initiated Bearer Resource Allocation Deactivation in WLAN with GTP on S2a. The procedure if Fig. 12 is preferably as in TS 23.402, clause 16.4.1 with the following difference: If all TWAN resources related to a PDN/NSWO connection are released, then in step 3 the UE is preferably informed of the PDN/NSWO release using WLCP.

[0060] The present invention can be realized in hardware, or a combination of hardware and software. Any kind of computing system, or other apparatus adapted for carrying out the methods described herein, is suited to perform the functions described herein. A typical combination of hardware and software could be a specialized computer system, e.g., a router, having one or more processing elements and a computer program stored on a storage medium that, when loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer

program product, which comprises all the features enabling the implementation of the methods described herein, and which, when loaded in a computing system is able to carry out these methods. Storage medium refers to any volatile or non-volatile storage device.

[0061] Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form. Computer readable medium means any non-transitory medium capable of storing program code which, when loaded into one or more processors, causes functions to be performed as described herein.

[0062] Thus, one embodiment is a computer readable medium containing computer readable instruction that, when executed by a processor, cause the processor to perform functions for maintaining clock synchronization between a first and a second radio.

[0063] All documents, specifications, clauses, etc. discussed herein are hereby incorporated into this disclosure by reference.

[0064] In addition, unless mention was made above to the contrary, it should be noted that all of the accompanying drawings are not to scale. It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described herein above. A variety of modifications and variations are possible in light of the above teachings without departing from the scope and spirit of the invention, which is limited only by the following claims.

What is Claimed Is:

1. A method of providing, to a client, access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, comprising the steps of:

assigning said client a plurality of virtual Media Access Control (MAC) addresses;

assigning each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and

providing to said client at least one of said virtual MAC addresses via a 4 address MAC frame for said client to communicate with the associated data service.

2. The method according to claim 1, wherein said client comprises a Wi-Fi client, and wherein said Wi-Fi client communicates with the associated data service over a cellular data network using the provided 4 address MAC frame.

3. The method according to claim 2, wherein the Wi-Fi client communicates with plural associated data services at the same time.

4. The method according to claim 2, wherein the communicating comprises providing an upstream 4 address MAC frame comprising:

a Receiver Address corresponding to an Access Point (AP) Basic Service Set Identifier (BSSID);

a Transmitter Address corresponding to a User Equipment (UE) MAC address1;

a Destination Address corresponding to a Trusted WLAN Access Gateway; and

a Source Address corresponding to a UE MAC address2.

5. The method according to claim 4, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

6. The method according to claim 2, wherein the communicating comprises providing a downstream 4 address MAC frame comprising:

a Receiver Address corresponding to a UE MAC address1;

a Transmitter Address corresponding to an AP BSSID;

a Destination Address corresponding to a UE MAC address2; and

a Source Address corresponding to a Trusted WLAN Access Gateway.

7. The method according to claim 6, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

8. The method according to claim 2, further comprising a second step of the client communicating with a second associated data service over the cellular data network using a second one of said virtual MAC addresses via a second 4 address MAC frame, and wherein the second step of communicating comprises providing an upstream 4 address MAC frame comprising:

a Receiver Address corresponding to an AP BSSID;

a Transmitter Address corresponding to a UE MAC address1;

a Destination Address corresponding to a Trusted WLAN Access Gateway; and

a Source Address corresponding to a UE MAC address3.

9. The method according to claim 8, wherein the client has a first connection to a PDN, and wherein the UE MAC address3 comprises a virtual address corresponding to another PDN connection.

10. The method according to claim 9, wherein the second step of communicating comprises providing a downstream 4 address MAC frame comprising:

a Receiver Address corresponding to a UE MAC address1;

a Transmitter Address corresponding to an AP BSSID;

a Destination Address corresponding to a UE MAC address3; and

a Source Address corresponding to a Trusted WLAN Access Gateway.

11. The method according to claim 10, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to another PDN connection.

12. The method according to claim 1, wherein said Wi-Fi client comprises a cellular telephone.

13. The method according to claim 1, wherein said Wi-Fi client comprises a pad device.

14. The method according to claim 1, wherein the virtual MAC addresses are provided to the client prior to said client contacting an access point.

15. The method according to claim 1, wherein the virtual MAC addresses are provided to the client after said client contacts an access point.

16. The method according to claim 1, wherein the virtual MAC addresses are provided to the client by a network during an authentication process.

17. The method according to claim 1, wherein the virtual MAC addresses are provided to the client by a negotiation during an address resolution negotiation.

18. The method according to claim 1, wherein the virtual MAC addresses provided to the client are stored in a client memory.

19. Apparatus providing to a client, access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, comprising:

an Access Point (AP) configured to communicate with (i) the client and (ii) the plurality of PDNs, the AP further configured to:

assign said client a plurality of virtual Media Access Control (MAC) addresses;

assign each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and

provide to said client at least one of said virtual MAC addresses via a 4 address MAC frame for said client to communicate with the associated data service.

20. The apparatus according to claim 19, wherein said client comprises a Wi-Fi client, and wherein said Wi-Fi client communicates with the associated data service over a cellular data network using the provided 4 address MAC frame.

21. The apparatus according to claim 20, wherein the AP is further configured to provide the client an upstream 4 address MAC frame comprising:

a Receiver Address corresponding to an Access Point (AP) Basic Service Set Identifier (BSSID);

a Transmitter Address corresponding to a User Equipment (UE) MAC address1;

a Destination Address corresponding to a Trusted WLAN Access Gateway; and

a Source Address corresponding to a UE MAC address2.

22. The apparatus according to claim 21, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

23. The apparatus according to claim 21, wherein the AP is further configured to provide the client a downstream 4 address MAC frame comprising:

a Receiver Address corresponding to a UE MAC address1;

a Transmitter Address corresponding to an AP BSSID;

a Destination Address corresponding to a UE MAC address2; and

a Source Address corresponding to a Trusted WLAN Access Gateway.

24. The apparatus according to claim 23, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

25. The apparatus according to claim 19, wherein the AP is further configured to provide the client with a second one of said virtual MAC addresses via a second 4 address MAC frame for the client to communicate with another associated data service, and wherein the AP is further configured to provide to the client an upstream 4 address MAC frame comprising:

a Receiver Address corresponding to an AP BSSID;

a Transmitter Address corresponding to a UE MAC address1;

a Destination Address corresponding to a Trusted WLAN Access Gateway; and

a Source Address corresponding to a UE MAC address3.

26. The apparatus according to claim 25, wherein the client has a first connection to a PDN, and wherein the UE MAC address3 comprises a virtual address corresponding to another PDN connection.

27. The apparatus according to claim 26, wherein the AP is further configured to provide to the client a downstream 4 address MAC frame comprising:

a Receiver Address corresponding to a UE MAC address1;

a Transmitter Address corresponding to an AP BSSID;

a Destination Address corresponding to a UE MAC address3; and

a Source Address corresponding to a Trusted WLAN Access Gateway.

28. The apparatus according to claim 27, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to another PDN connection.

29. The apparatus according to claim 19, further comprising the Wi-Fi client, which comprises a cellular telephone.

30. At least one computer-readable, non-transitory medium containing program code which, when loaded into one or more processors of an Access Point (AP) causes said one or more processors to provide to a client access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, said program code also causing said one or more processors to:

assign to said client a plurality of virtual Media Access Control (MAC) addresses;

assign each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and

provide to the client at least one of said virtual MAC addresses via a 4 address MAC frame when said client is communicating with the associated data service.

31. A cellular telephone, comprising:

transmitter and receiver structure configured to communicate with an access point;

a memory storing a plurality of virtual Media Access Control (MAC) addresses, each corresponding to a dedicated PDN connection; and

at least one processor configured to communicate with said access point, through said transmitter and receiver structure, using at least one of the stored virtual MAC addresses in a 4 address MAC frame.

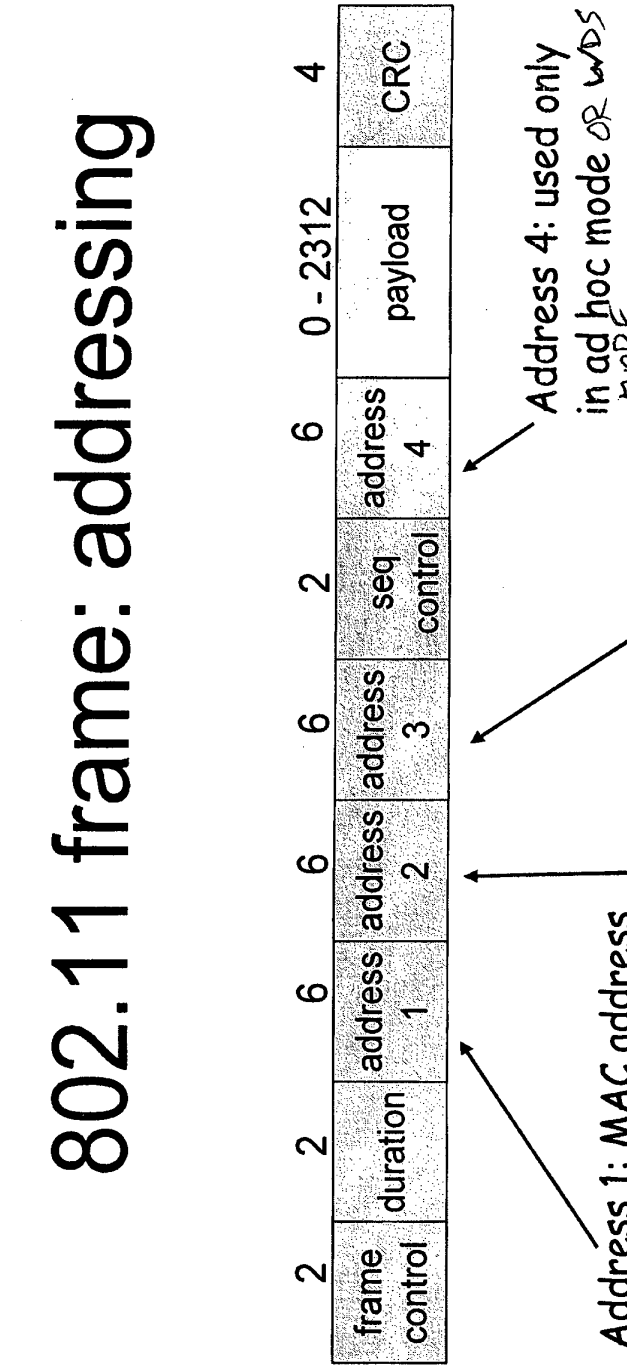

802.11 frame: addressing
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
2
2
6
6
6
2
6
0 - 2312
4
Address 1: MAC address of wireless host or AP to receive this frame
Address 2: MAC address of wireless host or AP transmitting this frame
Address 3: MAC address of router interface to which AP is attached
Address 4: used only in ad hoc mode OR WDS mode

Fig. 1a

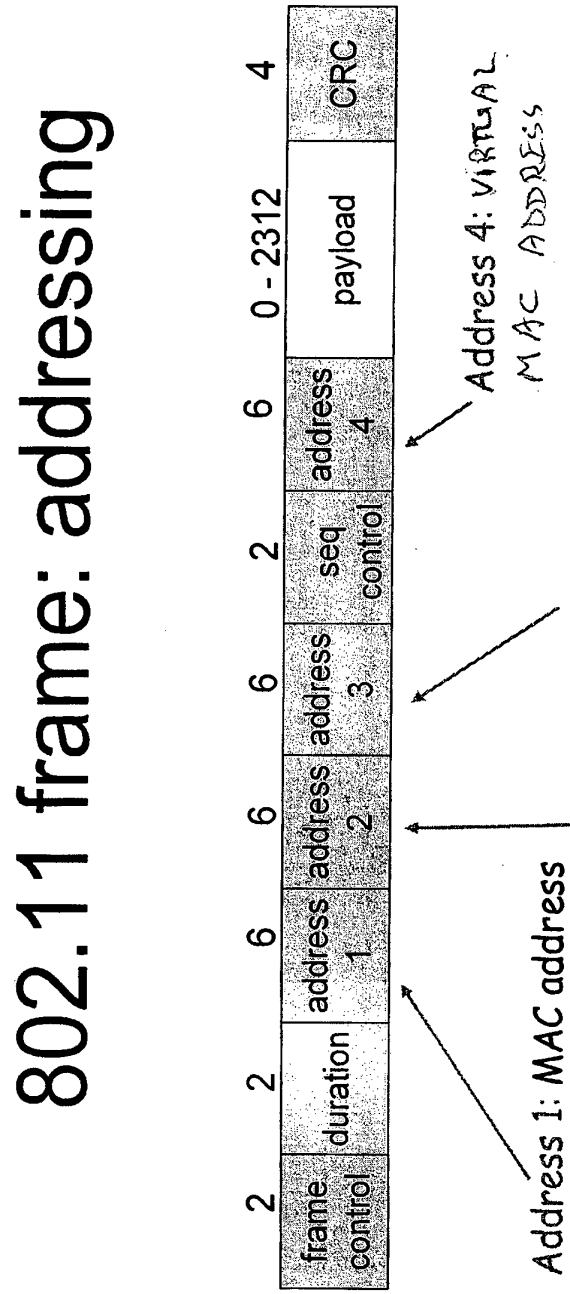

802.11 frame: addressing
2
2
6
6
6
2
6
0 - 2312
4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
Address 1: MAC address of wireless host or AP to receive this frame
Address 2: MAC address of wireless host or AP transmitting this frame
Address 3: MAC address of router interface to which AP is attached
Address 4: VIRTUAL MAC ADDRESS

Fig. 1b

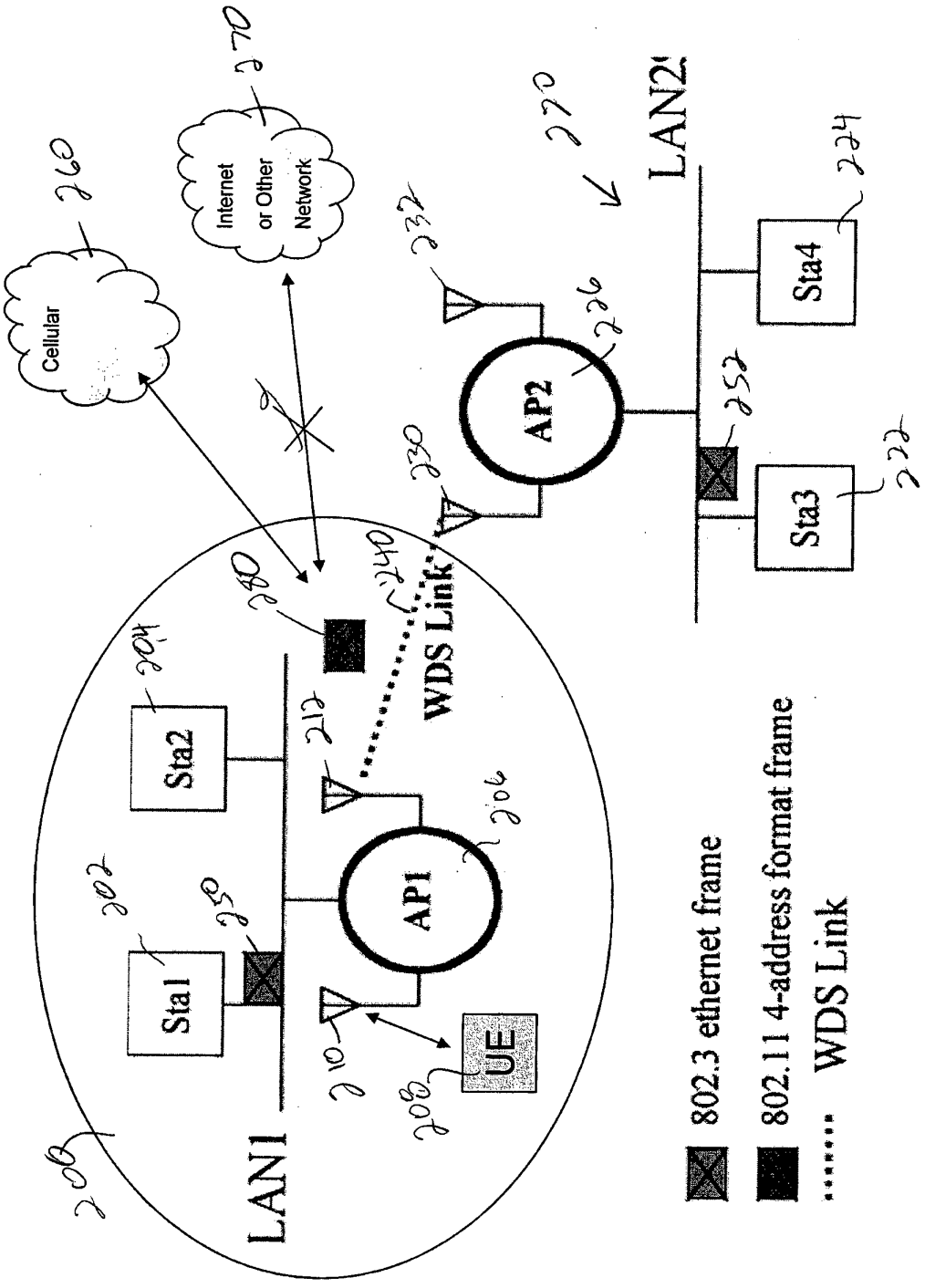


Fig. 2 PRIOR ART

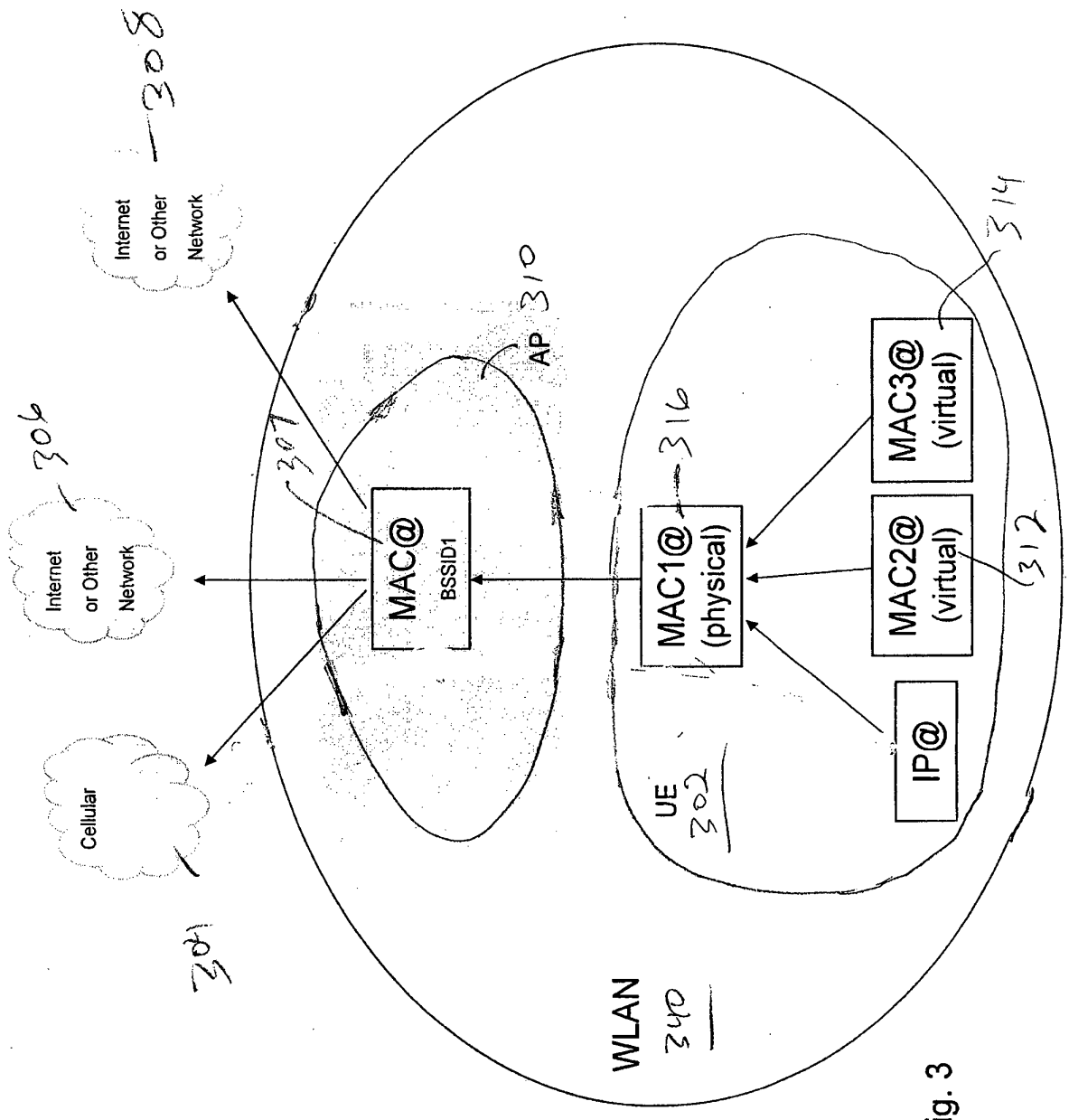

Internet or Other Network
308
Internet or Other Network
306
Cellular
301
MAC@
BSSID1
307
AP
310
WLAN
340
MAC1@
(physical)
316
UE
302
MAC2@
(virtual)
MAC3@
(virtual)
314
312
IP@

Fig. 3

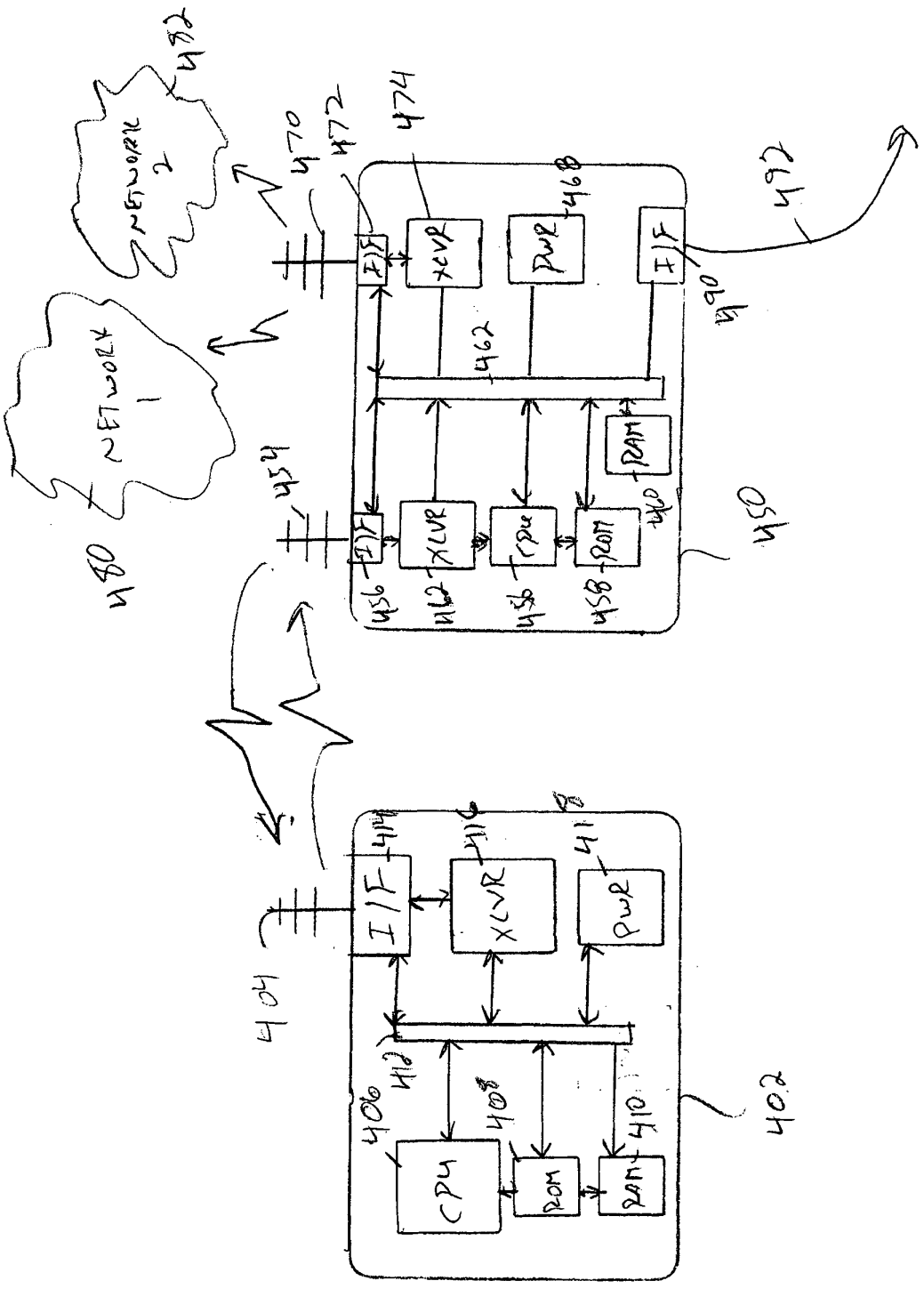

NETWORK 1
NETWORK 2
480
482
470
472
474
454
462
468
490
492
450
456
458
460
452
IF
XCVR
PWR
RAM
ROM
CPU
402
404
406
408
410
412
414
416

Fig. 4

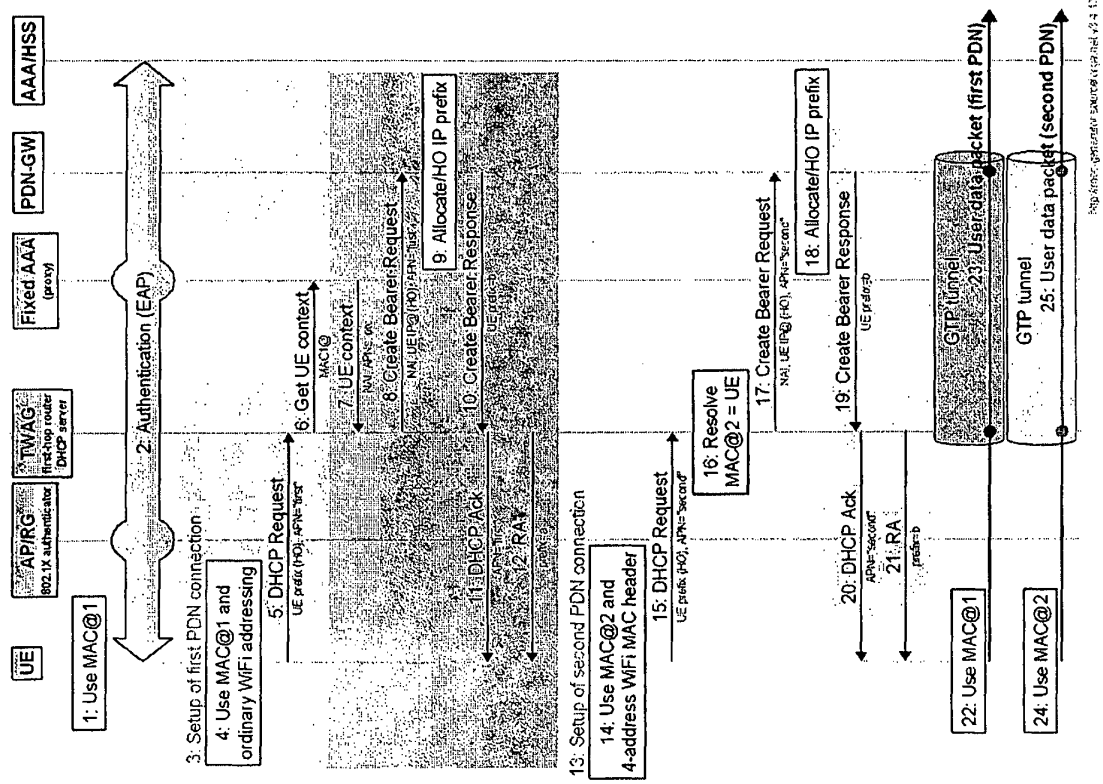

UE
AP/RG
802.1X authenticator
TWAG
first-hop router
DHCP server
Fixed AAA
(proxy)
PDN-GW
AAA/HSS
1: Use MAC@1
2: Authentication (EAP)
3: Setup of first PDN connection
4: Use MAC@1 and ordinary WiFi addressing
5: DHCP Request
6: Get UE context
7: UE context
8: Create Bearer Request
9: Allocate/HO IP prefix
10: Create Bearer Response
11: DHCP Ack
12: RA
13: Setup of second PDN connection
14: Use MAC@2 and 4-address WiFi MAC header
15: DHCP Request
16: Resolve MAC@2 = UE
17: Create Bearer Request
18: Allocate/HO IP prefix
19: Create Bearer Response
20: DHCP Ack
21: RA
GTP tunnel
23: User data packet (first PDN)
GTP tunnel
25: User data packet (second PDN)
22: Use MAC@1
24: Use MAC@2

Fig. 5

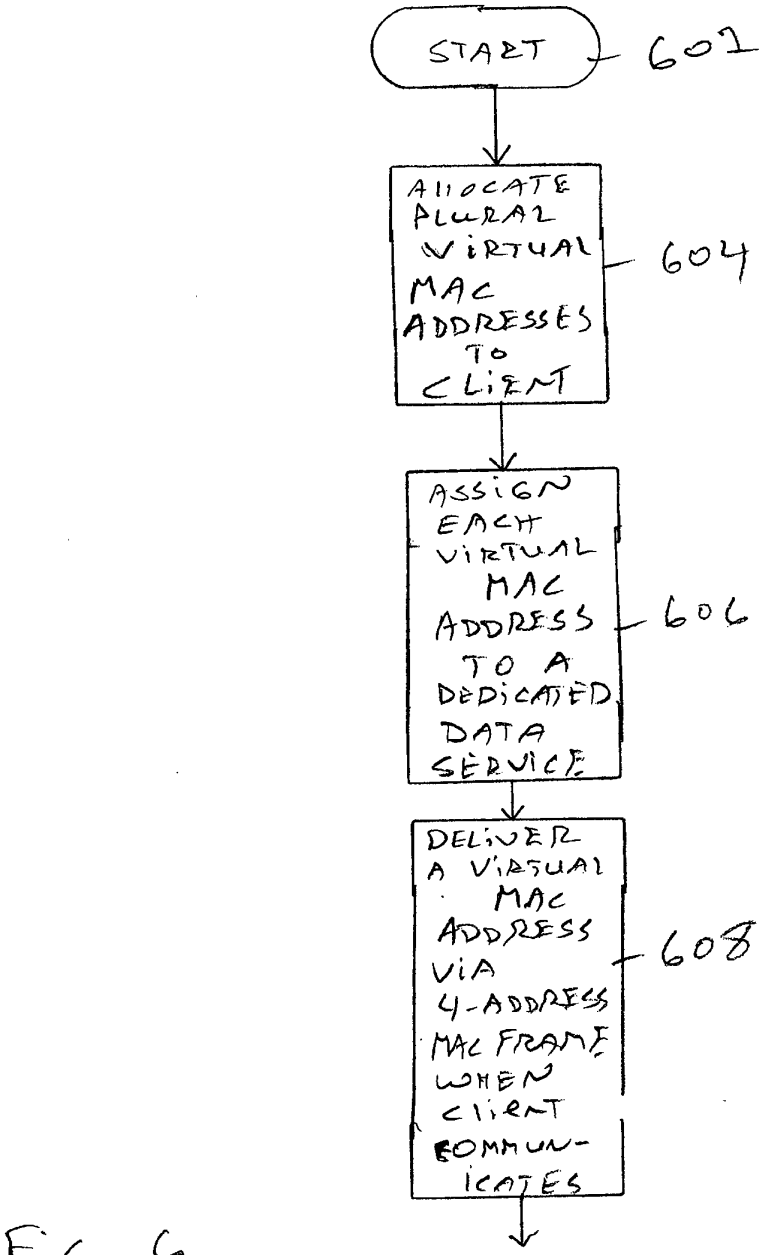

START
602
ALLOCATE PLURAL VIRTUAL MAC ADDRESSES TO CLIENT
604
ASSIGN EACH VIRTUAL MAC ADDRESS TO A DEDICATED DATA SERVICE
606
DELIVER A VIRTUAL MAC ADDRESS VIA 4-ADDRESS MAC FRAME WHEN CLIENT COMMUNICATES
608

FIG. 6

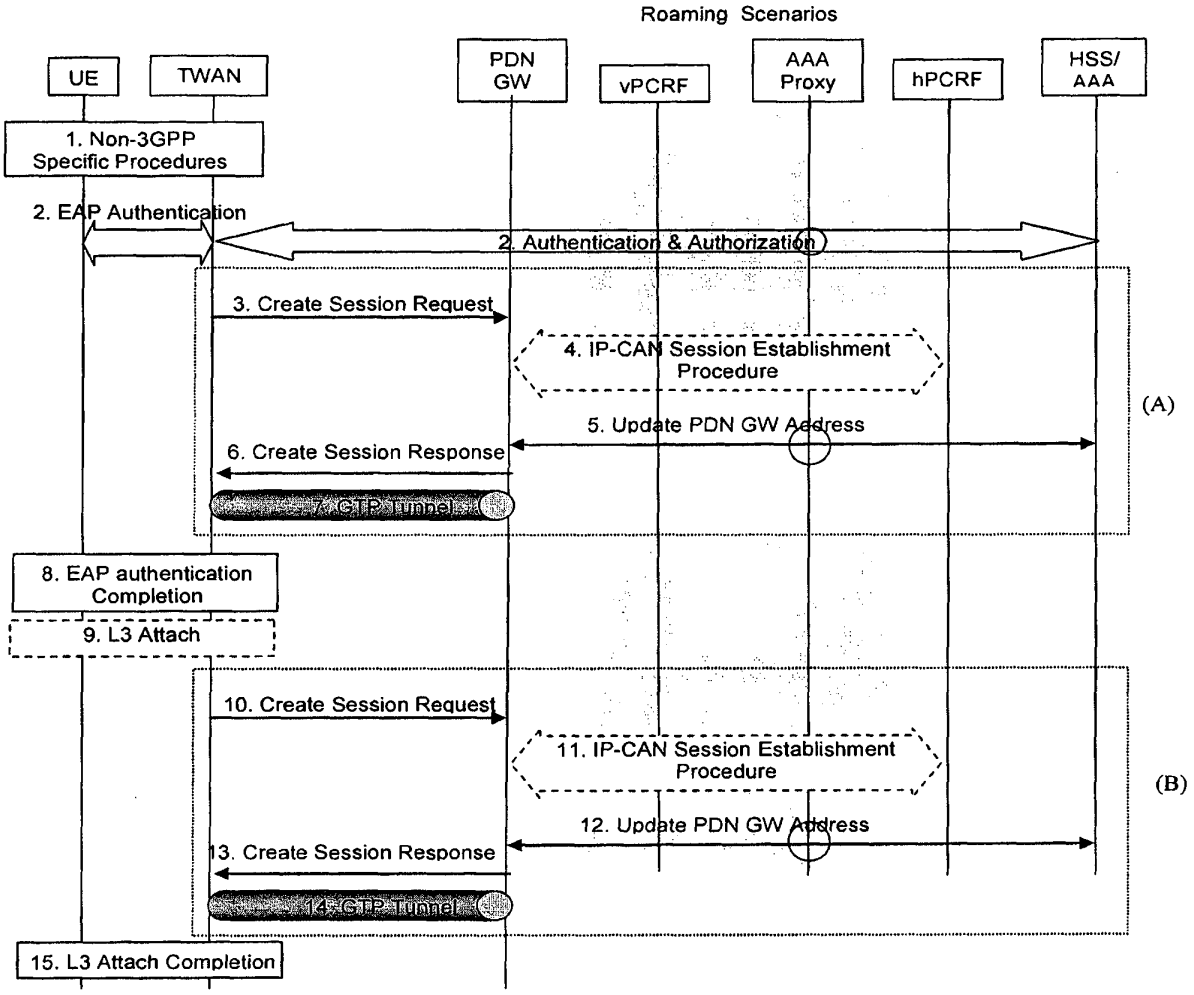

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request
4. IP-CAN Session Establishment Procedure
5. Update PDN GW Address
6. Create Session Response
7. GTP Tunnel
(A)
8. EAP authentication Completion
9. L3 Attach
10. Create Session Request
11. IP-CAN Session Establishment Procedure
12. Update PDN GW Address
13. Create Session Response
14. GTP Tunnel
(B)
15. L3 Attach Completion

Fig. 7

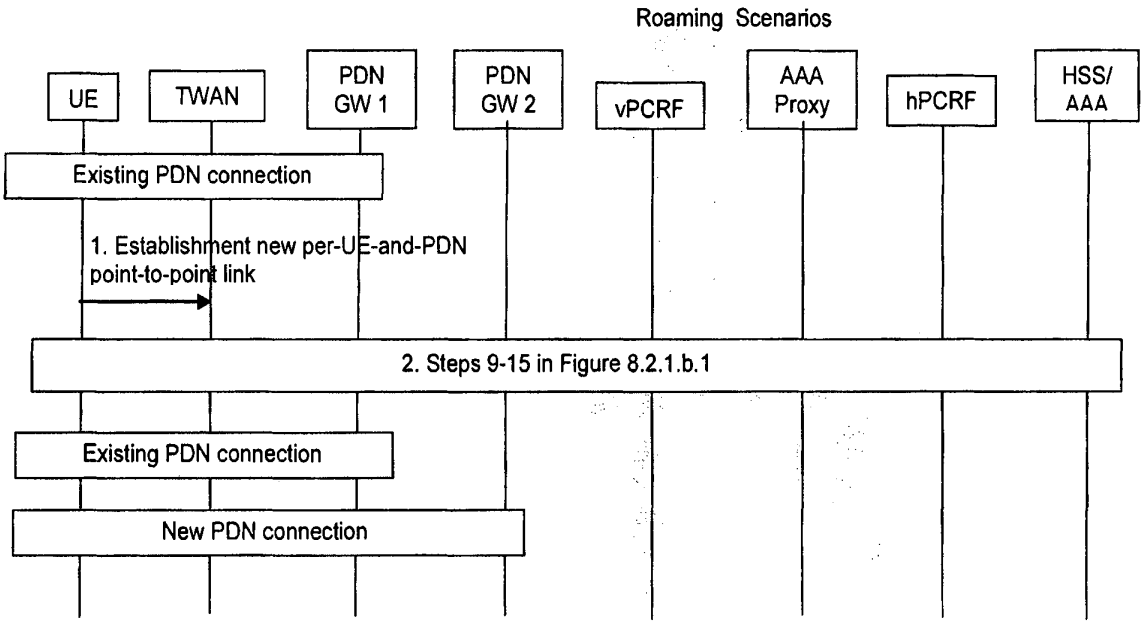

Roaming Scenarios
UE
TWAN
PDN GW 1
PDN GW 2
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
Existing PDN connection
1. Establishment new per-UE-and-PDN point-to-point link
2. Steps 9-15 in Figure 8.2.1.b.1
Existing PDN connection
New PDN connection

Fig. 8

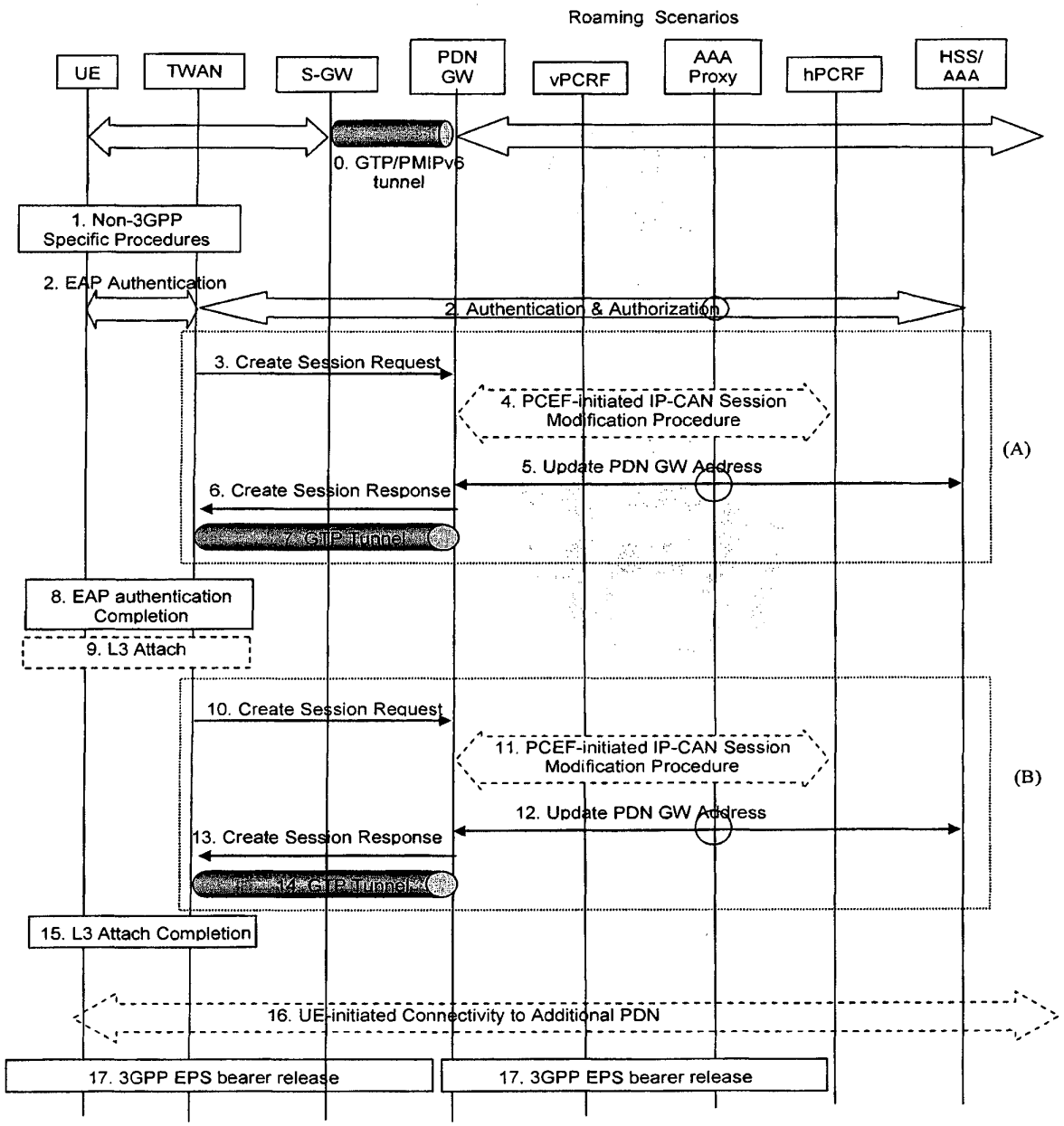

Roaming Scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA Proxy
hPCRF
HSS/ AAA
0. GTP/PMIPv6 tunnel
1. Non-3GPP Specific Procedures
2. EAP Authentication
2. Authentication & Authorization
3. Create Session Request
4. PCEF-initiated IP-CAN Session Modification Procedure
5. Update PDN GW Address
6. Create Session Response
7. GTP Tunnel
(A)
8. EAP authentication Completion
9. L3 Attach
10. Create Session Request
11. PCEF-initiated IP-CAN Session Modification Procedure
12. Update PDN GW Address
13. Create Session Response
14. GTP Tunnel
(B)
15. L3 Attach Completion
16. UE-initiated Connectivity to Additional PDN
17. 3GPP EPS bearer release
17. 3GPP EPS bearer release

Fig. 9

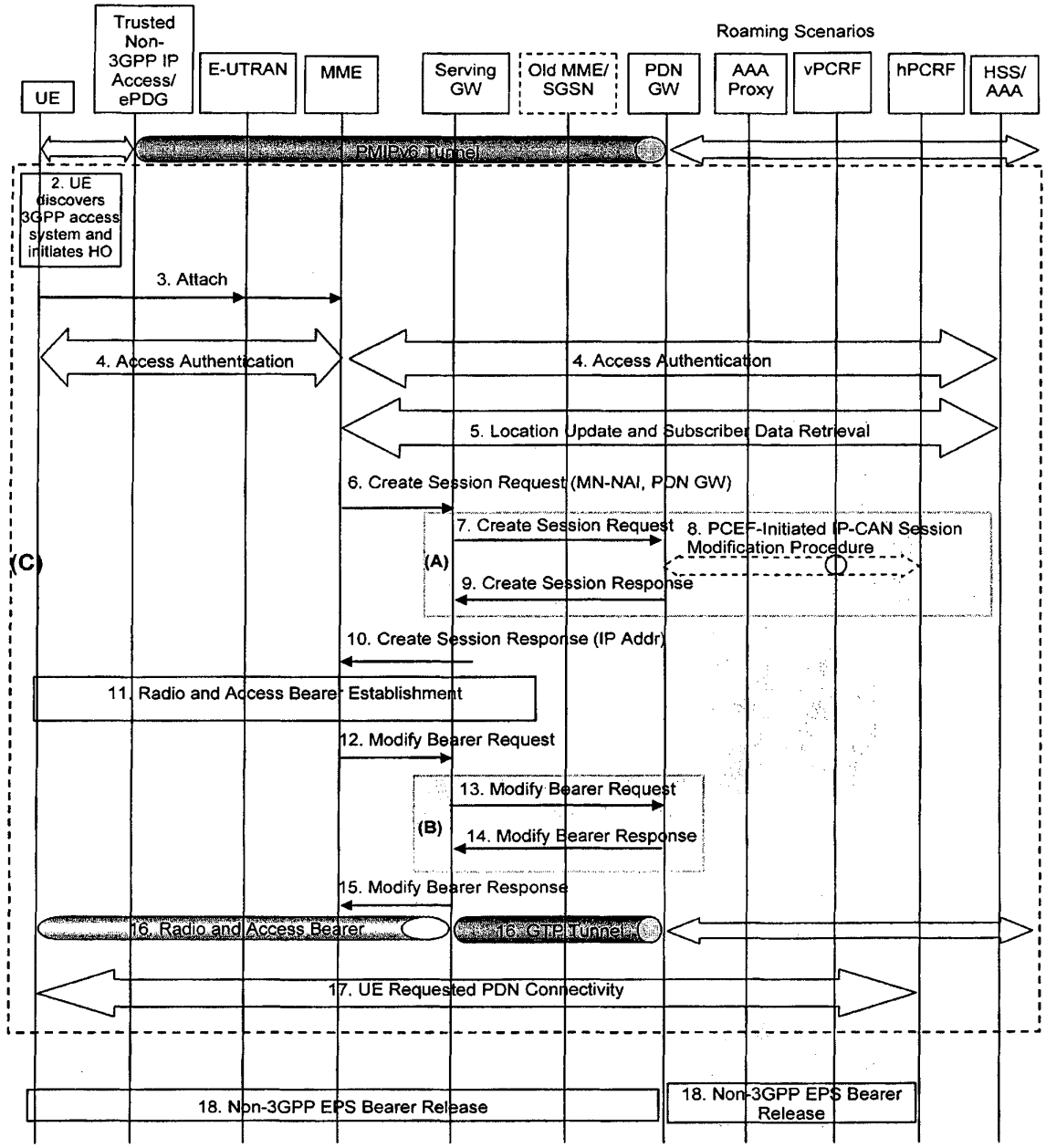

Roaming Scenarios
UE
Trusted Non-3GPP IP Access/ ePDG
E-UTRAN
MME
Serving GW
Old MME/ SGSN
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
PMIPv6 Tunnel
2. UE discovers 3GPP access system and initiates HO
3. Attach
4. Access Authentication
4. Access Authentication
5. Location Update and Subscriber Data Retrieval
6. Create Session Request (MN-NAI, PDN GW)
(C)
(A)
7. Create Session Request
8. PCEF-Initiated IP-CAN Session Modification Procedure
9. Create Session Response
10. Create Session Response (IP Addr)
11. Radio and Access Bearer Establishment
12. Modify Bearer Request
(B)
13. Modify Bearer Request
14. Modify Bearer Response
15. Modify Bearer Response
16. Radio and Access Bearer
16. GTP Tunnel
17. UE Requested PDN Connectivity
18. Non-3GPP EPS Bearer Release
18. Non-3GPP EPS Bearer Release

Fig. 10

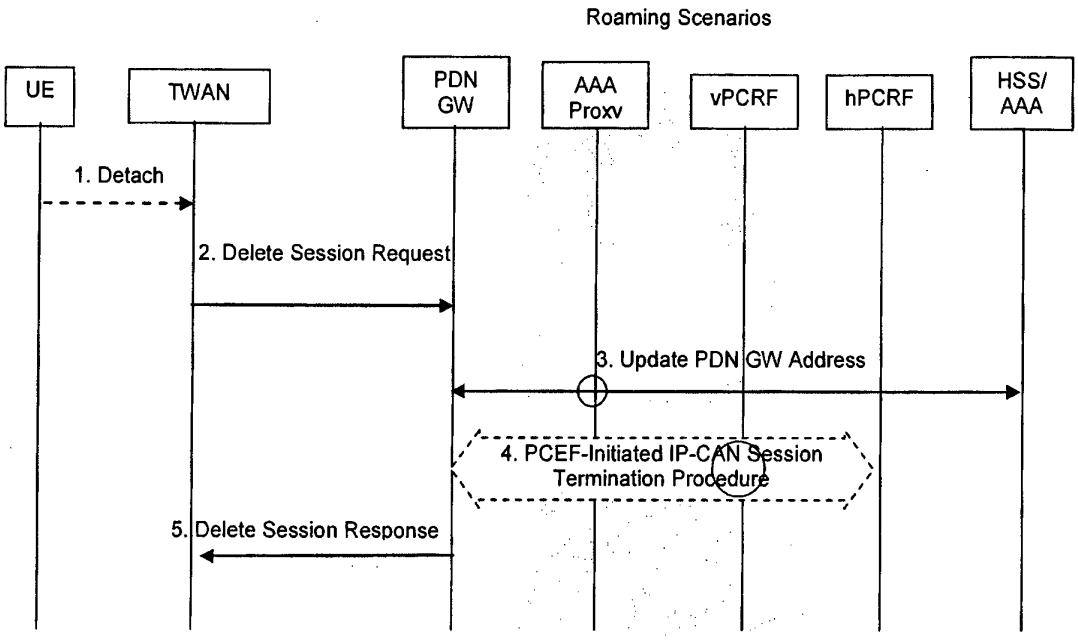

Roaming Scenarios
UE
TWAN
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. Detach
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response

Fig. 11

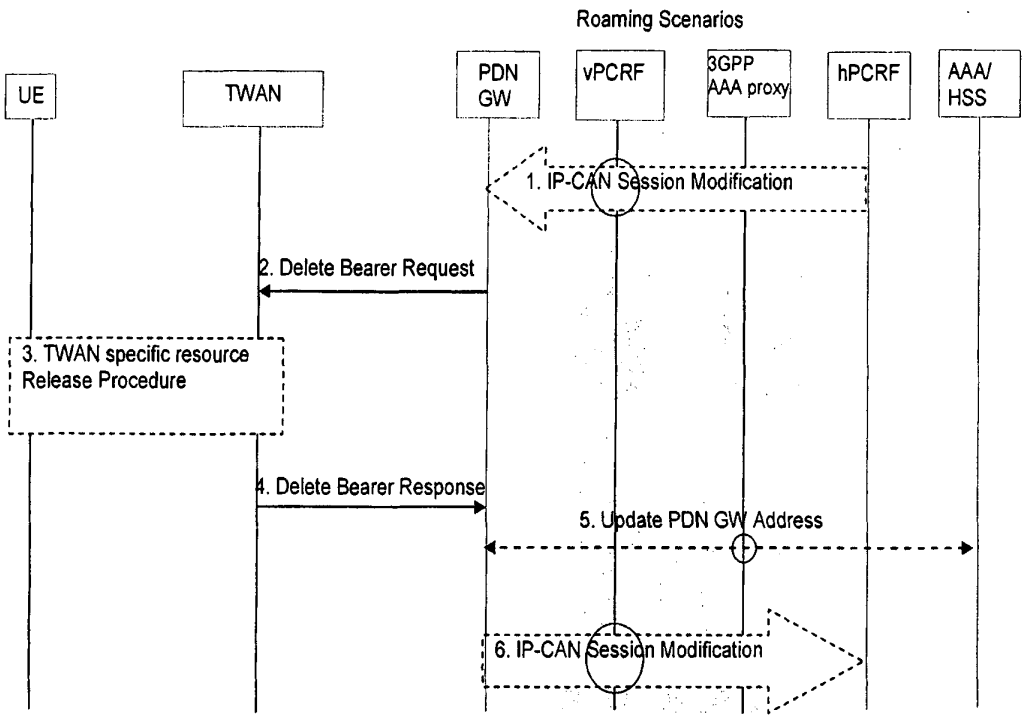

Roaming Scenarios
UE
TWAN
PDN GW
vPCRF
3GPP AAA proxy
hPCRF
AAA/ HSS
1. IP-CAN Session Modification
2. Delete Bearer Request
3. TWAN specific resource Release Procedure
4. Delete Bearer Response
5. Update PDN GW Address
6. IP-CAN Session Modification

Fig. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/001660

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/12 H04W76/02
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 075 959 A1 (THOMSON LICENSING [FR]) 1 July 2009 (2009-07-01)	1,12-18, 31
Y	paragraph [0002]	2-11
A	paragraph [0021] - paragraph [0036]; figures 2-4	19-30

Y	CISCO ET AL: "Multiple APN Support - Approaches and Considerations", 3GPP DRAFT; S2-123004_FS-SAMOG_MULTIPLE-APN-ARCHITECTU RAL-OPTIONS, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Barcelona, Spain, 3 July 2012 (2012-07-03), XP050633521, [retrieved on 2012-07-03]	2-11
A	page 3 - page 5	1,12-31

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2013	06/12/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Eraso Helguera, J

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/174962 A1 (GUREVICH DAVID [US]) 11 August 2005 (2005-08-11) paragraph [0002] - paragraph [0071]; figures 1-13	1-31
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on S2a Mobility based On GTP & WLAN access to EPC (SaMOG); Stage 2 (Release 12)", 3GPP STANDARD; 3GPP TR 23.852, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V1.2.0, 20 July 2012 (2012-07-20), pages 1-63, XP050648988, [retrieved on 2012-07-20] paragraph [0008]	1-31

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2013/001660

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2075959 A1	01-07-2009	EP 2075959 A1	01-07-2009
		EP 2232778 A1	29-09-2010
		JP 2011508551 A	10-03-2011
		KR 20100103639 A	27-09-2010
		US 2010290391 A1	18-11-2010
		WO 2009083430 A1	09-07-2009
US 2005174962 A1	11-08-2005	EP 1714399 A2	25-10-2006
		JP 2007527156 A	20-09-2007
		US 2005174962 A1	11-08-2005
		WO 2005076889 A2	25-08-2005

Form PCT/ISA/210 (patent family annex) (April 2005)

PTO/AIA/80 (07-17)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☑ Practitioners associated with Customer Number: 30565

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☑ The address associated with Customer Number: 30565

OR

☐

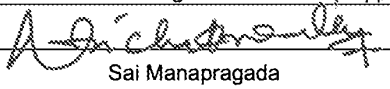
Firm or individual name		
Address		
City	State	Zip
Country		
Telephone	Email	

Assignee name and address: XiFi Networks R&D Inc.
21214 Chelton Beach Drive
Cypress, TX 77433
United States

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature		Date	July 29, 2023
Name	Sai Manapragada	Telephone	(510) 543-9655
Title	CEO		

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

(12) UK Patent Application (19) GB (11) 2516132 (13) A

(43) Date of A Publication 14.01.2015

(21) Application No: 1402416.0

(22) Date of Filing: 12.02.2014

(30) Priority Data:
(31) 1302414 (32) 12.02.2013 (33) GB

(71) Applicant(s):
Sepura plc
(Incorporated in the United Kingdom)
Radio House, St Andrews Road, CAMBRIDGE, CB4 1GR, United Kingdom

(72) Inventor(s):
Peter Stephens
Paul Nodar

(74) Agent and/or Address for Service:
Dehns
St. Bride's House, 10 Salisbury Square, LONDON, EC4Y 8JD, United Kingdom

(51) INT CL:
H04W 84/08 (2009.01) ***H04L 5/00*** (2006.01)
H04L 27/26 (2006.01)

(56) Documents Cited:
GB 2510718 A **WO 2014/125265 A1**
MEHDI NOURI et al): TEDS: A high speed digital mobile communication air interface for professional users. IEEE Vehicular Technology Magazine IEEE, US vol. 1, no.4 1 December 2006.
ETSI TS 100 392-2 v3.6.1 (2013-05). Terrestrial Trunked Radio (TETRA); Voice plus data (V+D); Part 2: Air Interface (AI) Section 6.2 and page 73

(58) Field of Search:
INT CL **H04B, H04L, H04W**
Other: **WPI EPODOC TXTE**

(54) Title of the Invention: **Mobile communications system**
Abstract Title: **Providing a higher capacity communications system that can operate in narrower bands than existing TETRA systems**

(57) A modulation scheme for use in a digital mobile radio communications system. The modulation scheme uses a four slot time-division multiple access scheme with 12.5 kHz channels. Each 12.5 kHz channel contains plural sub-carriers and each sub-carrier is modulated with a modulation scheme that encodes at least 4 bits per symbol. The modulation scheme can be used in a standalone mobile radio communications system, or in a hybrid mobile radio communications system that also uses standard TETRA modulation schemes. The invention can be used to provide a narrow band digital mobile radio communications system operating in 12.5 kHz channels that has a high degree of compatibility with existing TETRA systems.

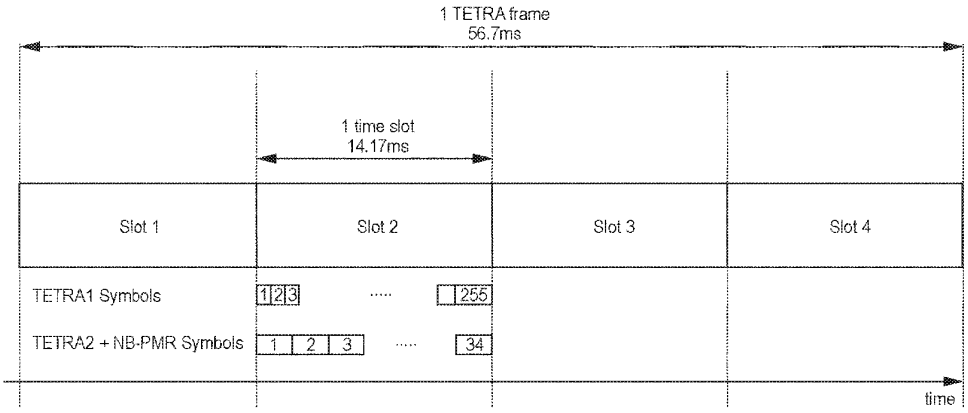


FIG. 3

GB 2516132 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

06 03 14

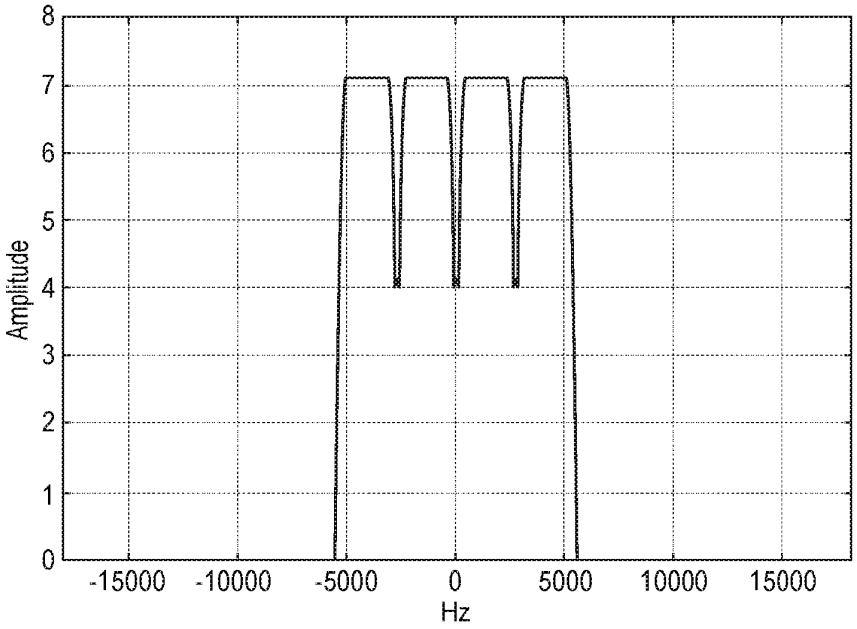


FIG. 1

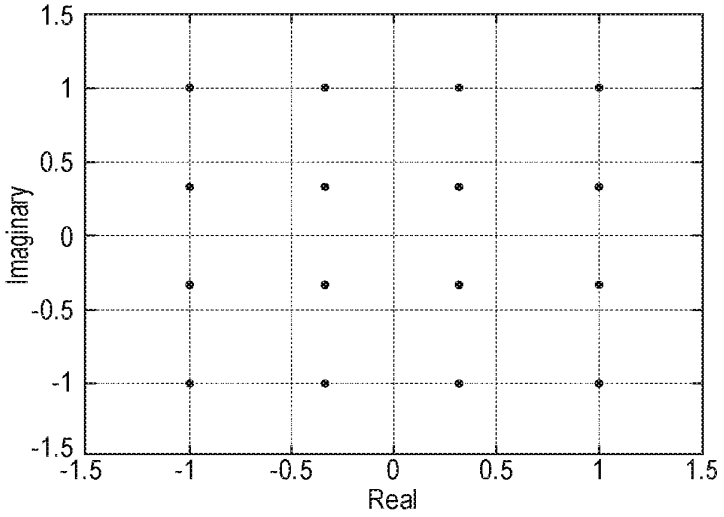


FIG. 2

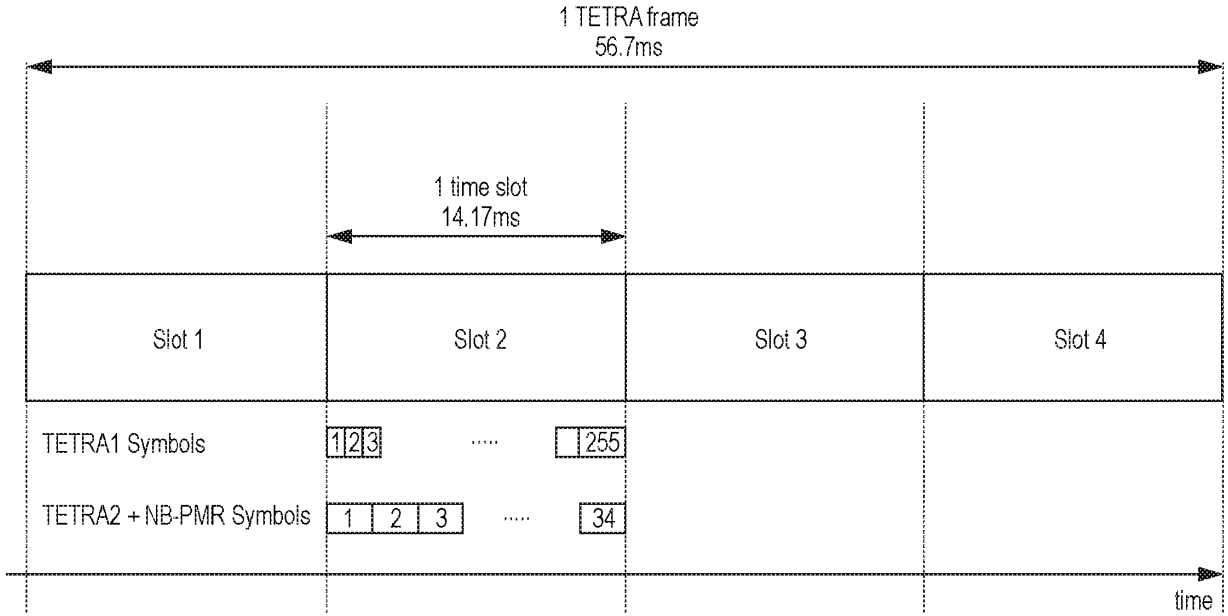


FIG. 3

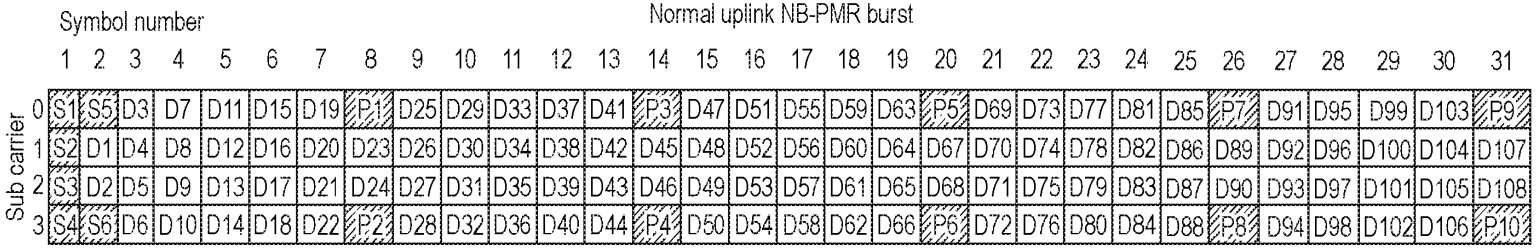


FIG. 4

Samsung Ex. 1004, Page 215 of 563

Normal downlink NB-PMR burst

Sub carrier \ Symbol number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
0	S1	S5	D1	D5	D9	D13	D17	P1	D21	D25	D29	D33	D37	P3	D41	D45	D49	D53	P5	D57	D61	D65	D69	P7	D73	D77	D81	D85	P9	D89	D93	D97	D101	D105
1	S2	H1	D2	D6	D10	D14	D18	H3	D22	D26	D30	D34	D38	H5	D42	D46	D50	D54	H7	D58	D62	D66	D70	H9	D74	D78	D82	D86	H11	D90	D94	D98	D102	D106
2	S3	H2	D3	D7	D11	D15	D19	H4	D23	D27	D31	D35	D39	H6	D43	D47	D51	D55	H8	D59	D63	D67	D71	H10	D75	D79	D83	D87	H12	D91	D95	D99	D103	D107
3	S4	S6	D4	D8	D12	D16	D20	P2	D24	D28	D32	D36	D40	P4	D44	D48	D52	D56	P6	D60	D64	D68	D72	P8	D76	D80	D84	D88	P10	D92	D96	D100	D104	D108

FIG. 5

Control uplink NB-PMR burst

Sub carrier \ Symbol number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	S1	S5	D1	D5	D9	P1	D15	D19	D23	P3	D29	D33	D37	P5
1	S2	S6	D2	D6	D10	D13	D16	D20	D24	D27	D30	D34	D38	D41
2	S3	S7	D3	D7	D11	D14	D17	D21	D25	D28	D31	D35	D39	D42
3	S4	S8	D4	D8	D12	P2	D18	D22	D26	P4	D32	D36	D40	P6

FIG. 6

Samsung Ex. 1004, Page 216 of 563

Downlink Synchronisation NB-PMR burst

Sub carrier \ Symbol number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
0	S1	S5	F1	F5	F9	F13	F17	F21	D1	P1	D5	D9	D13	D17	P3	D21	D25	D29	D33	P5	D37	D41	D45	D49	P7	D53	D57	D61	D65	P9	D69	D73	D77	D81
1	S2	H1	F2	F6	F10	F14	F18	F22	D2	H3	D6	D10	D14	D18	H5	D22	D26	D30	D34	H7	D38	D42	D46	D50	H9	D54	D58	D62	D66	H11	D70	D74	D78	D82
2	S3	H2	F3	F7	F11	F15	F19	F23	D3	H4	D7	D11	D15	D19	H6	D23	D27	D31	D35	H8	D39	D43	D47	D51	H10	D55	D59	D63	D67	H12	D71	D75	D79	D83
3	S4	S6	F4	F8	F12	F16	F20	F24	D4	P2	D8	D12	D16	D20	P4	D24	D28	D32	D36	P6	D40	D44	D48	D52	P8	D56	D60	D64	D68	P10	D72	D76	D80	D84

FIG. 7

Direct mode sync NB-PMR burst

Sub carrier \ Symbol number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	S1	S5	F1	F5	F9	F13	F17	F21	D3	D7	P1	D13	D17	D21	D25	P3	D31	D35	D39	D43	P5	D49	D53	D57	D61	P7	D67	D71	D75	D79	P9
1	S2	D1	F2	F6	F10	F14	F18	F22	D4	D8	D11	D14	D18	D22	D26	D29	D32	D36	D40	D44	D47	D50	D54	D58	D62	D65	D68	D72	D76	D80	D83
2	S3	D2	F3	F7	F11	F15	F19	F23	D5	D9	D12	D15	D19	D23	D27	D30	D33	D37	D41	D45	D48	D51	D55	D59	D63	D66	D69	D73	D77	D81	D84
3	S4	S6	F4	F8	F12	F16	F20	F24	D6	D10	P2	D16	D20	D24	D28	P4	D34	D38	D42	D46	P6	D52	D56	D60	D64	P8	D70	D74	D78	D82	P10

FIG. 8

06 03 14

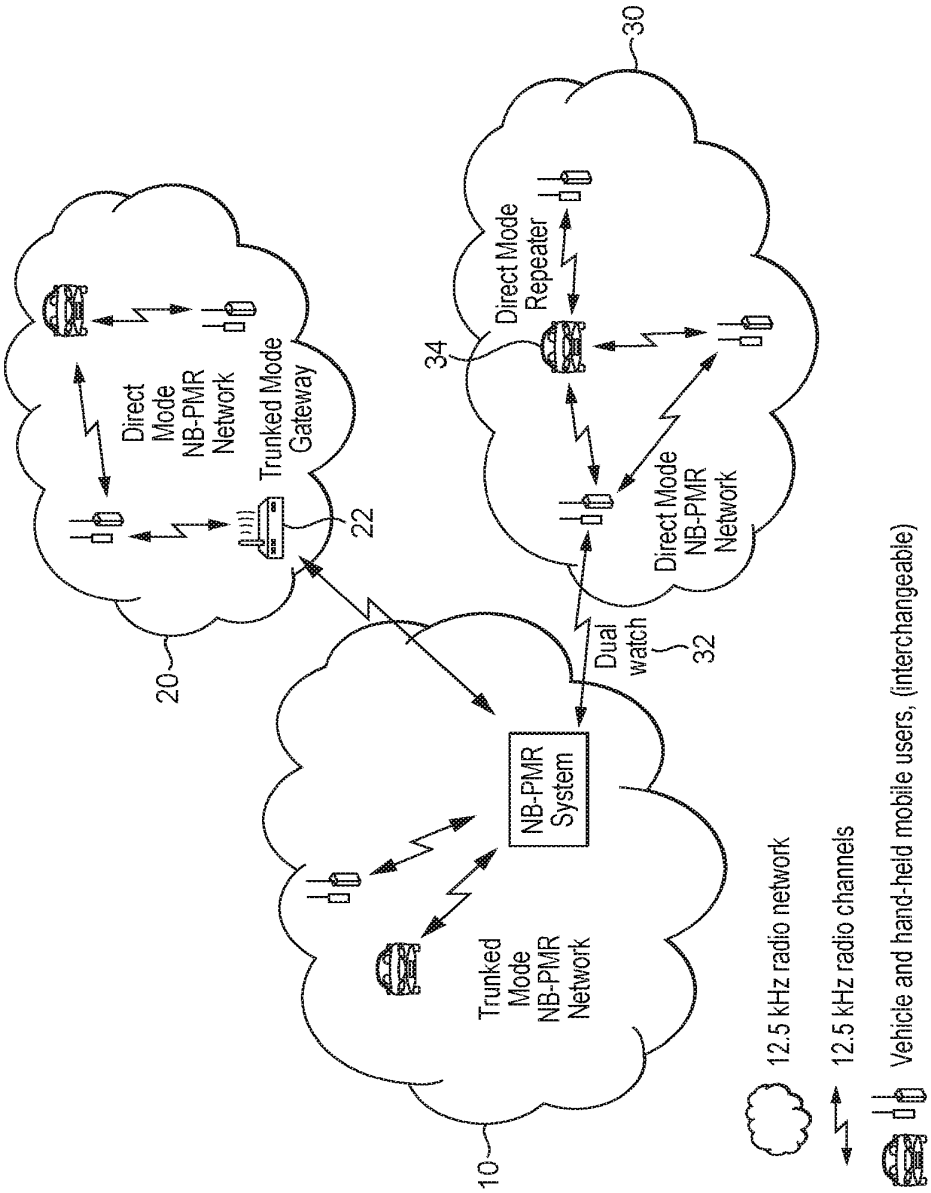

Direct Mode NB-PMR Network
Trunked Mode Gateway
22
20
Direct Mode Repeater
34
30
Direct Mode NB-PMR Network
Dual watch
32
NB-PMR System
Trunked Mode NB-PMR Network
10
12.5 kHz radio network
12.5 kHz radio channels
Vehicle and hand-held mobile users, (interchangeable)

FIG. 9

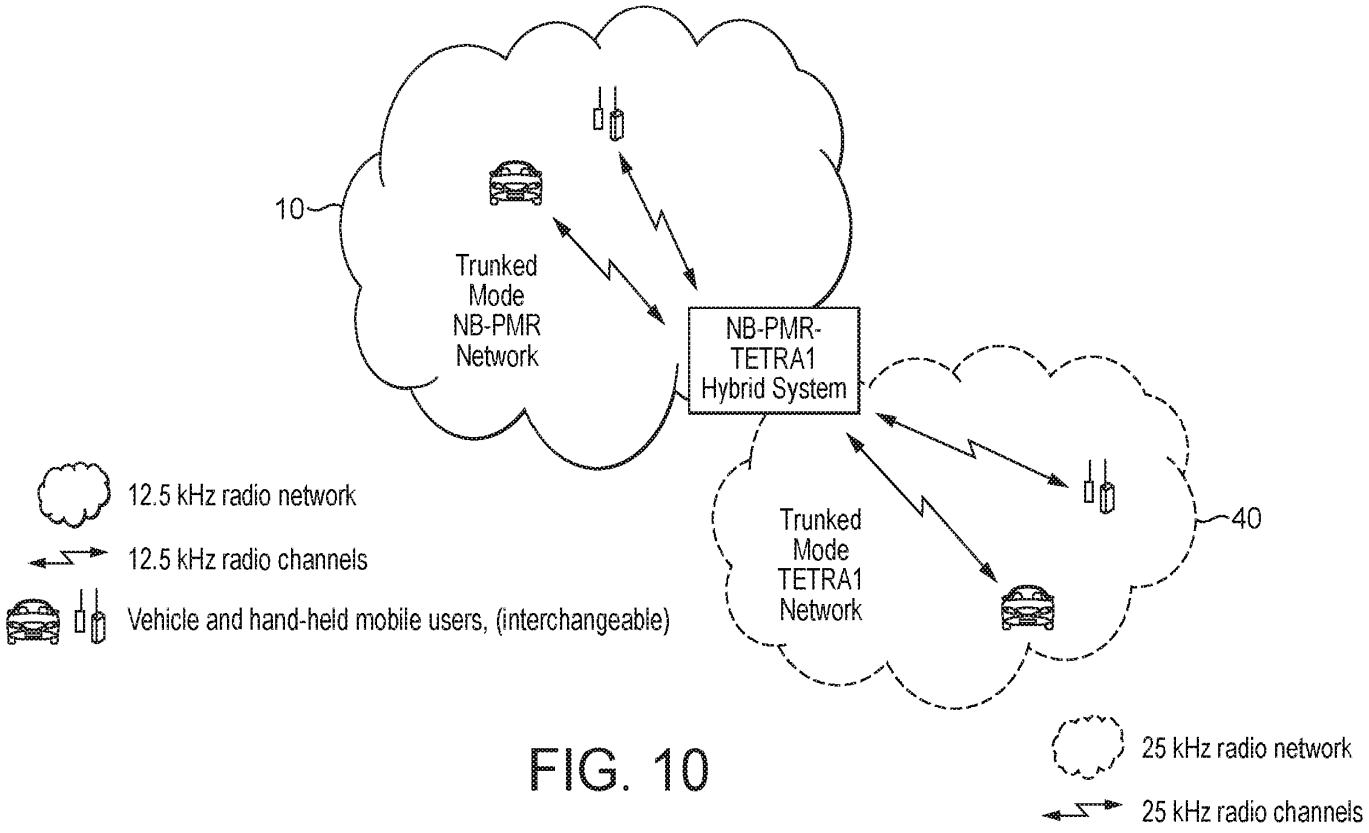


FIG. 10

Samsung Ex. 1004, Page 219 of 563

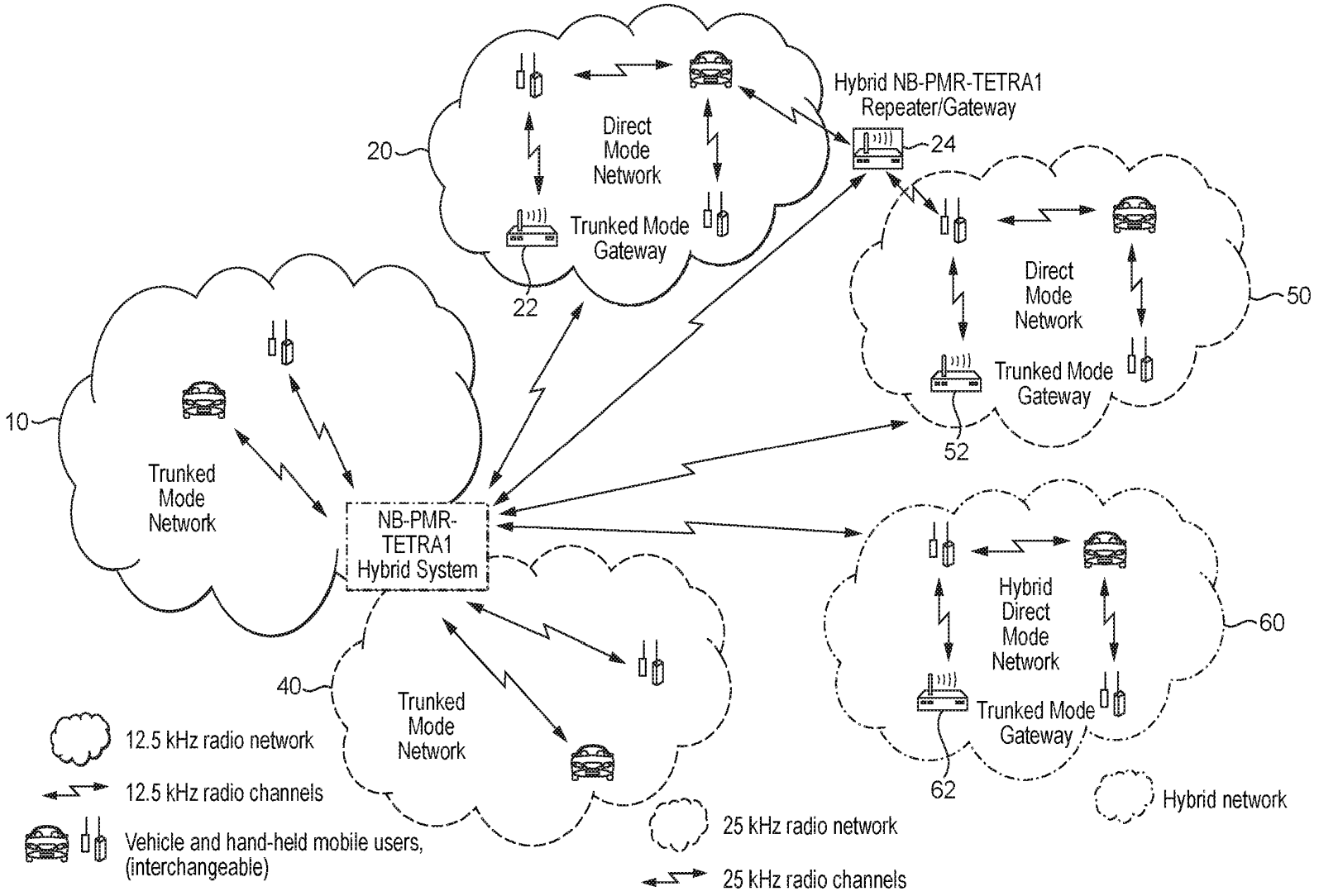


FIG. 11

Samsung Ex. 1004, Page 220 of 563

Mobile Communications System

The present invention relates to mobile communications systems, and in particular to digital mobile radio communications systems, such as the TETRA (TErrestrial TRunked RAdio) system.

Mobile radio communications systems typically use predefined frequency channels to carry signalling and traffic. The arrangement of the frequency channels, for example the frequency bandwidth of each channel, is usually specified in the telecommunications Standard with which the communications system complies, and all signalling and traffic transmitted in the system must be arranged in accordance with the defined frequency channel arrangement.

The way that the radio spectrum is allowed to be divided into frequency channels will also normally be specified by the relevant regulatory authorities. For example, in some countries and/or frequency bands, the radio frequencies available for mobile radio communication systems are divided into (allocated in) 25 kHz channels, while in other countries and/or frequency bands, the available radio frequencies are divided into 12.5 kHz channels.

Accordingly, a number of modern digital mobile radio communication systems are configured to use 25 kHz channels, and other systems are configured to use 12.5 kHz channels. For example, the TETRA (TETRA 1) system uses 25 kHz channels, while the DMR (Digital Mobile Radio) and P25 (Project 25 or APCO-25) systems use 12.5 kHz channels, and the dPMR (Digital Private Mobile Radio) system operates in a Frequency Division Multiple Access (FDMA) scheme using two 6.25 kHz channels.

There is also a recent extension to the TETRA Standard known as TETRA Release 2 (TETRA2 or TEDS) that is intended to provide higher data rates for packet data. The TEDS Standard defines a system which can operate with channels having bandwidths between 25 kHz and 150 kHz (in particular 25 kHz, 50 kHz, 100 kHz and 150 kHz).

A mobile radio communications system intended for use with a particular frequency channel arrangement will usually be optimised for that frequency channel arrangement. It will therefore not normally be, and not be expected to be, readily suitable for use with a second, different frequency channel arrangement, because it

would generate transmissions which are not appropriate for the other frequency channel arrangement.

This may not be a problem where communications systems are intended to be self-contained and not intended to interoperate with other systems. However, the Applicants have recognised that it may be desirable for radio systems to be able to operate in regions that use different frequency channel arrangements. For example, it may be desired to introduce a newer radio system (that would normally operate with a particular frequency channel arrangement) into a region where the permitted frequency channel arrangement is different. For example, with regard to the TETRA system, it may be desirable to introduce radio systems offering TETRA services into parts of the world where the radio spectrum is divided into 12.5 kHz channels. In such instances, it would not be possible to use existing TETRA systems, which operate using 25 kHz channels.

Another consideration for existing communications systems, is that over a period of time enhancements may be desirable. This could be, for example, for reasons of system capacity (e.g. because the number of users wishing to use the system has increased), or because communications applications requiring higher data rates need to be supported by the system. In such cases it may be desired to make more efficient use of the spectrum available for operation of the communications system, since radio spectrum is a scarce resource.

However, this may not be readily possible with existing mobile communications systems. For example, with regard to the existing TETRA (TETRA 1) system, each 25 kHz channel supports four users in a four slot Time Division Multiple Access (TDMA) scheme. Accordingly, the system requires the equivalent of 6.25 kHz bandwidth per voice channel, and this is the most efficient use that TETRA 1 compliant systems can make of the radio spectrum.

The existing digital mobile radio systems that operate with 12.5 kHz channels (e.g. DMR, P25, as discussed above) also generally require at least 6.25 kHz equivalent bandwidth per voice channel. For example, "Phase 1" P25 is a mixed analogue/digital system that operates with 12.5 kHz channels using FDMA. "Phase 2" P25 uses a two slot TDMA scheme. The DMR system operates with 12.5 kHz channels using a two slot TDMA scheme and the dPMR system operates an FDMA scheme with two 6.25 kHz channels. Thus, these systems at best offer only the same spectral efficiency as TETRA (TETRA 1). Furthermore, these

systems generally have reduced functionality compared to the TETRA (TETRA 1) system, and are not compatible with nor interoperable with the TETRA system.

The Applicants believe therefore that there remains a need to be able to provide reduced bandwidth/higher spectral efficiency digital mobile radio communications systems.

According to a first aspect of the present invention, there is provided a method of operating a digital mobile radio communications system, comprising:

using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol, for transmissions in the system.

According to a second aspect of the present invention, there is provided a communications terminal for a digital mobile radio communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

According to a third aspect of the present invention, there is provided a digital mobile radio communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

The present invention provides a digital mobile communications system that operates in 12.5 kHz channels, using a 4-slot TDMA arrangement and a particular form of modulation scheme for its transmissions. As will be discussed further below, this system can operate with an effective 3.125 kHz equivalent channel width per user, thereby using the radio spectrum more efficiently (providing increased capacity). Moreover, the system can, again as will be discussed further below, provide a high degree of compatibility with existing TETRA 1 systems, thereby allowing interoperability with and in existing TETRA 1 systems, and the functionality of TETRA 1 to be supported by this new mobile communications system. For example, as will be discussed further below, the system of the present invention, in its preferred embodiments at least, can still use the TETRA 1 slot and

frame structure (i.e. 4 timeslots per frame, eighteen frames per-multiframe, slot and frame durations, etc.), and when doing so provide and support data rates and timeslot payload capacities that are compatible with and correspond to TETRA 1.

Thus, the present invention can provide a higher capacity (more radio spectrum efficient) communications system, that can operate in narrower frequency bands than existing TETRA systems, while still being able to remain compatible with many aspects of existing TETRA systems, such as the TETRA transmission format and structure, and support a comprehensive set of TETRA functions and services. The present invention can accordingly be used, for example, to provide a narrow band digital mobile radio communications system operating in 12.5 kHz channels that has a high degree of compatibility with existing TETRA systems.

The enhanced communications system and scheme of the present invention can also accordingly be used in and with existing TETRA (for example) communications networks and equipment, without the need for substantial modifications and changes to that equipment, and without the need for significant investment in new equipment. This is particularly true for more modern TETRA communications systems that are able to support both TETRA 1 and TEDS functionalities.

Thus the scheme of the present invention can be used to upgrade an existing TETRA system in a way which requires no new frequencies and requires relatively minimal new equipment investment. Similarly, the invention can be employed in green field TETRA systems to enhance the basic TETRA system capability. It can also be used to allow a substantially TETRA compatible and/or TETRA-based system to be deployed in regions and frequency bands that specify 12.5 kHz, rather than 25 kHz, radio channels.

The present invention can thus effectively provide a "narrow band" mobile communications system, that can, for example, in particular, be used in and with TETRA systems and TETRA equipment, and can support TETRA services.

It should be noted here that the present invention does not simply use the existing TETRA (TETRA 1) system but halve the bandwidth of the filter (i.e. simply halve the channel bandwidth). This is because although this would provide an appropriately narrow channel bandwidth, the Applicants have recognised that such a scheme would result in severe distortion of the modulated signal. Similarly, while one could in order to address the above problems with distortion, in principle simply halve the modulation rate of the signal (i.e. double the symbol period), the

Applicants have recognised that in that case the bit rate of the system would then be halved, and the system would then at best comprise a two slot TDMA scheme, thereby not fully preserving the TETRA 1 functionality, nor increasing the spectral efficiency over TETRA 1.

To address this, the present invention uses, for information-carrying symbols such as the header and/or payload (data) symbols, at least, a higher level modulation scheme that encodes more (and at least 4) bits per symbol. This then allows longer symbol periods to be used, whilst still achieving a given bit rate. However, the present invention does not simply use any form of higher level modulation scheme, but uses multi-sub-carriers with a higher level modulation scheme. This is because the Applicants have recognised that using a single carrier with a higher level modulation scheme would still require relatively high symbol rates, but at higher symbol rates may not perform well in fading channels due to multipath distortion. The present invention avoids this by using multi-sub-carriers with a higher level modulation scheme, as by using a multi-sub-carrier arrangement, the symbol rate for each individual sub-carrier can be relatively lower (and thus the symbol duration can be relatively longer).

The communications station of the present invention may be a mobile station or a base station, as is known in the art. In one preferred embodiment it is a base station. In another preferred embodiment it is a mobile station.

The present invention uses a four-slot TDMA arrangement. While any suitable and desired such arrangement can be used in the present invention, in a particularly preferred embodiment, a 4-slot TDMA time slot and frame structure having the timings (the timing structure) of TETRA 1 (and thus TEDS) is used. Thus, in a preferred embodiment, the system of the present invention uses frames of 4-timeslots and multiframes of 18 frames. Preferably each time-slot is 14.17 ms long, and each frame is 56.7 ms long. This facilitates compatibility with TETRA 1 and TEDS systems.

Each timeslot preferably contains a given (and the same) number of symbols per sub-carrier. Preferably the number of symbols per-sub-carrier per timeslot is even, as that then facilitates the transmission of half-slots, and therefore compatibility with TETRA 1. Where, as will be discussed further below, the modulation scheme of the present invention encodes 4 bits per symbol, each timeslot preferably contains 34 such symbols per-sub-carrier. As will be discussed further below, this then means that with timeslots corresponding to the TETRA 1

timing structure, the scheme of the present invention can support a timeslot payload bit capacity (bit rate) that is compatible with existing TETRA systems, protocols and equipment.

Each 12.5 kHz channel that is used in the present invention may be divided into the requisite multiple sub-carriers (sub-channels) in any desired and suitable manner. Most preferably, the sub-carriers (sub-channels) are equally spaced within the channel. Any (plural) number of sub-carriers can be used. Preferably not more than eight sub-carriers are used. In a particularly preferred embodiment, four sub-carriers are used. This has been found to facilitate the use of longer symbols, thereby making the signal more robust in mobile fading propagation channels, but without making the symbols so long that other problems such as excessive latency waiting for symbols to arrive then arise. In a preferred such embodiment, a sub-carrier spacing of 2.7 kHz is used in each 12.5 kHz channel. In other embodiments, two, six, or eight sub-carriers can be used. The system may use only a single 12.5 kHz channel, but as will be appreciated by those skilled in the art, plural 12.5 kHz channels are preferably provided (supported) and used.

The modulation scheme that is used in the present invention can be any desired and suitable modulation scheme that encodes at least four bits per symbol. Suitable modulation schemes include QAM, PSK/DPSK, or OFDM schemes. Each sub-carrier should be and is preferably modulated using the same modulation scheme.

In a particularly preferred embodiment, 16-QAM is used. This encodes 4-bits per-symbol, and thus when used in a timeslot having the TETRA 1 timing structure that can contain 34 symbols per sub-carrier per timeslot, will provide 4 x 34 = 136 bits per sub-carrier per timeslot, and so can be used to provide 544 bits (4 x 136) per timeslot where 4 sub-carriers (each carrying 34 16-QAM symbols) are being used. As will be discussed further below, this bit capacity can be used to provide a system that is compatible with TETRA.

In a preferred embodiment, the modulation scheme of the present invention uses 2400 symbols per second, sub-carrier spacing of 2.7 kHz, and an RRC modulation filter with alpha=0.2. In this case, the nominal overall modulation bandwidth (for a frequency channel) will be 10.8 kHz. This has the effect that the modulation scheme will then generally (apart from the number of sub-carriers) correspond to and be compatible with the modulation scheme that is used in TEDS.

The 4-bit per symbol modulation scheme, such as 16-QAM, should be, and preferably is, used for the information-carrying symbols, such as header and payload (data) symbols in each burst. However, other symbols in a burst, such as pilot and synchronisation symbols, need not use the 4-bit per symbol modulation scheme, and may, e.g. have their own particular symbol constellations. Thus, the requirement is that at least some data (payload) symbols on a sub-carrier are encoded using a 4-bit per symbol modulation scheme.

The present invention preferably uses particular (and identifiable) burst structures for its transmissions (as is conventional in mobile communications systems), so as to, e.g., allow particular forms (types) of transmissions to be readily identified and processed.

While it would be possible to define and use any desired and suitable set of burst types for this purpose, in a particularly preferred embodiment, burst types that correspond to burst types that are used in TETRA 1 are preferably used. This facilitates compatibility with TETRA 1.

Thus, in a preferred embodiment, the system of the present invention supports and uses one or more of, and preferably all of the following burst types: normal uplink burst; normal downlink burst; control uplink burst; and downlink synchronisation bursts.

In a preferred embodiment, unlike for TETRA 1, the system of the present invention does not use (nor support) discontinuous downlink bursts. In this regard, the Applicants have recognised that it is not necessary to provide the facility to transmit discontinuous downlink bursts. This is because discontinuous downlink bursts solely serve to provide ramp up and ramp down periods for base stations, but the Applicants have realised that in practice this functionality is not generally needed, so these bursts can be omitted, thereby simplifying the burst types to be used.

Furthermore, the Applicants have recognised that it would in fact be advantageous to operate the system without using discontinuous downlink bursts (i.e. using continuous downlink bursts (only)), since the concatenation of slots in the continuous downlink bursts will allow (a mobile station of) the system to use some of the synchronisation and pilot symbols from the current (its own) and from the next (or previous) slot for synchronisation and equalisation purposes. This then means that fewer synchronisation and pilot symbols need to be provided in each

slot (each burst), so that more symbols in a given burst can be used as data symbols, thereby providing an increased useful payload capacity in each timeslot.

In another embodiment, ramp down periods, preferably periodic ramp down periods, are provided. In this embodiment, the system of the present invention preferably uses (supports) a dedicated ramp down burst. This then can be used for linearization of base stations.

In a particularly preferred embodiment, the burst types that are used in the present invention have a close correspondence to burst types used in TETRA 1, and formats (burst structures) that are similar to but modified with respect to the existing TEDS burst formats.

The Applicants have recognised in particular that it would not be possible to simply use the TEDS (TETRA 2) synchronisation and pilot symbol structures in the scheme of the present invention, as this would result in a payload which is too small for TETRA 1 compatibility. Instead, the present invention uses new pilot and synchronisation symbol arrangements that provide space for sufficient payload symbols (and still provide adequate synchronisation and equalisation performance).

In general, each burst preferably includes pilot symbols spaced to facilitate equalisation at the receiver, synchronisation symbols to facilitate frame and symbol timing recovery at the receiver, and data symbols for carrying the useful payload (and any required header). The data symbols are preferably ordered regularly across and along the multiple sub-carriers in the 12.5 kHz channel. In a preferred embodiment, pilot symbols are included (used) in the outer sub-carriers in the channel only (so in the outer two, but not the inner two, sub-carriers where four sub-carriers are being used). This helps to provide more symbols for data purposes. The pilot symbols are preferably spaced (approximately) evenly in time and frequency.

In a preferred embodiment, the burst structures that are used in the present invention have relatively fewer synchronisation and/or pilot symbols with respect to the existing TEDS corresponding burst types. Most preferably, the ratio of synchronisation and pilot symbols to payload symbols is smaller in burst structures of the present invention with respect to the burst structures of existing TEDS corresponding burst types. In this regard, the Applicants have recognised that in the narrow band system of the present invention, the performance of the synchronisation is less critical to the overall performance of the system. Equally, the Applicants have recognised that it is possible to space the pilot symbols further

apart with respect to the existing corresponding TEDS burst types. Thus, it is possible to reduce the proportion of synchronisation and/or pilot symbols with respect to the existing TEDS corresponding burst types, and thereby increase the proportion of symbols available for the payload (e.g. to provide a sufficient payload for TETRA 1 compatibility).

In a preferred embodiment of the present invention, the system uses a fixed constant modulation level (supports a fixed modulation level only). This then means that header symbols can be removed from the uplink bursts and/or some of the downlink symbols can be removed (with respect to the existing TEDS corresponding burst types) in the burst structures used in the present invention (these symbols are used in TEDS to indicate the modulation level being used). Again, this increases the number of symbols available for the payload.

In a preferred embodiment, for burst types which include header symbols, the header symbols are arranged to be close to pilot symbols. Most preferably, the header symbols are arranged to be adjacent in time and/or in frequency to pilot symbols. This has the advantage of reducing equalisation errors.

The preferred burst structures allow, for example, the four sub-carrier modulation scheme of the present invention having the preferred symbol duration and slot duration described above (i.e. providing a total of 136 (4 x 34) symbols per timeslot) (and thus a "raw" bit rate of 544 bits per timeslot) (with four bits per symbol) (on the downlink) to provide sufficient capacity to support TETRA 1 compatible payloads which require 432 bits per timeslot, and an additional 30 bits for the AACH channel on the downlink, whilst still allocating a number of symbols in each slot as synchronisation symbols and as pilot symbols in order to support synchronisation and channel equalisation, etc.. (TETRA 1 provides a "raw" bit rate of 510 bits per timeslot.) (As is known in the art, synchronisation symbols are used to allow a receiver to determine the correct timing of bursts, while pilot symbols are for channel equalisation so that the information payload can be properly recovered from the modulated signal.)

(The equivalent uplink capacity, allowing for ramp-up and down periods, is 124 symbols per timeslot (i.e. 4x31 symbols per timeslot), or 496 bits per timeslot.)

The preferred burst structures of the present invention can thus be used to achieve payload capacities that are sufficient for compatibility with TETRA 1.

The present invention similarly preferably uses particular (and identifiable) logical channels for its transmissions (as is conventional in mobile communications

systems), so as to, e.g., allow particular forms (types) of transmissions to be readily identified and processed.

While it would be possible to define and use any desired and suitable set of logical channels and mapping of logical channels onto bursts for this purpose, in a particularly preferred embodiment, logical channels and logical channel mappings that are based on, and that correspond to, logical channel types and mappings that are used in TETRA 1 are preferably used.

Thus, in a preferred embodiment, the system of the present invention supports and uses logical channels that are used in TETRA 1.

However, in a preferred embodiment, the AACH channel is transmitted using 16-QAM symbols, thereby reducing the number of AACH symbols that are used compared to TEDS, and no logical channel equivalent to the TEDS SICH channel on the uplink is provided, as this is not needed (since in the preferred embodiment of the present invention as described above, a fixed modulation level is used (as is known in the art, SICH is used in TEDS to dynamically indicate the modulation level)).

The system of the present invention preferably uses a layered protocol arrangement for its protocol (as is conventional in mobile communications systems). While the protocol that is used in the present invention could be configured and arranged in any desired manner, in a particularly preferred embodiment, only layer 1 (i.e. the "physical layer") and part of layer 2 (i.e. part of the "data link layer") are changed with respect to the protocol layers of the TETRA (TETRA 1) system. Most preferably, only layer 1 and the Lower MAC layers are changed. In this embodiment, protocol layers above the Lower MAC layer (i.e. the Upper MAC layer and above) are accordingly preferably the same as in TETRA 1. Thus, higher level protocol layers, services and applications are preferably unchanged with respect to TETRA 1.

This allows many or all of the functionalities of TETRA 1 to be preserved, and means that the protocol changes necessary to existing TETRA equipment for it to be able to use the modulation scheme of the present invention can be relatively small. Thus the changes necessary to existing TETRA equipment for it to be able to use the scheme of the present invention can be relatively small. Equally, the new scheme can have a high degree of interoperability with existing TETRA systems.

This is possible because, as discussed above, the present invention can, in its preferred embodiments at least, provide (and be configured as) a system that apart from at the physical layer, can be very similar to, and compatible with, existing TETRA 1 (particularly in terms of the payload bit rate that can be delivered to the higher protocol layers once signalling overhead has been removed).

In alternative embodiments, various changes to the higher level protocol layers (i.e. changes to the protocol layers above the Lower MAC layer) may be made as desired. For example, it could in some instances be advantageous to configure the system such that it has some knowledge of the particular modulation scheme or schemes supported by each mobile unit within the system, so that the mobile units can be assigned to appropriate frequency channels.

In a particularly preferred embodiment, the system of the present invention is configured to support Direct Mode Operation (DMO), i.e. direct terminal to terminal communications (not via the network infrastructure). This again helps to provide interoperability and compatibility with existing TETRA 1 systems (and the functionality of TETRA 1 systems).

Where DMO is supported, the system of the present invention preferably also has a defined direct mode synchronisation burst structure and a defined direct mode normal burst structure. In a preferred embodiment, the direct mode normal burst has the same structure as a normal uplink burst for the trunked mode operation.

The present invention may be used in and for any suitable and desired mobile communications system. Indeed, it may be used to provide a stand-alone "narrow band" mobile communications system if desired.

However, as will be appreciated from the above, the present invention is envisaged as having particular application to, and being particularly advantageous for, use with or in a TETRA mobile communications system, and/or with TETRA communications stations.

Thus, in a particularly preferred embodiment, the present invention is used in or with a TETRA mobile communications system, and the mobile communications station is a TETRA communications station (i.e. a communications station that can operate according to the TETRA standard, as well as in the manner of the present invention).

Thus, according to another aspect of the present invention, there is provided a method of operating a TETRA-compatible mobile communications system, comprising:

using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol, for transmissions in the system.

According to another aspect of the present invention, there is provided a communications terminal for a TETRA-compatible mobile communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

According to another aspect of the present invention, there is provided a TETRA-compatible mobile communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

As will be appreciated by those skilled in the art, these embodiments and aspects of the present invention can and preferably do include any one or more or all of the preferred and optional features of the invention described herein, as appropriate.

It is envisaged that the present invention may operate as a standalone "narrow band" TETRA-compatible system simply operating using the "narrow band" modulation scheme of the present invention. In this case the system infrastructure and mobile terminals could still be closely based on, and reuse many aspects of, existing TETRA 1 infrastructure and mobile terminals, with the only modifications needing to be made being the modifications discussed above to handle the new modulation scheme of the present invention at the physical and potentially lower MAC layer of the TETRA 1 protocol.

However, it is also envisaged that a system of the present invention could be operated simultaneously with and could coexist with a "standard" TETRA system, for example. In this case it is preferred that the system will comprise base

stations that can support normal TETRA 1 25 kHz RF channels and/or TEDS 25 kHz to 150 kHz RF channels, as well as the narrow band, 12.5 kHz RF channels, of the present invention. In this case, base stations are preferably able to operate using both modulation schemes. Mobile terminals may be capable of operating only using existing TETRA 1 25 kHz channels and/or TEDS 25 kHz to 150 kHz channels, or only in the narrow band 12.5 kHz channels, or both. For example, some mobile stations are preferably able to operate in both modes and to act as gateways between the two transmission schemes, i.e. receive incoming signals on 25 kHz channels and send outgoing signals on 12.5 kHz channels, and/or vice-versa, in networks that have a mixture of 25 kHz and 12.5 kHz channels.

The system is preferably configured to be able to switch dynamically between the narrow band and TETRA operation, for example based on equipment capability and/or other factors such as quality of service. The system infrastructure could, e.g., allocate a mobile station to a narrow band channel or a normal TETRA channel, based on its knowledge of the mobile station's capability.

Thus, in a particularly preferred embodiment, it is envisaged that TETRA systems will use the modulation scheme of the present invention together with the existing π/4 DQPSK TETRA modulation and/or TEDS modulation. In other words, channels modulated with the different modulation schemes will coexist in the system. Such an arrangement will then support standard TETRA equipment and the "narrow band" TETRA-compatible equipment and system of the present invention at the same time, thus maintaining compatibility between the old and new system (and equipment). Such a system preferably uses the normal 25 kHz TETRA channels with existing π/4 DQPSK TETRA modulation, but also provides narrow band 12.5 kHz channels in accordance with the present invention.

Thus, the present invention also extends to hybrid radio systems comprising one or more traditional TETRA 1 mobile units operating in 25 kHz channels, and one or more mobile units of the present invention operating in 12.5 kHz channels.

Thus, according to an aspect of the present invention, there is provided a method of operating a TETRA mobile communications system, comprising:

using the TETRA π/4 DQPSK modulation scheme for transmissions in the system; and

using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier

being modulated with a modulation scheme that encodes at least 4 bits per symbol, for transmissions in the system.

According to another aspect of the present invention, there is provided a communications station for a TETRA mobile communications system, comprising:

means for making transmissions using the TETRA π/4 DQPSK modulation scheme; and

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

According to another aspect of the present invention, there is provided a TETRA mobile communications system, comprising:

one or more communications stations capable of making transmissions using the TETRA π/4 DQPSK modulation scheme; and

one or more communications stations capable of making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

As will be appreciated by those skilled in the art, these embodiments and aspects of the present invention can and preferably do include any one or more or all of the preferred and optional features of the invention described herein, as appropriate.

In these arrangements, it is preferred that signalling on a π/4 DQPSK modulated channel is used to indicate the availability of the "narrow band" channels of the present invention, as appropriate. Thus the system preferably signals on a π/4-DQPSK modulation channel an indication that the "narrow band" modulation scheme of the present invention is available.

For example, in embodiments, a base station of the system can indicate its capabilities (e.g. its "narrow band" capability) using one of the reserved “modulation mode” and/or “bandwidth elements" in the “channel characteristics” element that is sent in the D-NWRK BROADCAST EXTENSION PDU (EN 300 392-2 clauses 18.4.1.4.1b and 18.5.5a). Alternatively, a spare value in the augmented channel allocation (EN 300 292-2 clause 21.5.2) could be used.

Equally, in embodiments, a communications terminal (mobile station) can indicate its capabilities (e.g. its "narrow band" capability) to the communications

system during registration (e.g. using the U-LOCATION UPDATE PDU in the optional “class of MS” and/or “extended capabilities” information elements (as will be appreciated by those skilled in the art, there are spare (reserved) bits in the extended capabilities element (EN300 392-2 clause 16.10.10a))). Alternatively, an unused QAM bandwidth value in the extended capabilities could be used. This information can be used by the communications system to allocate an appropriate channel to the communications terminal.

Where a TETRA system supports both "normal" TETRA π/4 DQPSK modulated channels operating at 25 kHz channels and "narrow band" operation in the manner of the present invention operating in 12.5 kHz channels, respective synchronisation bursts for both modulation schemes are preferably provided, but are preferably configured and arranged such that a TETRA 1 terminal scanning for a TETRA 1 synchronisation burst will not detect the "narrow band" modulation scheme synchronisation burst, but a "narrow band" capable terminal scanning for synchronisation bursts will be able to detect both types of synchronisation burst and discriminate between the two. This will then allow a base station receiver or a mobile receiver to be able to detect whether an incoming signal is a 25 kHz channel signal or a 12.5 kHz channel signal.

The present invention also extends to apparatus for allowing a TETRA communications station (which could be a base station or a mobile station as is known in the art) to use the modulation schemes of the present invention.

As will be appreciated by those skilled in the art, all of the described aspects and embodiments of the present invention can and preferably do include any one or more or all of the preferred and optional features of the invention described herein, as appropriate.

The methods in accordance with the present invention may be implemented at least partially using software e.g. computer programs. It will thus be seen that when viewed from further aspects the present invention provides computer software specifically adapted to carry out the methods hereinabove described when installed on data processing means, and a computer program element comprising computer software code portions for performing the methods hereinabove described when the program element is run on data processing means. The invention also extends to a computer software carrier comprising such software which when used to operate a communications system and a communications station comprising data processing means causes in conjunction with said data processing means said system or

station to carry out the steps of the method of the present invention. Such a computer software carrier could be a physical storage medium such as a ROM chip, CD ROM or disk, or could be a signal such as an electronic signal over wires, an optical signal or a radio signal such as to a satellite or the like.

It will further be appreciated that not all steps of the method of the invention need be carried out by computer software and thus from a further broad aspect the present invention provides computer software and such software installed on a computer software carrier for carrying out at least one of the steps of the methods set out hereinabove.

A number of preferred embodiments of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 shows an exemplary spectrum of a single 12.5 kHz channel for a preferred embodiment of a narrow band mobile communications system in accordance with the present invention;

Figure 2 shows the symbol constellation diagram for a modulation scheme in accordance with a preferred embodiment of the present invention;

Figure 3 illustrates the structure of a frame for use in a preferred embodiment of the present invention;

Figures 4-7 show preferred embodiments of the normal uplink burst structure (Figure 4), the normal downlink burst structure (Figure 5), the control uplink burst structure (Figure 6), and the downlink synchronisation burst structure (Figure 7), to be used in preferred embodiments of the present invention;

Figure 8 shows a preferred embodiment of a DMO synchronisation burst structure to be used in preferred embodiments of the present invention;

Figure 9 shows a schematic diagram of an exemplary hybrid mobile communications system in accordance with an embodiment of the present invention;

Figure 10 shows a schematic diagram of an exemplary hybrid mobile communications system in accordance with an embodiment of the present invention; and

Figure 11 shows a schematic diagram of another exemplary hybrid mobile communications system in accordance with an embodiment of the present invention.

A preferred embodiment of the present invention will now be described with particular reference to a narrow band TETRA-compatible mobile communications system in which 12.5 kHz channels are used for transmission. However, as will be appreciated, the present invention is not exclusively limited to such an arrangement and will be applicable to other radio Standards and systems.

For convenience, the narrow band communication scheme of the present embodiment will be referred to as NB-PMR.

Figure 1 shows an exemplary spectrum of a single 12.5 kHz channel that is used in this embodiment of the present invention. While Figure 1 illustrates a spectrum for one such channel, it will be appreciated that in practice preferably plural 12.5 kHz channels are provided (supported) and used.

According to this embodiment, and as shown in Figure 1, each 12.5 kHz channel carries (is divided into) four equally spaced sub-carriers, having a spacing of 2.7 kHz. The modulation scheme uses 2400 symbols per second, and an RRC modulation filter with alpha=0.2. Accordingly, the nominal overall modulation bandwidth provided within the 12.5 kHz channel is 10.8 kHz.

A 16-QAM modulation scheme is used to modulate the data and header symbols on each respective sub-carrier in the 12.5 kHz channel. Figure 2 shows the symbol constellation diagram for the 16-QAM modulation scheme which is used in this embodiment of the present invention. This modulation scheme encodes 4-bits per-symbol. Other modulation schemes could be used, if desired.

Figure 3 illustrates the timeslot and frame structure that is used in this preferred embodiment of the present invention. As discussed above, and as shown in Figure 3, a four-slot TDMA arrangement, having the timing structure of TETRA 1 is used. Thus, each frame has four timeslots (shown as Slots 1 to 4), each time-slot is 14.17 ms long, and each frame is 56.7 ms long. Also, as shown in Figure 3, the arrangement is such that each timeslot contains 34 (NB-PMR) symbols per-sub-carrier. This facilitates compatibility with TETRA 1 systems whose time slot and frame structure is also shown in Figure 3 for comparison purposes.

In this arrangement, using the 16-QAM modulation scheme in a timeslot having the TETRA 1 timing structure and containing 34 symbols per sub-carrier, provides 4 x 34 = 136 bits per sub-carrier per timeslot, and so can be used to provide 544 bits (4 x 136) per timeslot where 4 sub-carriers (each carrying 34 16-QAM symbols) are being used. This bit capacity can be used to provide a system that is compatible with TETRA 1.

As well as the above modulation scheme and sub-carrier arrangement, etc., the present embodiment also uses particular burst structures for its transmissions when operating in the 12.5 kHz channels. Figures 4-8 show the burst structures that are used in the present embodiment.

Figures 4-7 show the normal uplink burst structure (Figure 4), the normal downlink burst structure (Figure 5), the control uplink burst structure (Figure 6), and the downlink synchronisation burst structure (Figure 7), used in this embodiment of the present invention.

Figure 8 shows the DMO (Direct Mode Operation) synchronisation burst structure which is used in this embodiment of the present invention for synchronising in DMO. Direct mode operation also uses a DMO normal burst structure that has the same structure as the normal uplink burst for the trunked mode operation shown in Figure 4.

In Figures 4-8, the various symbols depicted comprise data symbols (labelled D) (from the 16-QAM symbol constellation), frequency correction symbols (labelled F) (from a frequency correction symbol constellation), header symbols (labelled H) (from the 16-QAM symbol constellation), pilot symbols (labelled P) (from a pilot symbol constellation), and synchronisation symbols (labelled S) (from a synchronisation symbol constellation).

These burst structures have been designed to allow the four sub-carrier modulation scheme having the symbol duration and slot duration described above (i.e. providing a total of 136 (4 x 34) symbols per timeslot) (and thus 544 bits per timeslot) (with four bits per symbol) (on the downlink) of the present embodiment to provide sufficient capacity to support TETRA 1 compatible payloads which require 432 bits per timeslot, and an additional 30 bits for the AACH channel on the downlink, whilst still allocating a number of symbols in each slot as synchronisation symbols and as pilot symbols in order to support synchronisation and channel equalisation, etc..

(The equivalent uplink capacity, allowing for ramp-up and down periods, is 124 symbols per timeslot (i.e. 4x31 symbols per timeslot), or 496 bits per timeslot.)

Thus, the burst structures of this embodiment can be used to achieve payload capacities that are sufficient for compatibility with TETRA 1.

Other burst structures would be possible, if desired.

The present embodiment of the present invention also uses particular (and identifiable) logical channels for transmission (as is conventional in mobile

communications systems), so as to, e.g., allow particular forms (types) of transmissions to be readily identified and processed. In the present embodiment, logical channels corresponding to the TETRA 1 logical channels shown in the table below are used and supported. These logical channels are mapped onto bursts as set out in the table below.

TETRA 1 Logical Channel	**TETRA 1 Forward Error Correction (FEC) and Error Detection and Correction (EDC)**	**NB-PMR FEC**
AACH	TETRA 1 (14,30) Reed-Muller FEC. Mapped to broadcast block in TETRA 1 downlink bursts.	FEC: As TETRA1, or TEDS 3x(5,16) Reed-Muller FEC. Mapped onto the 12 Header symbols in downlink bursts (NDB, DSB). 48 bits available in 12*4 16-QAM header symbols.
BSCH	Rate 2/3 RCPC + 16 bit CRC. Mapped to Block 1 of synchronisation bursts in TETRA 1.	FEC: As TETRA 1 or replace R2/3 RCPC with Turbo code. Mapped to 30 data symbols in the NB-PMR sync burst. (120 data bits).
TCH/7.2	Uncoded traffic channel, no FEC, only scrambling. Mapped to Block 1 and Block 2 of NDB and NUB.	FEC: As TETRA 1. Mapped to 108 data symbols in NB-PMR NDB and NUB. (432 bits).
TCH/4.8	Rate 2/3 RCPC coded channel with 4 bit termination. Mapped to Block 1 and Block 2 of NDB and NUB.	FEC: As TETRA 1, or use 3 bit terminated r2/3 Turbo code. Mapped to 108 data symbols in NB-PMR NDB and NUB. (432 bits).
TCH/2.4	Rate 1/3 RCPC coded channel with 4 bit termination Mapped to Block 1 and Block 2 of NDB and NUB.	FEC: As TETRA 1, or use r1/2 Turbo code or concatenated code for rate 1/3. (Rate 1/3 Turbo code could be used).

		Mapped to 108 data symbols in NB-PMR NDB and NUB. (432 bits).
SCH/HD, BNCH,	Rate 2/3 RCPC coded channel with 4 bit termination.	FEC: As TETRA 1, or replace with r2/3 Turbo code.
SCH/HU	Rate 2/3 RCPC coded channel with 4 bit termination. Mapped to CB.	FEC: As TETRA 1, or replace with r2/3 Turbo code. Mapped to CB data symbols.
SCH/F	Rate 2/3 RCPC coded channel with 4 bit termination. Mapped to Block 1 and Block 2 of NDB and NUB.	As TETRA1 , or use r2/3 Turbo code. Mapped to 108 data symbols in NB-PMR NDB and NUB. (432 bits).
TCH/S	Multi-rate RCPC coded channel optimised for speech codec. Half and full slot. Mapped to Block 1 and Block 2 for full slot speech traffic, or Block 1 or Block 2 for half slot.	FEC: As TETRA1, or replace with Turbo code. Mapped to 108 data symbols in NB-PMR NDB and NUB. (432 bits) for full slot, or 54 data symbols for half slot.

Other arrangements would, of course, be possible.

The present embodiment uses a layered protocol arrangement for its protocol as is conventional in mobile communications systems. The table below sets out the layer protocol arrangement that is used in the present embodiment in terms of the changes made to the TETRA 1 layered protocol arrangement, and with reference to the ISO 7 layer protocol model. In this embodiment, only layer 1 (i.e. the "physical layer") and the Lower MAC layer of layer 2 (i.e. of the "data link layer") are changed with respect to the protocol layers of the TETRA (TETRA 1) system. Protocol layers above the Lower MAC layer (i.e. the Upper MAC layer and above) are the same as in (i.e. not changed with respect to) TETRA 1.

Layer	**ISO 7 layer protocol model**	**Approximate equivalent TETRA1 protocol name/function**	**Changes**

7	Application layer	Application layer, speech codec	No change
6	Presentation layer	E2E encryption	No change
5	Session layer		No change
4	Transport layer		No change
3	Network layer	MM, CMCE, PD MLE	No change
2	Data link layer	LLC Upper MAC Lower MAC	No change No change Some change
1	Physical layer	Physical layer	Change

The system of the present embodiment may be used, for example, to provide a standalone, narrow-band mobile communications system. Figure 9 shows a schematic diagram of an exemplary such narrow band Private Mobile Radio (NB-PMR) TETRA-compatible mobile communications system in which 12.5 kHz channels are used for transmission in accordance with this preferred embodiment of the present invention. In Figure 9, the arrowed lines indicate 12.5 kHz channels. Also shown are vehicle and hand-held communications terminals (which are interchangeable). The system includes one or more base stations and infrastructure elements which form a 12.5 kHz trunked mode network 10, as is conventional in mobile communications systems.

Figure 9 also shows Direct Mode Operation, with 12.5 kHz direct mode networks 20, 30 which allow communications terminals to operate in direct mode with each other, and to communicate with the trunked mode network 10 via a trunked mode gateway 22 and/or a dual watch mobile station 32. One or more direct mode repeaters 34 may be provided in the system to extend the range of communication between communications terminals operating in direct mode.

It is also envisaged that the scheme of the present invention can be used in conjunction with existing and conventional TETRA networks.

Figure 10 shows a schematic diagram of a trunked mode network for an exemplary hybrid mobile communications system in which both 12.5 kHz NB-PMR channels in the manner of the above embodiment and 25 kHz TETRA 1 channels

are used for transmission (are supported). Vehicle and hand-held communications terminals are shown (which are interchangeable).

This exemplary hybrid system comprises a TETRA 1 trunked mode network 40 which comprises users (communications terminals) that operate using conventional 25 kHz channels, and a NB-PMR trunked mode network 10 which comprises users (communications terminals) that operate using 12.5 kHz channels in the manner of the above embodiment. Users (communications terminals) that operate using 25 kHz channels, can preferably interoperate with users (communications terminals) that operate using 12.5 kHz channels via the hybrid system. Preferably, the hybrid system comprises base stations that can support both 12.5 kHz and 25 kHz channels.

Preferably, the hybrid system is able to switch dynamically between operating using 12.5 kHz channels for transmission and using 25 kHz channels for transmission based on the capabilities of the (e.g.) communications terminals in the system and/or the quality of the signal. Preferably, the hybrid system can allocate 25 kHz channels to communications terminals operating using 25 kHz channels (e.g. conventional TETRA 1 communication terminals), and can allocate 12.5k Hz channels to communications terminals operating using 12.5 kHz channels (e.g. NB-PMR communication terminals).

In a preferred embodiment, the allocation is based on protocol elements in the control channel and/or characteristics of the modulation being used. For example, a communications terminal (mobile station) can indicate its capabilities (e.g. its "narrow band" capability) to the communications system during registration (e.g. using the U-LOCATION UPDATE PDU in the optional “class of MS” and/or “extended capabilities” information elements (as will be appreciated by those skilled in the art, there are spare (reserved) bits in the extended capabilities element (EN300 392-2 clause 16.10.10a))). Alternatively, an unused QAM bandwidth value in the extended capabilities may be used. This information can be used by the communications system to allocate an appropriate channel to the communications terminal.

Equally, the communications terminals used in the hybrid system are preferably able to operate using 25 kHz channels or using 12.5 kHz channels as required at any given time. The communications terminals can be configured such that if they detect 12.5 kHz transmissions, they preferably switch to operate using a

12.5 kHz channel, and if they detect 25 kHz TETRA 1 transmission, they preferably switch to operate using a 25 kHz (TETRA 1) channel.

For example, a base station of the system can indicate the bandwidth of a channel using one of the reserved “modulation mode” and/or “bandwidth elements" in the “channel characteristics” element that is sent in the D-NWRK BROADCAST EXTENSION PDU (EN 300 392-2 clauses 18.4.1.4.1b and 18.5.5a). Alternatively, a spare value in the augmented channel allocation (EN 300 292-2 clause 21.5.2) can be used. This information can be used by the communications to terminal to switch between the two modes of operation.

Similarly, a TETRA system with a mobile station on a 25 kHz $\pi/4$-DQPSK MCCH could allocate the mobile station to a 12.5 kHz assigned channel, and/or a mobile station on a 12.5 kHz MCCH could be allocated to a TETRA 25 kHz $\pi/4$-DQPSK assigned channel (or a QAM assigned channel).

Figure 11 shows a schematic diagram of another exemplary hybrid mobile communications system in which both 12.5 kHz (NB-PMR) channels and 25 kHz (TETRA 1) channels can be used for transmission (are supported). Networks 10 and 40 correspond to networks 10 and 40 in Figure 10. In this case DMO is also supported. Vehicle and hand-held communications terminals (which are interchangeable) are shown.

The hybrid mobile communications system in this embodiment preferably comprises a direct mode network 50 which can support communications terminals that operate using conventional 25 kHz channels (e.g. purely TETRA 1), a direct mode network 20 which can support communications terminals that operate using 12.5 kHz channels (e.g. purely NB-PMR), as well as a hybrid direct mode network 60 which preferably supports both communications terminals that operate using conventional 25 kHz channels and communications terminals that operate using 12.5 kHz channels (e.g. a mixture of NB-PMR and TETRA 1 users).

Preferably, gateways 22, 24, 52, 62 and/or dual watch mobile stations are provided in order to provide interoperability between the infrastructure elements. In this embodiment, gateways 22, 52 and 62 comprise trunked mode gateways and gateway 24 comprises a hybrid NB-PMR-TETRA 1 repeater or gateway. Preferably, certain communications terminals (mobile stations) are able to operate using both modulation schemes, and can act as gateways between the two modulation schemes. These mobile stations are preferably able to receive

incoming signals on 25 kHz channels and send outgoing signals on 12.5 kHz channels, and vice versa.

It can be seen from the above, that the present invention, in its preferred embodiments at least, can provide a narrower band mobile communications system that still allows many or all of the functionalities of TETRA 1 to be preserved, and the changes necessary to existing TETRA equipment for it to be able to use the modulation scheme of the present invention to be relatively small. Equally, the new scheme can have a high degree of interoperability with existing TETRA systems.

The scheme of the present invention can also accordingly be used to upgrade an existing TETRA system in a way which requires no new frequencies and requires relatively minimal new equipment investment. Similarly, the invention can be employed in green field TETRA systems to enhance the basic TETRA system capability. It can also be used to allow a substantially TETRA compatible and/or TETRA-based system to be deployed in regions and frequency bands that specify 12.5 kHz, rather than 25 kHz, radio channels.

This is achieved in the preferred embodiments of the present invention at least by providing a digital mobile radio communications system that makes transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, and using a multi-carrier modulation scheme that encodes at least 4 bits per symbol.

Claims

1. A method of operating a digital mobile radio communications system, comprising:

using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol, for transmissions in the system.

2. The method of claim 1, where the digital mobile radio communications system comprises a TETRA-compatible mobile communications system.

3. The method of claim 1 or 2, further comprising:

using the TETRA π/4 DQPSK modulation scheme for transmissions in the system.

4. The method of claim 1, 2 or 3, further comprising using the time slot and frame structure of the TETRA 1 standard for the 12.5 kHz four slot time-division multiple access scheme.

5. The method of any one of the preceding claims, further comprising using not more than eight sub-carriers in each 12.5 kHz channel.

6. The method of any one of the preceding claims further comprising using four sub-carriers and 34 symbols per sub-carrier in each 12.5 kHz channel.

7. The method of any one of the preceding claims, further comprising using one of QAM, PSK/DPSK, and OFDM for the modulation scheme that encodes at least 4 bits per symbol.

8. The method of any one of the preceding claims, further comprising:

using the 4 bits per symbol modulation scheme to encode at least some data symbols on a sub-carrier of a 12.5 kHz channel; and

using a different modulation scheme to encode at least some other symbols on a sub-carrier of a 12.5 kHz channel.

9. The method of any one of the preceding claims, further comprising using a fixed constant modulation level for the 12.5 kHz four slot time-division multiple access scheme.

10. The method of any one of the preceding claims further comprising including pilot symbols only in the outer sub-carriers of a 12.5 kHz channel.

11. The method of any one of the preceding claims further comprising including relatively fewer synchronisation and/or pilot symbols in transmissions using the 12.5 kHz four slot time-division multiple access scheme than are included in transmission using the TEDS standard.

12. A communications station for a digital mobile radio communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

13. A digital mobile radio communications system, comprising:

means for making transmissions using a four slot time-division multiple access scheme in 12.5 kHz channels, with each 12.5 kHz channel containing plural sub-carriers and each sub-carrier being modulated with a modulation scheme that encodes at least 4 bits per symbol.

14. The station or system of claim 12 or 13, wherein the digital mobile radio communications system comprises a TETRA-compatible mobile communications system.

15. The station or system of claim 12, 13 or 14, further comprising:

means for making transmissions using the TETRA π/4 DQPSK modulation scheme.

16. The station or system of any one of claims 12 to 15, wherein each 12.5 kHz channel comprises not more than eight sub-carriers.

17. The station or system of any one of claims 12 to 16, wherein each 12.5 kHz channel comprises four sub-carriers with 34 symbols per sub-carrier.

18. The station or system of any one of claims 12 to 17, wherein the modulation scheme that encodes at least 4 bits per symbol comprises one of QAM, PSK/DPSK, and OFDM.

19. The station or system of any one of claims 12 to 18, wherein:

at least some data symbols on a sub-carrier of a 12.5 kHz channel are encoded with the 4 bits per symbol modulation scheme; and

at least some other symbols on a sub-carrier of a 12.5 kHz channel are encoded with a different modulation scheme.

20. The station or system of any one of claims 12 to 19, wherein the means for making transmissions using the 12.5 kHz four slot time-division multiple access scheme is configured to use a fixed constant modulation level.

21. The station or system of any one of claims 12 to 20, wherein pilot symbols are included only in the outer sub-carriers of a 12.5 kHz channel.

22. The station or system of any one of claims 12 to 21, wherein relatively fewer synchronisation and/or pilot symbols are included in transmissions using the 12.5 kHz four slot time-division multiple access scheme than are used in transmission using the TEDS standard.

23. A computer program element comprising computer software code portions for performing the method of any one of claims 1 to 11 when the program element is run on data processing means.

24. A method of operating a digital mobile radio communications system substantially as herein described.

25. An apparatus for use in a digital mobile radio communications system substantially as herein described.

Intellectual Property Office

Application No:	GB1402416.0	**Examiner:**	Mrs Hannah Sylvester
Claims searched:	1-25	**Date of search:**	5 November 2014

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-25	WO2014/125265 A1 (SEPURA PLC) see whole document
X	1-7, 12-18 and 23-25 at least	GB2510718 A1 (SEPURA PLC) see whole document
X	1-25	MEHDI NOURI et al): TEDS: A high speed digital mobile communication air interface for professional users. IEEE Vehicular Technology Magazine IEEE, US vol. 1, no.4 1 December 2006. pages 32-42, sections 2, 3.1, 3.2, 3.3. ISSN: 1556-6072. XP011176540
X	1-25	ETSI TS 100 392-2 v3.6.1 (2013-05). Terrestrial Trunked Radio (TETRA); Voice plus data (V+D); Part 2: Air Interface (AI) Section 6.2 and page 73 http://www.etsi.org/deliver/etsi_ts/100300_100399/10039202/03.06.01_60/ts_10039202v030601p.pdf

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

H04B; H04L; H04W

The following online and other databases have been used in the preparation of this search report

WPI EPODOC TXTE

International Classification:

Subclass	Subgroup	Valid From
None		

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Patent Application Ser. No. 18/532,175 filed December 7, 2023, titled "Method and Apparatus for Processing Bandwidth Intensive Data Streams Using Virtual Media Access Control and Physical Layers", which claims the benefit of U.S. Patent Application Ser. No. 18/448,281 filed August 11, 2023, titled "Method and Apparatus for Processing Bandwidth Intensive Data Streams Using Virtual Media Access Control and Physical Layers", now U.S. Patent No. 11,849,337, which claims the benefit of U.S. Patent Application Ser. No. 17/468,509 filed September 7, 2021, titled "Method and Apparatus for Processing Bandwidth Intensive Data Streams Using Virtual Media Access Control and Physical Layers", now U.S. Patent No. 11,818,591, which claims the benefit of U.S. Patent Application Ser. No. 16/039,660, filed July 19, 2018, titled "System and Method For Extending Range and Coverage of Bandwidth Intensive Wireless Data Streams", now U.S. Patent No. 11,115,834, which claims the benefit of U.S. Patent Application Ser. No. 14/526,799, filed October 29, 2014, titled "System and Method For Extending Range and Coverage of Bandwidth Intensive Wireless Data Streams", now U.S. Patent No. 10,034,179, which claims the benefit of U.S. Provisional Patent Application Ser. No. 61/897,219, filed October 30, 2013, and U.S. Provisional Patent Application Ser. No. 61/897,216, filed October 30, 2013, all of which are incorporated by reference herein in their entirety.

TECHNICAL FIELD

[0002] The disclosure herein relates to wireless networks, and more specifically to high-bandwidth wireless networks for distributing multi-media content.

BACKGROUND

[0003] Wireless networks may take many forms, depending on the application. Various WiFi standards exist where users within range of a "hotspot" may establish a wireless link to access a given network. A given hotspot, or wireless access point, typically has a limited range

and coverage area. WiFi and cellular technologies rely on very different wireless radios and data protocols in transferring data over the network.

[0004] With the proliferation of multi-media content over wireless networks comes an insatiable demand for more bandwidth over the networks. Conventional wireless networking architectures fail to provide adequate resources to efficiently provide optimum range and coverage for wireless network users, and fail to take full advantage of the resources available to satisfy the desire for more bandwidth.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Embodiments of the disclosure are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0006] FIG. 1 illustrates one embodiment of a virtualization mode and an actual mode for processing wireless signals.

[0007] FIG. 2 illustrates a flowchart of steps employed in one embodiment of a method of operation of the system of FIG. 1.

[0008] FIG. 3 illustrates how a virtual MAC and virtual PHY are coordinated to manage actual MAC and PHY layers.

[0009] FIG. 4 illustrates how the system of FIG. 2 manages signal processing by determining which resources are available.

[0010] FIGs. 5A and 5B illustrate alternative ways to manage one embodiment of a variable-duplex link.

[0011] FIG. 6 illustrates one embodiment of a variable duplex link that is configurable to manage transmit and receive process cycles, including preset process cycle configurations of different types.

[0012] FIG. 7 illustrates one embodiment of a system for wirelessly extending range of a wireless network linearly from one access point to another.

[0013] FIG. 8 illustrates a wireless management system that utilizes a virtual MAC and virtual PHY to wirelessly and adaptively manage and control multiple radios in a given wireless access point.

[0014] FIG. 9 illustrates a flowchart of steps for one embodiment of a method of wirelessly accessing a wireless network, consistent with the systems shown in FIGs. 1 and 2.

[0015] FIG. 10A – 10C illustrate embodiments of a system for wirelessly extending range of a wireless network radially from one access point to other access points.

[0016] FIG. 11 illustrates one embodiment of multiple wireless management systems that cooperate to allocate transceiver resources between users.

DETAILED DESCRIPTION

[0017] Embodiments of wireless networking systems, wireless transceivers and associated methods are disclosed herein. In one embodiment, a wireless networking system is disclosed. The wireless networking system includes an application layer associated with one or more applications having a wireless bandwidth requirement. A first wireless transceiver resource associated with an actual MAC layer and PHY layer is employed. The first wireless transceiver resource has a first bandwidth availability up to a first actual bandwidth. A second wireless transceiver resource associated with the actual MAC layer and the PHY layer is employed. The second wireless transceiver resource has a second bandwidth availability up to a second actual bandwidth. A processing layer evaluates the wireless bandwidth requirement and the first and second bandwidth availabilities of the wireless transceiver resources. The processing layer includes a bandwidth allocator to allocate at least a portion of each of the first and second actual bandwidths to virtual MAC and virtual PHY layers, and to satisfy the application layer wireless bandwidth requirement.

[0018] In a further embodiment, a method of a method of operating a wireless transceiver system is disclosed. The wireless transceiver system includes an application layer, actual MAC and PHY layers, and a processing layer between the actual MAC and PHY layers. The method includes evaluating, with processing logic, application bandwidth requirements of applications associated with the applications layer. A virtual MAC layer and a virtual PHY layer are defined between the processing layer and the actual MAC and PHY layers. A bandwidth allocator allocates multiple wireless transceiver resources in the actual MAC and PHY layer to be controlled by the virtual MAC and PHY layer to satisfy the application bandwidth requirements. A stream of processed data is transferred via a wireless link with the allocated wireless transceiver resources.

[0019] In yet another embodiment, a wireless transceiver for coupling to a wireless duplex link is disclosed. The wireless transceiver includes programmable storage, a transmitter and a receiver. The transmitter couples to the programmable storage and transmits data along a wireless link during a first portion of a programmed data transfer cycle. The receiver couples to the programmable storage and receives data from the wireless link during a second portion of the

programmed data transfer cycle. The wireless link exhibits an asymmetric transmit/receive profile based on information stored in the programmable storage.

[0020] Referring to Figure 1, one embodiment of a wireless networking system, generally designated 100, is shown in an abstract "layer" context. Generally speaking, the system may involve a WiFi network, a mobile wireless network, or a combination of the two. The network includes an application layer "APP", at 102, with one or more data-intensive software applications "APP A" – "APP D." The individual applications, for example, may have different peak bandwidth requirements in terms of data transfer rates. Thus, for instance, application APP A may have a peak bandwidth requirement of 450 Megabits per second (Mbps), while application APP D may have a peak bandwidth requirement of 750 Mbps.

[0021] Further referring to Figure 1, the application layer 102 cooperates with a process layer, at 104. The process layer includes a decision block 106 that interfaces with a processing block 108. The decision block determines the size and type of data stream being received, and the type of processing necessary to put the stream in a format where it is capable of being transmitted. The processing block processes the data stream as determined by the decision block, and couples to an ultra-streaming block 110. The ultra-streaming block manages the processing of signal streams or sub-streams given the available resources (memory, processing speed, number of available radios, etc.), and packetizes sufficiently processed streams or sub-streams. The ultra-streaming block feeds data to and from an RF block 112. While not explicitly shown in FIG. 1, the ultra-streaming block carries out a monitoring function, more fully described below, that feeds back wireless resource availability to the decision block 106. Various ways for determining availability of resources include common memory, host interfaces, common threads, and/or queues or other data structures.

[0022] The decision block 106, processing block 108 and ultra-streaming block 110 together form a virtual MAC layer 111. The RF block 112 forms a virtual PHY layer. As more fully described below, the virtual MAC and PHY layers enable simultaneous allocation of multiple PHY resources for different signal types associated with different applications. As a result, the wireless networking system 100 exhibits significant performance improvements and efficiency advantages.

[0023] With continued reference to FIG. 1, the wireless networking system 100 includes an actual media access control (MAC) layer, at 114, and an actual physical (PHY) layer, at 116. The

actual MAC layer 114 generally includes software resources capable of controlling one or more transceiver resources 118 that are at the actual PHY layer, such as various radios and receivers. The actual PHY layer 116 may include multiple transceiver resources corresponding to multiple radios, each with an actual data transfer capability, or bandwidth.

[0024] The actual PHY layer transceivers may transmit and receive data consistent with a variety of signal protocols, such as High Definition Multimedia Interface (HDMI) consistent with the IEEE 802.11 Standard, Multiple-In Multiple-Out (MIMO), standard Wi-Fi physical control layer (PHY) and Media Access Control (MAC) layer, and existing IP protocols. Additionally, extremely high bandwidth applications such as Voice Over IP (VOIP), streaming audio and video content, multicast applications, convergent and ad-hoc network environment may employ signal protocols consistent with the wireless network system described herein. Additionally, the wireless networking system may be employed and/or embedded into a variety of electronic devices, including wireless access points, base stations, handhelds, tablets, computers, telephones, televisions, DVD players, BluRay players, media players, storage devices, or any such devices that use wireless networks to send and receive data including stand-alone add-on devices such as "dongles" that serve as wireless interfaces between devices.

[0025] In operation, and referring to FIG. 2, the wireless networking system generally determines an overall wireless bandwidth demand or requirement from one or more applications associated with the application layer 102, at 202. FIG. 1 illustrates one example, with Application A demanding a peak bandwidth of 450 Mbps, and Application D requiring a peak bandwidth of 750 Mbps. At 204, the process layer 104 determines available resources in the actual MAC and PHY layers 114 and 116, and allocates the available resources to satisfy the bandwidth demands, at 206.

[0026] Using the same example shown in FIG. 1, and assuming that all of the PHY transceivers are available, each PHY transceiver 118 is capable of providing a transmit/receive bandwidth of 300 Mbps. Grouping the entire bandwidth of one transceiver with half the bandwidth of a second satisfies the bandwidth demand for Application A. In a similar manner, allocating the bandwidths of two transceivers, and half the bandwidth of a third transceiver satisfies the bandwidth demand for Application D. The allocating is managed by defining the virtual MAC/PHY layers 111 and 112 with the allocated resources, at 208.

[0027] Figure 3 illustrates how, in one embodiment, elements associated with the process layer 104 can define a virtual MAC management layer 302 and a virtual PHY layer 304 to enable the sharing of multiple transceiver resources in a way sufficient to satisfy the bandwidth requirements of multiple applications running simultaneously. The virtual MAC and PHY layers manage signals from one or more applications before sending the signals to the actual MAC and PHY layers. The virtual MAC management layer 302 may include the decision block 106, the processing block 108 and the ultra-streaming block 110. The virtual PHY layer 304 may include the RF block 112, shown as multiple RF blocks to denote the virtual use of two sets of allocated transceiver resources. For one embodiment, the RF block(s) communicate directly with the ultra-streaming block about actual resource availability, and the ultra-streaming block sends the information back to the decision block in the virtual MAC layer. Alternatively, the virtual PHY RF block may directly communicate with the virtual MAC decision block and/or the processing block.

[0028] Referring now to FIG. 4, defining the virtual MAC and PHY layers 302 and 304 involves an evaluation of available transceiver resources to meet peak bandwidth demands of applications running in the application layer. One or more applications, such as "Application A" and "Application B", may be initially supported with transceiver resources "Device 1" and "Device 2" through an initialization or training process at startup. The virtual MAC 302 interfaces with the virtual PHY 304 to determine device availability. This further involves a determination at the PHY layer as to the actual availability of the initially assigned transceiver resources. Should a given resource be unavailable, such as through insufficient bandwidth or having an existing assignment, a replacement resource may be identified and assigned. Availability monitoring may be carried out at initialization, as described above, or through periodic or continuous updating based on environmental conditions or through random on demand programming. Adaptively managing the actual resources provides efficient utilization of resources and power.

[0029] For one embodiment, the virtual MAC 302 and virtual PHY 304 may be employed to control respective transmit and receive times (also referred to as an RF cycle) for a transceiver coupled to a variable duplex wireless link. FIG. 5A illustrates a way of ensuring an RF cycle that has a transmit time equal to a receive time, such that a first amount of data is transmitted along a given link that is equal to a second amount of data that is received along the link. A physical

resource PHY 502, such as a wireless transceiver, is shown coupled to a transmit buffer 504 and a receive buffer 506. By providing transmit buffer storage that is equal to the receive buffer storage, the amount of data transmitted during both portions of the cycle is equal (since the transceiver generally transmits and receives the entire contents of a given buffer before switching to the next portion of the cycle).

[0030] While equal transmit and receive portions of the RF cycle may be beneficial in some circumstances, allocating different PHY resources for different applications, as described above, may benefit from asymmetric wireless links, where the transmit or receive times may be different to optimize wireless data traffic. FIG. 5B illustrates one embodiment of a variable duplex link that includes a transmit buffer 504 that is larger than a receive buffer 506. A programmable register 508 provides a way to specify the storage capacities of each of the buffers, thus enabling control of the respective transmit and receive time. In another embodiment, the programmable register may include storage to specify precise transmit and receive times for the RF cycle in addition to, or instead of varying the buffer sizes. For some embodiments, sub-programmable mask intervals may be programmed which disable a given transmitter or receiver during the pre-programmed transmit or receive time.

[0031] FIG. 6 illustrates one embodiment of the wireless networking system, described above, utilizing the variable duplex link to optimize uplink (transmit) and downlink (receive) data transfer efficiency for a given application. As shown in FIG. 6, a decision block 602 associated with a virtual MAC 604 detects application types, APP A and APP B, for which a preset transmit/receive cycle ratio has been assigned. A processing block 606 processes the substream signals together with the preset cycle ratio information. A virtual PHY 608, configures available devices to the preset cycle ratio in terms of either configuring transmit and receive buffer sizes, and/or configuring actual transmit and receive cycle times.

[0032] The virtual MAC and PHY layers 604 and 608 may also be used to reconfigure, or update, the RF cycle times of the link periodically or continuously. Additionally, random on-demand programming may be employed to reconfigure the link. By monitoring parameters associated with the link, a predictive model of optimal link operation may be adaptively generated, resulting in enhanced link operability.

[0033] Those skilled in the art will appreciate that the embodiments described above enable wireless networking systems to operate at higher levels of performance and with better

efficiencies. By employing a virtual MAC and virtual PHY between an application layer and an actual MAC and PHY layer, wireless transceiver resources may be allocated more efficiently to handle various data bandwidth requirements from different applications. Additionally, by selectively employing a variable duplex link, data transfers may be further optimized through finer control of link transmit and receive times.

[0034] When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described circuits may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs including, without limitation, net-list generation programs, place and route programs and the like, to generate a representation or image of a physical manifestation of such circuits. Such representation or image may thereafter be used in device fabrication, for example, by enabling generation of one or more masks that are used to form various components of the circuits in a device fabrication process.

[0035] Further embodiments of wireless networking systems, wireless transceivers and associated methods are disclosed herein. In one embodiment, a wireless networking system is disclosed. The system includes a first wireless access point having a first coverage area. The first wireless access point includes a first wireless transceiver to access a wireless network and a second wireless transceiver coupled to the first wireless transceiver. A second wireless access point has a second coverage area. The second wireless access point includes a third wireless transceiver for establishing a wireless link with the second wireless transceiver, and a fourth wireless transceiver coupled to the third wireless transceiver to provide user access to the wireless link. User access to the wireless link accesses the wireless network via the second and first wireless transceivers.

[0036] In a further embodiment, a method of providing wireless network access to a user is disclosed. The method includes accessing a wireless network with a first wireless transceiver associated with a first wireless access point. The first wireless access point has a first coverage area bounded by a range of a first broadcast transceiver associated with the first wireless access point. Wireless access to the wireless network is enabled within the first coverage area with the first broadcast transceiver. A wireless link is established between the first wireless access point and a third wireless transceiver associated with a second wireless access point. The second

wireless access point has a second coverage area bounded by a fourth wireless transceiver. The fourth wireless transceiver is in communication with the third wireless transceiver. Access to the wireless network from within the second coverage area is enabled via the fourth wireless transceiver.

[0037] In yet another embodiment, a wireless access point for use in a wireless networking system, the wireless access point includes a first wireless transceiver to establish a wireless link to a wireless network. A second wireless transceiver provides wireless access to the wireless link within a first coverage area. A third wireless transceiver establishes a wireless link to a second wireless access point. Processing logic controls each of the first, second and third wireless transceivers.

[0038] Referring to Figure 7, one embodiment of a wireless networking system is shown, generally designated 610, that increases the range of wireless network access. The wireless networking system 610 includes multiple wireless access points, or nodes, 612A – 612E. The nodes may be positioned linearly, such as in serial or wirelessly daisy-chained arrangement, to linearly extend wireless network access across multiple access point coverage zones. A similar embodiment that extends coverage radially is described below with reference to FIGs. 10A – 10C.

[0039] With continued reference to FIG. 7, for one specific embodiment, node 612A includes multiple radios A1 and A2. Radio A1 is configured as a receiver/transmitter (transceiver) that exhibits a wireless transceiver range, denoted by the circle at 614, to receive and transmit signals to a network, such as the Internet 615. Note that for purposes of clarity, each node is shown in FIG. 7 as having a range defined by the range of one of the radios. Radio A1, while acting as a receiver/transmitter (often referred to herein as a transceiver) is also able to broadcast and receive signals within its coverage area to users that are in the area 614, thereby serving as a wireless access point for that area. User U1 thus may access the Internet via radio A1. Radio A1 also communicates with a relay radio A2, which may be disposed near the periphery of the range 104 of radio A1. Relay radio A2 has a similar range as radio A1, and is able to communicate with radio B1 that is associated with node 612B. For some embodiments, the relay radio (such as radio A2) for a given node is assigned to one or more dedicated transceivers (such as B1) associated with respective adjacent nodes. Additionally, in general, the

transceivers of a given node can communicate to any of the transceivers available in adjacent nodes.

[0040] Further referring to FIG. 7, node 612B includes three radios, one to establish communication with radio A2 of node 612A, a second radio B2 to act as a relay to a third node 612C, and a third radio B3 to act as a wireless access point to a second user U2 within the node 102B. The third node 102C includes a first radio C1 to communicate with the second radio B2 of the second node 612B, and a second radio C2 to provide wireless access to a third user U3 within the access coverage area of the third node 612C. Thus, with communication links established from the Internet to radio A1, to radio A2, to radio B1 to radio B2 to radio C1 and to radio C2, the user U3 is able to access the Internet wirelessly even though the distance between the user U3 to the first wireless access point A1 exceeds the coverage or range of radio A1.

[0041] Each node 612A – 612C described above, may be configured differently depending on the available resources and bandwidth demands. Thus, a given radio may handle multiple tasks to receive and broadcast simultaneously, if the bandwidth demands are relatively low, or handle a single task, such as relay radio A2, if the bandwidth demand necessitates the need for additional wireless transceiver resources.

[0042] To manage the allocation and configuration of wireless transceiver resources, each node employs a management system, such as one embodiment shown in FIG. 8, and generally designated 710. The management systems for multiple nodes thus forms distributed logic that cooperate to efficiently manage bandwidth utilization for users. Further details of the management system for a variety of applications are disclosed in U.S. Patent Number 9,788,305, titled METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS, filed October 29, 2014, and expressly incorporated herein by reference.

[0043] Further referring to Figure 8, one specific embodiment of the management system 710, is shown in a networking "layer" context. Generally speaking, the wireless management system may be configured for coupling an available transceiver resource to a WiFi network, a mobile wireless network, or a combination of the two. The management system 710 includes an application layer "APP", at 712, with one or more data-intensive software applications "APP A" – "APP D." The individual applications, for example, may have different peak bandwidth requirements in terms of data transfer rates. Thus, for instance, application APP A may have a

peak bandwidth requirement of 450 Megabits per second (Mbps), while application APP D may have a peak bandwidth requirement of 750 Mbps.

[0044] Further referring to Figure 8, the application layer 712 cooperates with a process layer, at 714. The process layer includes a decision block 716 that interfaces with a processing block 718. The decision block determines the size and type of data stream being received, and the type of processing necessary to put the stream in a format where it is capable of being transmitted. The processing block processes the data stream as determined by the decision block, and couples to an ultra-streaming block 720. The ultra-streaming block manages the processing of signal streams or sub-streams given the available resources (memory, processing speed, number of available radios, etc.), and packetizes sufficiently processed streams or sub-streams. The ultra-streaming block feeds data to and from an RF block 722. While not explicitly shown in FIG. 8, the ultra-streaming block carries out a monitoring function, more fully described below, that feeds back wireless resource availability to the decision block 716. Various ways for determining availability of resources include common memory, host interfaces, common threads, and/or queues or other data structures.

[0045] The decision block 716, processing block 718 and ultra-streaming block 720 together form a virtual MAC layer 621. The RF block 722 forms a virtual PHY layer. The virtual MAC and PHY layers enable simultaneous allocation of multiple PHY resources for different signal types associated with different applications. Transceiver configurations may be applied at initialization of the system, periodically during normal operation, or randomly on demand during operation. As a result, the most efficient path for wireless access between a given user and the wireless network is paved. The wireless networking system 710 thus exhibits significant performance improvements and efficiency advantages.

[0046] With continued reference to FIG. 8, the wireless management system 710 includes an actual media access control (MAC) layer, at 724, and an actual physical (PHY) layer, at 726. The actual MAC layer 724 generally includes software resources capable of controlling one or more transceiver resources 728 that are at the actual PHY layer, such as various radios and receivers. The actual PHY layer 726 may include multiple transceiver resources corresponding to multiple radios, each with an actual data transfer capability, or bandwidth.

[0047] The actual PHY layer transceivers may transmit and receive data consistent with a variety of signal protocols, such as High Definition Multimedia Interface (HDMI) consistent

with the IEEE 802.11 Standard, Multiple-In Multiple-Out (MIMO), standard Wi-Fi physical control layer (PHY) and Media Access Control (MAC) layer, and existing IP protocols. Additionally, extremely high bandwidth applications such as Voice Over IP (VOIP), streaming audio and video content, multicast applications, convergent and ad-hoc network environment may employ signal protocols consistent with the wireless network system described herein. Additionally, the wireless management system may be employed and/or embedded into a variety of electronic devices, including wireless access points, base stations, handhelds, tablets, computers, telephones, televisions, DVD players, BluRay players, media players, storage devices, or any such devices that use wireless networks to send and receive data including stand-alone add-on devices such as "dongles" that serve as wireless interfaces between devices.

[0048] Figure 9 illustrates a flowchart that shows generic steps carried out during operation of the wireless networking system of FIG. 7. At 812, the first node 612A (FIG. 7) accesses a wireless network, such as the Internet 615, with a first radio or transceiver A1. A second transceiver A2, establishes a wireless link with the first transceiver A1, at 814. The second transceiver may then act as a relay to establish a further link with a radio in a different node, such as radio B1 in node 612B. The wireless network may then be accessed through the different node 612B via the wireless link (between radios B1 and A2) and the first access point, at 816. By employing a plurality of transceivers at each of the nodes that run the Ultra Streaming engine to allocate their available resources, either at initialization as configurable, or while in operation periodically, or dynamically in random demand while in operation, the most efficient path for wireless access is accomplished. This results in increased range and coverage for a given wireless network, and it's Internet access.

[0049] FIGs 10A – 10C illustrate a further embodiment of a wireless networking system, generally designated 910, that is similar to the system of FIG. 7, but configured with various nodes 912A – 912G that are positioned in a relative manner to extend coverage radially, rather than linearly. Each of the nodes includes a wireless management system, such as that shown in FIG. 8 and described above.

[0050] Further referring to FIG. 10A, a first node 912A includes radios A1 – A7, with radio A1 acting as an originating access point for a local network signal, such as the Internet 915. The remaining radios A2 – A7 may then be configured to communicate with specified adjacent nodes. The adjacent nodes have respective coverage zones that overlap the primary node 912A

radially outwardly. Thus, by encircling the primary node with the other nodes, the corresponding coverage area may be increased dramatically.

[0051] FIG. 10B illustrates one configuration where radio A1 acts as the originating radio to communicate with the local wireless network, and radio A2 communicates the network signal as a relay with radios B2 and C2 of nodes 912B and 912C. Radios B1 and C1 of each respective node broadcast wireless access to users within the respective coverage zones, bounded by coverage rings 914 and 916 associated with each respective node 912B and 912C. Similar arrangements are managed with radio A3 communicating with radios D2 and E2, and radios A4 and A5 communicating with F2 and G2, respectively. To optimize coverage radially, the nodes 912B – 912G are positioned radially around the primary node 912A in a honeycomb structure. The resulting coverage boundary, represented by the coverage circle 408, is significantly larger than the originating access coverage area (represented by ring 410) provided by the broadcast radio associated with node 402A by itself.

[0052] FIG. 10C illustrates different assignments of the radios in the wireless networking system of FIG. 10A managed by the wireless management system 910 of each node 912A – 912G. The assignments and radio configurations may be defined and managed during an initialization process, periodically during operation, or randomly on demand depending on the bandwidth demands of the system. Thus, if bandwidth demands are higher in nodes 912B and 912C, then instead of sharing the bandwidth of radio A2 with nodes 912B (radio B2) and 912C (radio C2), such as the arrangement of FIG. 10B, dedicated relay radios A2 and A3 may be assigned to each of those nodes so that maximum bandwidth may be provided to each, resulting in radio A2 communicating with radio B2 and radio A3 communicating with radio C2 (FIG. 10C).

[0053] For some embodiments, whether the wireless networking system is configured as a linear or radial architecture, there may be multiple transceivers assigned to a wireless node, and each node may have multiple transceivers assigned to a given user. FIG. 11 illustrates how multiple wireless management systems cooperate to efficiently allocate transceiver resources in such a situation. A first node management system 962 may control transceiver resources A1 and A2 within a first node. A second management system 964 may control transceiver resources B1, B2, and B3. The management systems 962 and 964 communicate with each other to determine the optimal resource allocation to service respective local users, at 958 and 960.

[0054] Thus, for the example shown in FIG. 11, the first local user 958 within the coverage of the first node may need bandwidth that may be sufficiently provided by transceiver A1 alone. The second local user 960, positioned within the vicinity of both the first and second nodes, may be assigned transceiver A2 from the first node, and transceiver B2 from the second node, thereby having access to twice the bandwidth. Other examples may involve partial transceiver allocations, where a portion of the transceiver bandwidth is allocated to a first user, and a second portion of the bandwidth allocated to a second user.

[0055] In some embodiments, a given wireless link may be configured as a variable duplex link. Each wireless management system may task the virtual MAC and virtual PHY to control respective transmit and receive cycles for one or more of the wireless transceivers. Varying the transmit and/or receive times may be accomplished in various ways, such as through programmable buffer resources and/or through programmable transmit and receive times. Further detail of such a variable duplex wireless link may be found in U.S. Patent Number 9,788,305, titled METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS, filed October 29, 2014, and expressly incorporated herein by reference.

[0056] Those skilled in the art will appreciate that the embodiments described above enable efficient wireless access to wireless networking systems by users that might be outside the range of a single wireless access point. By employing linear and/or radial wireless access system architectures, and configuring available wireless transceiver resources optimally within each node, a given wireless network may be accessed with greater bandwidth and more efficiently.

[0057] When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described circuits may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs including, without limitation, net-list generation programs, place and route programs and the like, to generate a representation or image of a physical manifestation of such circuits. Such representation or image may thereafter be used in device fabrication, for example, by enabling generation of one or more masks that are used to form various components of the circuits in a device fabrication process.

[0058] In the foregoing description and in the accompanying drawings, specific terminology and drawing symbols have been set forth to provide a thorough understanding of the present invention. In some instances, the terminology and symbols may imply specific details that are not required to practice the invention. For example, any of the specific numbers of bits, signal path widths, signaling or operating frequencies, component circuits or devices and the like may be different from those described above in alternative embodiments. Also, the interconnection between circuit elements or circuit blocks shown or described as multi-conductor signal links may alternatively be single-conductor signal links, and single conductor signal links may alternatively be multi-conductor signal links. Signals and signaling paths shown or described as being single-ended may also be differential, and vice-versa. Similarly, signals described or depicted as having active-high or active-low logic levels may have opposite logic levels in alternative embodiments. Component circuitry within integrated circuit devices may be implemented using metal oxide semiconductor (MOS) technology, bipolar technology or any other technology in which logical and analog circuits may be implemented. With respect to terminology, a signal is said to be "asserted" when the signal is driven to a low or high logic state (or charged to a high logic state or discharged to a low logic state) to indicate a particular condition. Conversely, a signal is said to be "deasserted" to indicate that the signal is driven (or charged or discharged) to a state other than the asserted state (including a high or low logic state, or the floating state that may occur when the signal driving circuit is transitioned to a high impedance condition, such as an open drain or open collector condition). A signal driving circuit is said to "output" a signal to a signal receiving circuit when the signal driving circuit asserts (or deasserts, if explicitly stated or indicated by context) the signal on a signal line coupled between the signal driving and signal receiving circuits. A signal line is said to be "activated" when a signal is asserted on the signal line, and "deactivated" when the signal is deasserted. Additionally, the prefix symbol "/" attached to signal names indicates that the signal is an active low signal (i.e., the asserted state is a logic low state). A line over a signal name (e.g., '$\overline{<\text{signal name}>}$') is also used to indicate an active low signal. The term "coupled" is used herein to express a direct connection as well as a connection through one or more intervening circuits or structures. Integrated circuit device "programming" may include, for example and without limitation, loading a control value into a register or other storage circuit within the device in response to a host instruction and thus controlling an operational aspect of the device,

establishing a device configuration or controlling an operational aspect of the device through a one-time programming operation (e.g., blowing fuses within a configuration circuit during device production), and/or connecting one or more selected pins or other contact structures of the device to reference voltage lines (also referred to as strapping) to establish a particular device configuration or operation aspect of the device. The term "exemplary" is used to express an example, not a preference or requirement.

[0059] While the invention has been described with reference to specific embodiments thereof, it will be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. For example, features or aspects of any of the embodiments may be applied, at least where practicable, in combination with any other of the embodiments or in place of counterpart features or aspects thereof. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method of improving the performance of circuitry, comprising the steps of:

providing a processing interface that is adapted to be connected to an application interface of a wireless networking device, the application interface being associated with a first application, the first application providing, after the circuitry has been connected to the application interface and when the wireless networking device is being used, a first data stream and having a first wireless bandwidth requirement;

connecting first and second actual MAC interfaces to the processing interface;

connecting first and second actual PHY interfaces respectively to the first and second actual MAC interfaces;

respectively associating first and second wireless transceivers with the first and second actual PHY interfaces, wherein each of the first and second wireless transceivers is suitable for use in a wireless local area network, and the first and second wireless transceivers, respectively, (i) have a first and second bandwidth availability up to first and second actual bandwidths, and (ii) are adapted to emit radio signals in first and second different bands of frequencies;

forming in the processing interface (i) at least one virtual MAC interface and (ii) first and second virtual PHY interfaces that, after the circuitry has been connected to the application interface and during operation of the wireless networking device, feed information regarding the bandwidth availabilities of the first and second wireless transceivers back to the at least one virtual MAC interface;

wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) request or create (i) a first association between a recipient and the first actual MAC and PHY interfaces and (ii) a second association between the recipient and the second actual MAC and PHY interfaces,

(b) identify at least one first portion of the first actual bandwidth of the first wireless transceiver, the identified at least one first portion comprising a set of given resources,

(c) evaluate whether any of the given resources of the first identified actual bandwidth portion are unavailable for communication, and

(d) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first bandwidth portion that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and

wherein, after the circuitry has been connected to the application interface and when the wireless networking is being used, the wireless networking device's utilization of the first available bandwidth portion of the first wireless transceiver does not prevent any wireless networking device devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first wireless transceiver for data transmission or reception purposes at the same time that the first bandwidth portion is being used for data transmission purposes.

2. The method of claim 1, wherein the wireless networking device comprises a wireless access point.

3. The method of claim 1, wherein the first and second frequency bands are specified in at least one member of the family of IEEE 802.11 standards that was in existence as of October 30, 2013.

4. The method of claim 1, wherein the at least one virtual MAC interface includes a decision block.

5. The method of claim 1, wherein the at least one virtual MAC interface includes a processing block.

6. The method of claim 1, wherein the at least one virtual MAC interface includes an ultra-streaming block.

7. The method of claim 1, wherein the first virtual PHY interface includes an RF block.

8. The method of claim 1, wherein the second virtual PHY interface includes an RF block.

9. The method of claim 1, wherein the processing interface comprises multiple virtual MAC interfaces.

10. The method of claim 1, wherein the processing interface includes a bandwidth allocator.

11. The method of claim 1, wherein the first identified actual bandwidth portion is contiguous.

12. The method of claim 1, wherein the first virtual PHY interface is not contiguous with the at least one virtual MAC interface.

13. The method of claim 1, wherein the second virtual PHY interface is not contiguous with the at least one virtual MAC interface.

14. The method of claim 1,

wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) identify at least one second portion of the first actual bandwidth of the first wireless transceiver, the identified second bandwidth portion comprising a set of given

resources, the first and second identified actual bandwidth portions not being contiguous with each other,

(b) evaluate whether any of the given resources of the second identified actual bandwidth portion are unavailable for communication, and

(c) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first and second bandwidth portions that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application.

15. The method of claim 14, wherein the second identified actual bandwidth portion is contiguous.

16. The method of claim 14, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) if all of the given resources of the first identified bandwidth portions are unavailable, identify at least one third portion of the first actual bandwidth of the first wireless transceiver, the third identified bandwidth portion comprising a set of given resources,

(b) evaluate whether any of the given resources of the third identified bandwidth portion are unavailable for communication, and

(c) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the third identified bandwidth portion that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application.

17. The method of claim 14, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) if all of the given resources of the second actual bandwidth portion are unavailable, identify at least one fourth portion of the actual bandwidth of the first wireless transceiver, the fourth identified bandwidth portion comprising a set of given resources,

(b) evaluate whether any of the given resources of the fourth identified bandwidth portion are unavailable for communication, and

(c) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the fourth identified bandwidth portion that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application.

18. The method of claim 1,

wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) identify at least one first portion of the second actual bandwidth of the second wireless transceiver, the first identified portion of the second wireless transceiver comprising a set of given resources,

(b) evaluate whether any of the given resources of the first identified actual bandwidth portion of the second wireless transceiver are unavailable for communication, and

(c) if none of the given resources of the first identified bandwidth portion of the first wireless transceiver are available for communication and if the first identified bandwidth portion of the second wireless transceiver is available for communication, use the second wireless transceiver to transmit the first data stream to the recipient, without requiring

disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding only to the given resources of the first identified actual bandwidth portion of the second wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and

wherein, after the circuitry has been connected to the application interface and when the wireless networking device is being used, the wireless networking device's utilization of the first identified actual bandwidth portion of the second wireless transceiver does not prevent any other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the second wireless transceiver for data transmission or reception purposes.

19. The method of claim 18, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) if both the first identified actual bandwidth portions of the first and second wireless transceivers are available for communication, evaluate the data transfer characteristics of both,

(b) if the data transfer characteristics of the first identified bandwidth portion of the first wireless transceiver are better than those of the first identified bandwidth portion of the second wireless transceiver, use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first identified bandwidth portion of the first wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application, and

(c) if the data transfer characteristics of the first identified portion of the second wireless transceiver are better than those of the first identified bandwidth portion of the first wireless transceiver, use the second wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of the recipient from either or both of the first and

second actual MAC and PHY interfaces, using a subset of frequencies corresponding to only the given resources of the first identified bandwidth portion of the second wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application.

20. The method of claim 19, wherein the data transfer characteristics are representative of one or more environmental conditions where the wireless networking device is used.

21. The method of claim 1, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface, aggregate the first identified actual bandwidth portion of the first wireless transceiver with an identified first portion of an available bandwidth of the second wireless transceiver to at least partially simultaneously transmit the first data stream to the first recipient from both of the first and second wireless transceivers.

22. The method of claim 21, wherein the first data stream is substantially simultaneously transmitted to the recipient from both of the first and second wireless transceivers.

23. The method of claim 21, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, and in a manner transparent to any layer of the wireless networking device above the processing interface, aggregate the first identified actual bandwidth portion of the first wireless transceiver with an identified first portion of an available bandwidth of the second wireless transceiver to cause the first and second wireless transceivers to at least partially simultaneously receive a second data stream from the recipient.

24. The method of claim 23, wherein the second data stream is substantially simultaneously received by both of the first and second wireless transceivers.

25. The method of claim 1, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) identify at least one first portion of bandwidth available for communication of the second wireless transceiver, the identified at least one first portion of the second wireless transceiver comprising a set of given resources,

(b) evaluate whether any of the given resources of the at least one first identified portions of the first and second wireless transceivers are not unavailable for communication,

(c) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of either or both of the first and second associations, using a specific subset of frequencies corresponding to the given resources of the identified at least one first bandwidth portion of the first wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application, and

(d) use the second wireless transceiver to receive a second data stream from the recipient at least partially simultaneously with the first data stream being transmitted to the recipient from the first wireless transceiver, without requiring disassociation of either or both of the first and second associations, using a specific subset of frequencies corresponding to only the given resources of the identified at least one first bandwidth portion of the second wireless transceiver that are not unavailable for communication to thereby at least partially satisfy a second wireless bandwidth requirement associated with the second data stream; and

wherein, after the circuitry has been connected to the application interface and when the wireless networking device is being used, the wireless networking device's utilization of the at least one first bandwidth portions of the first and second wireless transceivers does not prevent any wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the first and second wireless transceivers for data transmission or reception purposes at the same time that data is being transmitted from or received by the first and second wireless transceivers.

26. The method of claim 25, wherein the second data stream is received by the second wireless transceiver substantially simultaneously with the transmission of the first data stream from the first wireless transceiver.

27. The method of claim 25, wherein the start of the reception of the second data stream by the second wireless transceiver is substantially simultaneous with the start of the transmission of the first data stream from the first wireless transceiver.

28. The method of claim 25, wherein the end of the reception of the second data stream by the second wireless transceiver is substantially simultaneous with the end of the transmission of the first data stream from the first wireless transceiver.

29. The method of claim 25, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) identify at least one second portion of bandwidth available for communication of the first wireless transceiver, the identified at least one second portion of the first second wireless transceiver comprising a set of given resources,

(b) evaluate whether any of the given resources of the at least one first and identified portions of the first wireless transceiver are not unavailable for communication, and

(c) use the first wireless transceiver to transmit the first data stream to the recipient, without requiring disassociation of either or both of the first and second associations, using a specific subset of frequencies corresponding to the given resources of the identified at least one first and second bandwidth portion of the first wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the first application.

30. The method of claim 29, wherein the processing interface is configured to, after the circuitry has been connected to the application interface and when the wireless networking

device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface,

(a) identify at least one second portion of bandwidth available for communication of the second wireless transceiver, the identified at least one second portion of the second wireless transceiver comprising a set of given resources,

(b) evaluate whether any of the given resources of the at least one first and identified portions of the second wireless transceiver are not unavailable for communication, and

(c) use the second wireless transceiver to receive the second data stream from the recipient, without requiring disassociation of either or both of the first and second associations, using a specific subset of frequencies corresponding to the given resources of the identified at least one first and second bandwidth portion of the second wireless transceiver that are not unavailable for communication to thereby at least partially satisfy the first wireless bandwidth requirement of the second application.

ABSTRACT OF THE DISCLOSURE

A wireless networking system is disclosed. The wireless networking system includes an application layer associated with one or more applications having a wireless bandwidth requirement. A first wireless transceiver resource associated with an actual MAC layer and PHY layer is employed. The first wireless transceiver resource has a first bandwidth availability up to a first actual bandwidth. A second wireless transceiver resource associated with the actual MAC layer and the PHY layer is employed. The second wireless transceiver resource has a second bandwidth availability up to a second actual bandwidth. A processing layer evaluates the wireless bandwidth requirement and the first and second bandwidth availabilities of the wireless transceiver resources. The processing layer includes a bandwidth allocator to allocate at least a portion of each of the first and second actual bandwidths to virtual MAC and virtual PHY layers, and to satisfy the application layer wireless bandwidth requirement.

#2183845

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Sai C. Manapragada	Nonprovisional Application Number (if known):	
Title of Invention:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STR		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Blake R. Hartz, Reg. No. 73453/	Date March 4, 2024
Name (Print/Typed) Blake R. Hartz	Practitioner Registration Number 73453

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of 1 forms are submitted.

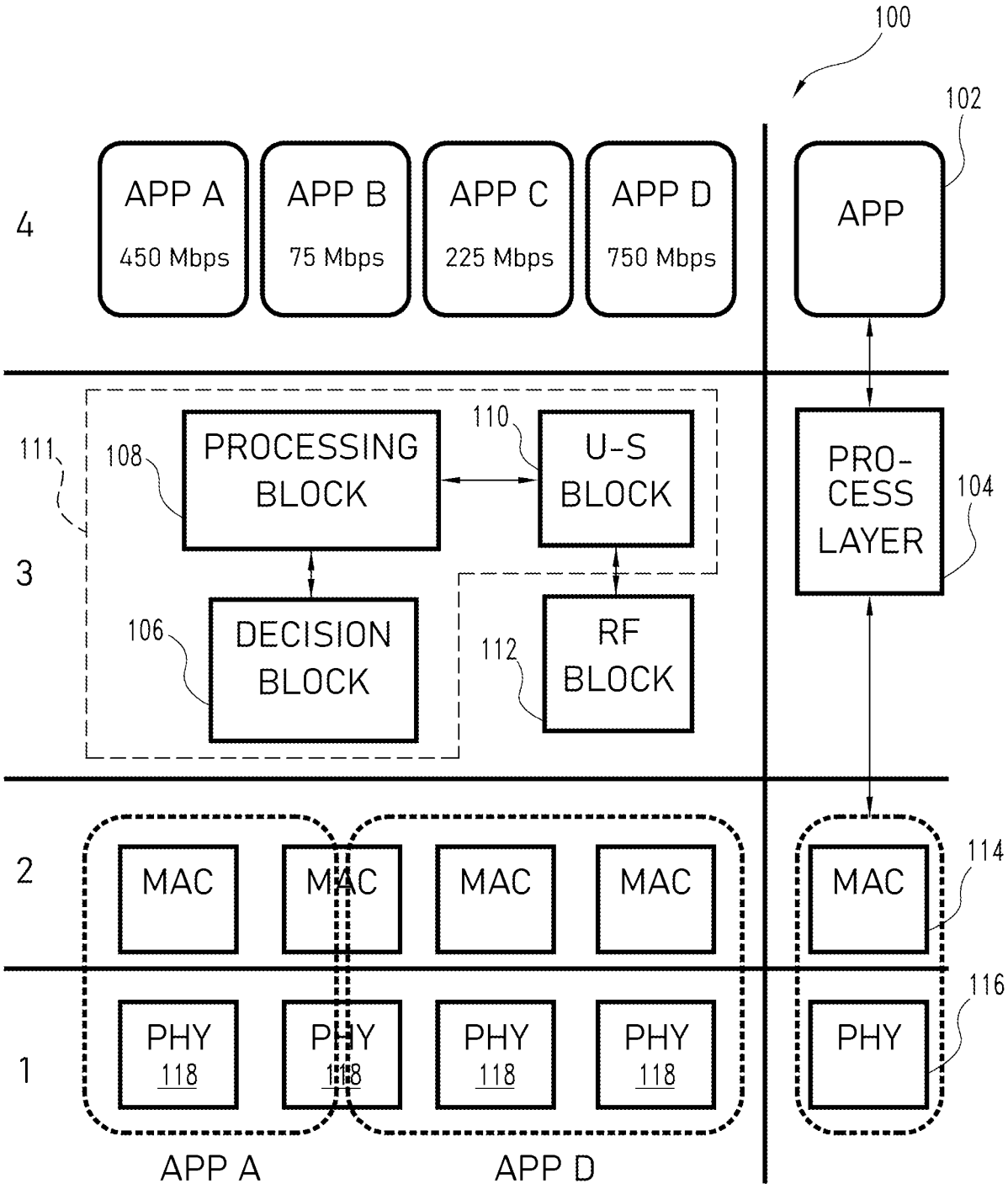

100
102
4
APP A
450 Mbps
APP B
75 Mbps
APP C
225 Mbps
APP D
750 Mbps
APP
111
108
PROCESSING BLOCK
110
U-S BLOCK
PRO-CESS LAYER
104
3
106
DECISION BLOCK
112
RF BLOCK
2
MAC
MAC
MAC
MAC
MAC
114
1
PHY 118
PHY 118
PHY 118
PHY 118
PHY
116
APP A
APP D

Fig. 1

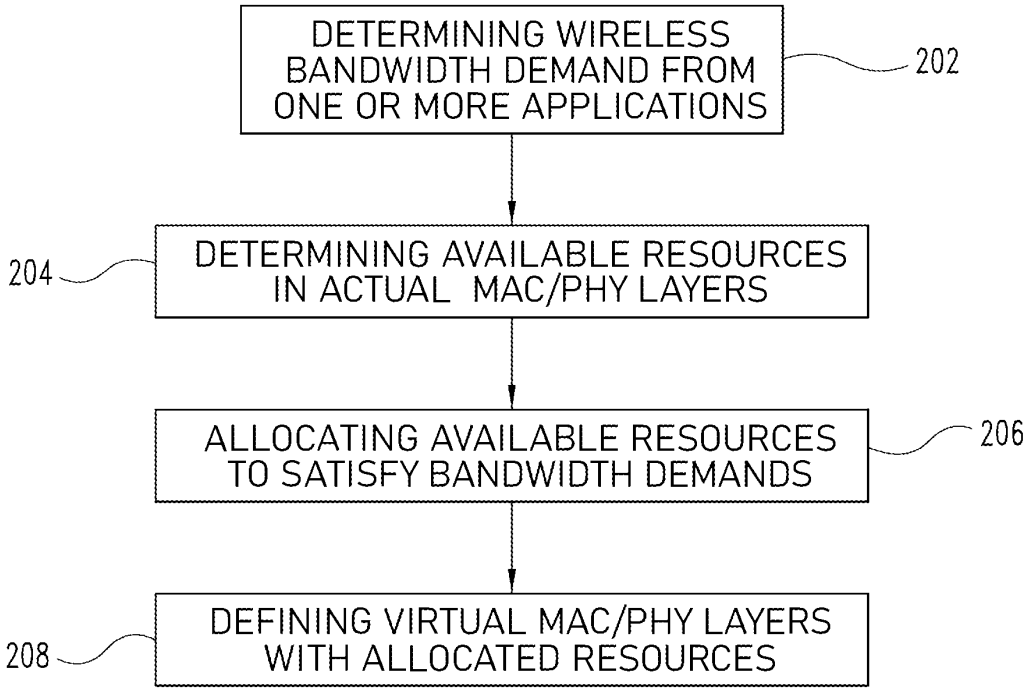

DETERMINING WIRELESS BANDWIDTH DEMAND FROM ONE OR MORE APPLICATIONS
202
DETERMINING AVAILABLE RESOURCES IN ACTUAL MAC/PHY LAYERS
204
ALLOCATING AVAILABLE RESOURCES TO SATISFY BANDWIDTH DEMANDS
206
DEFINING VIRTUAL MAC/PHY LAYERS WITH ALLOCATED RESOURCES
208

Fig. 2

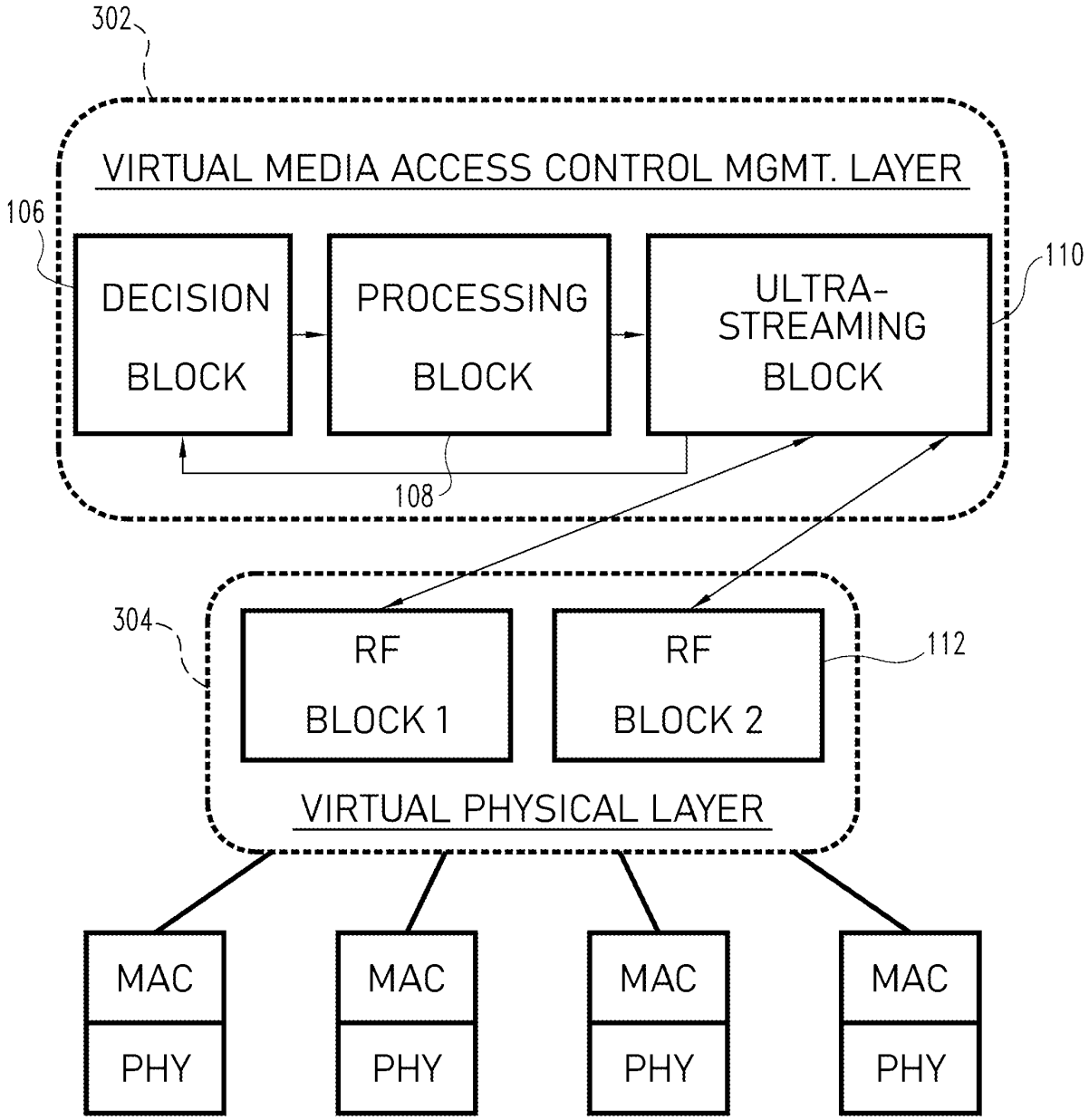

302
VIRTUAL MEDIA ACCESS CONTROL MGMT. LAYER
106
DECISION BLOCK
PROCESSING BLOCK
ULTRA-STREAMING BLOCK
110
108
304
RF BLOCK 1
RF BLOCK 2
112
VIRTUAL PHYSICAL LAYER
MAC
PHY
MAC
PHY
MAC
PHY
MAC
PHY

Fig. 3

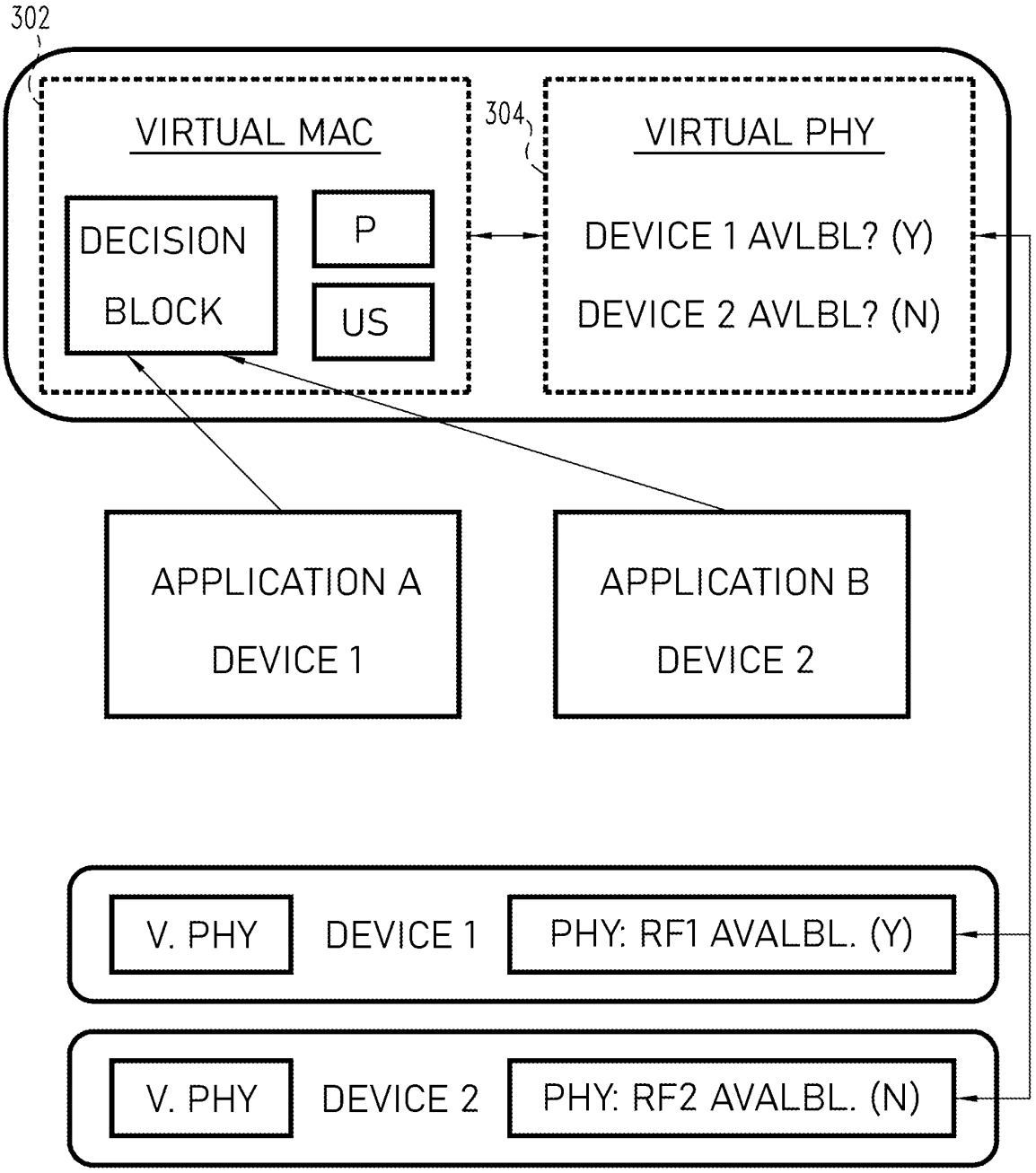

302
VIRTUAL MAC
304
VIRTUAL PHY
DECISION BLOCK
P
US
DEVICE 1 AVLBL? (Y)
DEVICE 2 AVLBL? (N)
APPLICATION A
DEVICE 1
APPLICATION B
DEVICE 2
V. PHY
DEVICE 1
PHY: RF1 AVALBL. (Y)
V. PHY
DEVICE 2
PHY: RF2 AVALBL. (N)

Fig. 4

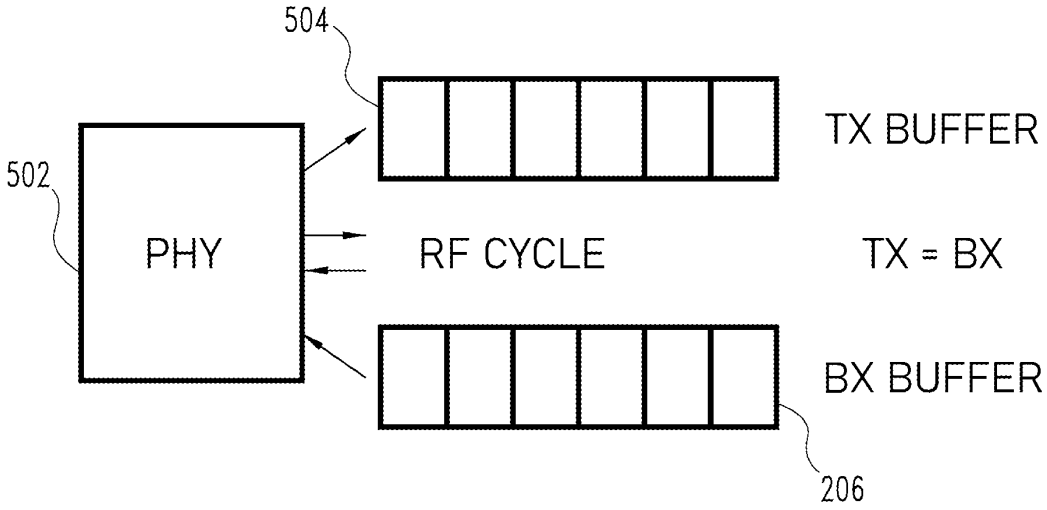

504
TX BUFFER
502
PHY
RF CYCLE
TX = BX
BX BUFFER
206

Fig. 5A

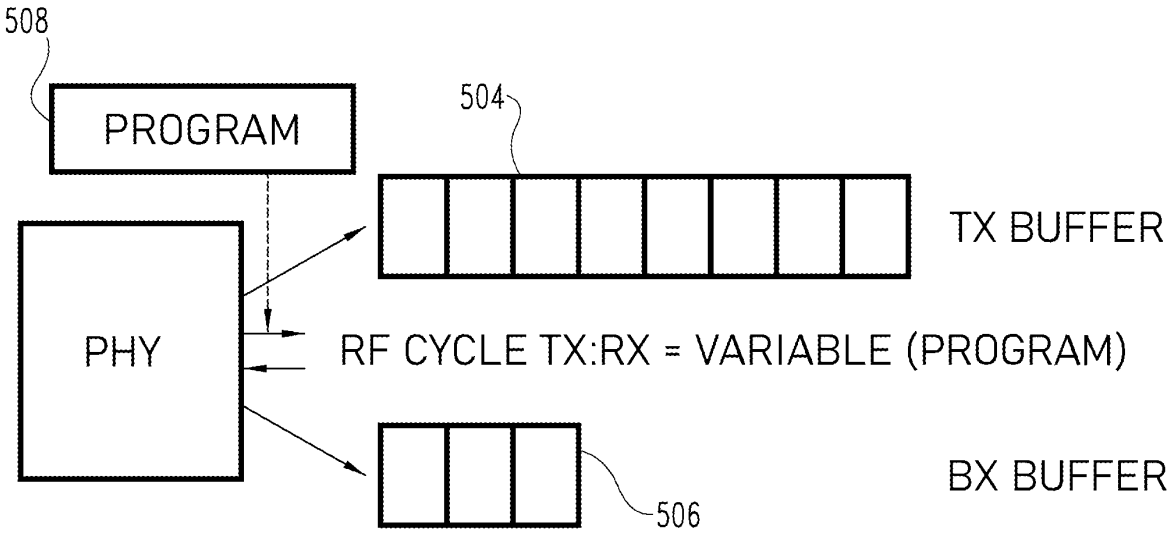

508
PROGRAM
504
TX BUFFER
PHY
RF CYCLE TX:RX = VARIABLE (PROGRAM)
BX BUFFER
506

Fig. 5B

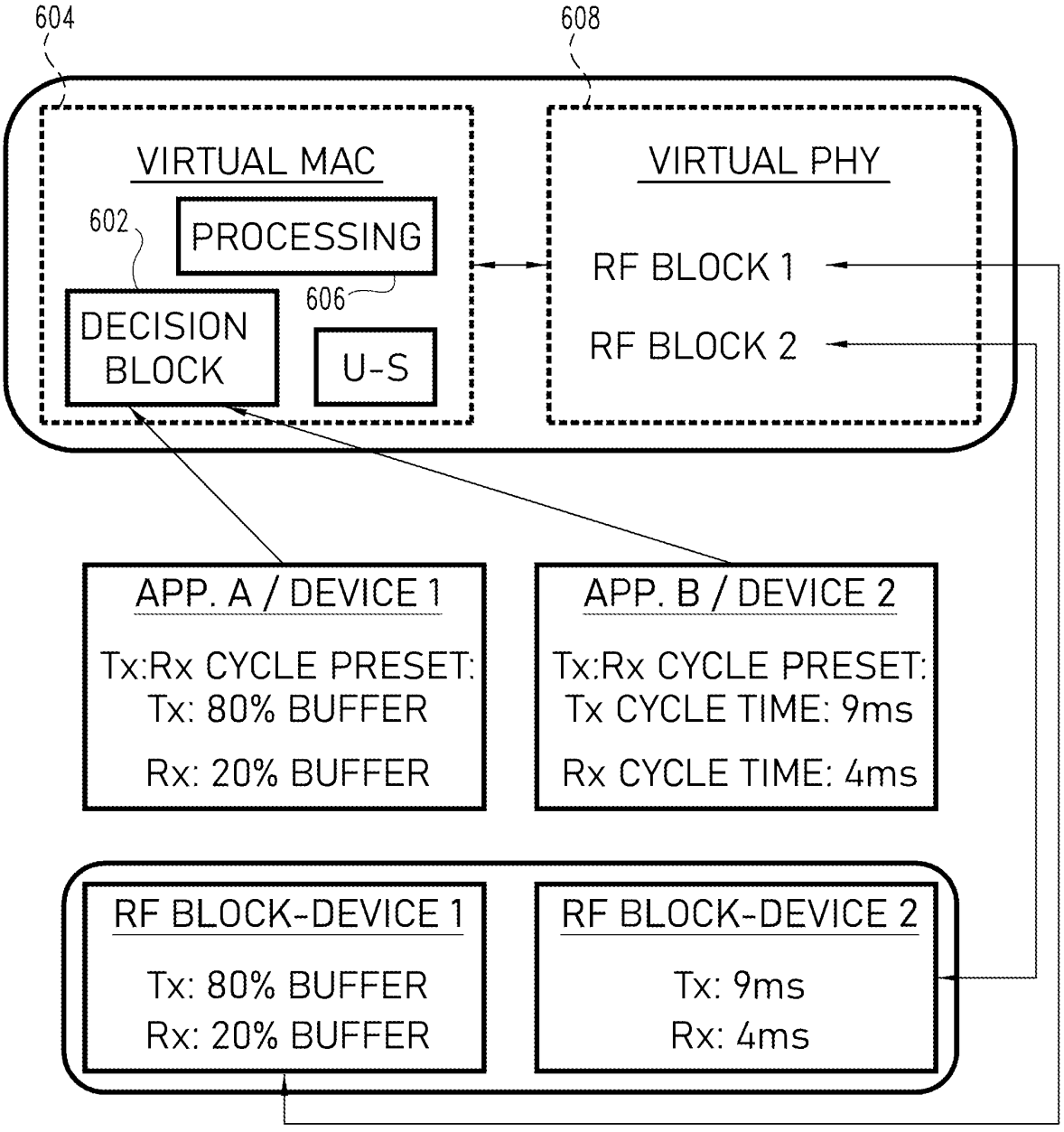

604
608
VIRTUAL MAC
602
PROCESSING
606
DECISION BLOCK
U-S
VIRTUAL PHY
RF BLOCK 1
RF BLOCK 2
APP. A / DEVICE 1
Tx:Rx CYCLE PRESET:
Tx: 80% BUFFER
Rx: 20% BUFFER
APP. B / DEVICE 2
Tx:Rx CYCLE PRESET:
Tx CYCLE TIME: 9ms
Rx CYCLE TIME: 4ms
RF BLOCK-DEVICE 1
Tx: 80% BUFFER
Rx: 20% BUFFER
RF BLOCK-DEVICE 2
Tx: 9ms
Rx: 4ms

Fig. 6

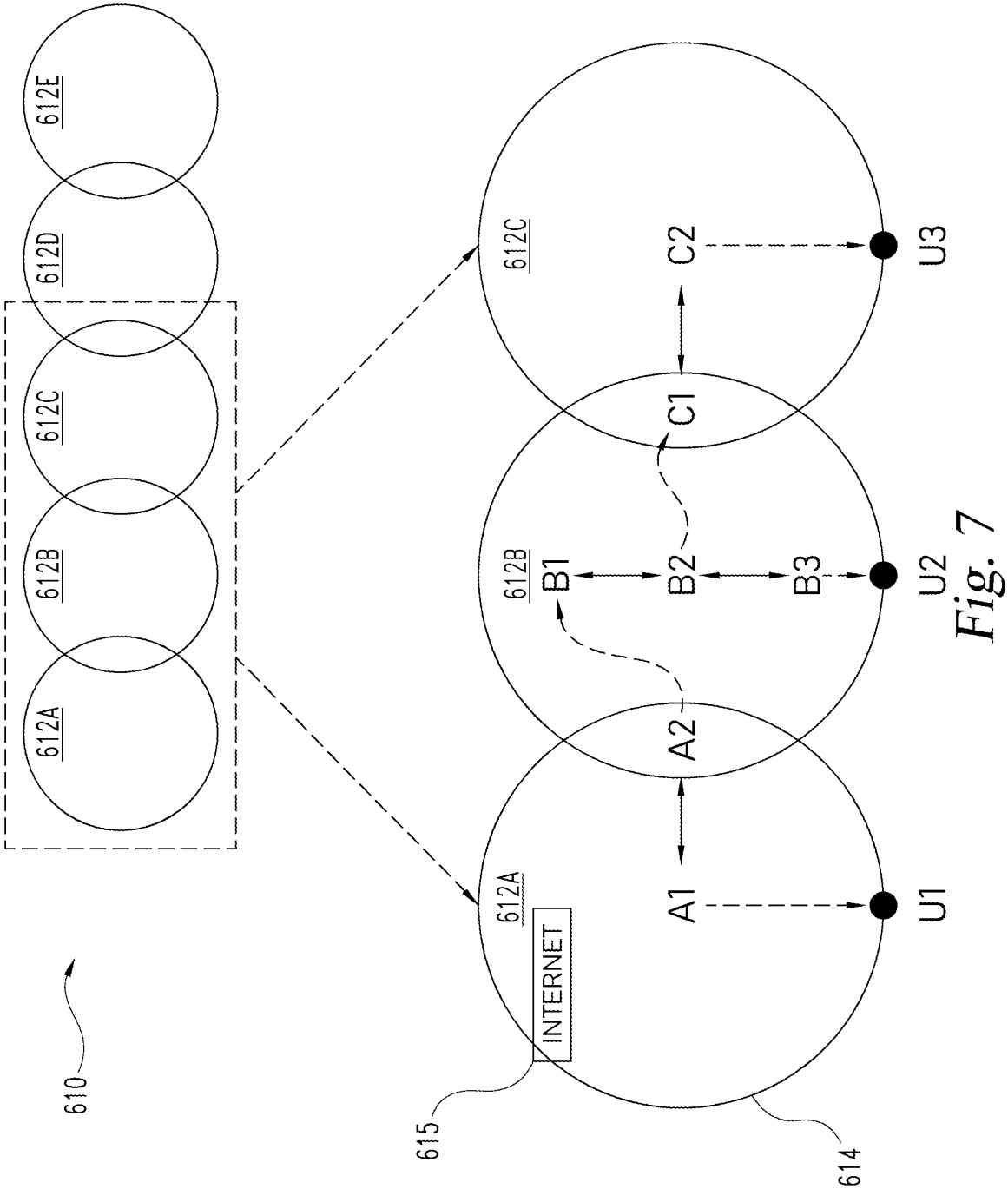

610
612A
612B
612C
612D
612E
615
INTERNET
614
A1
A2
B1
B2
B3
C1
C2
U1
U2
U3

Fig. 7

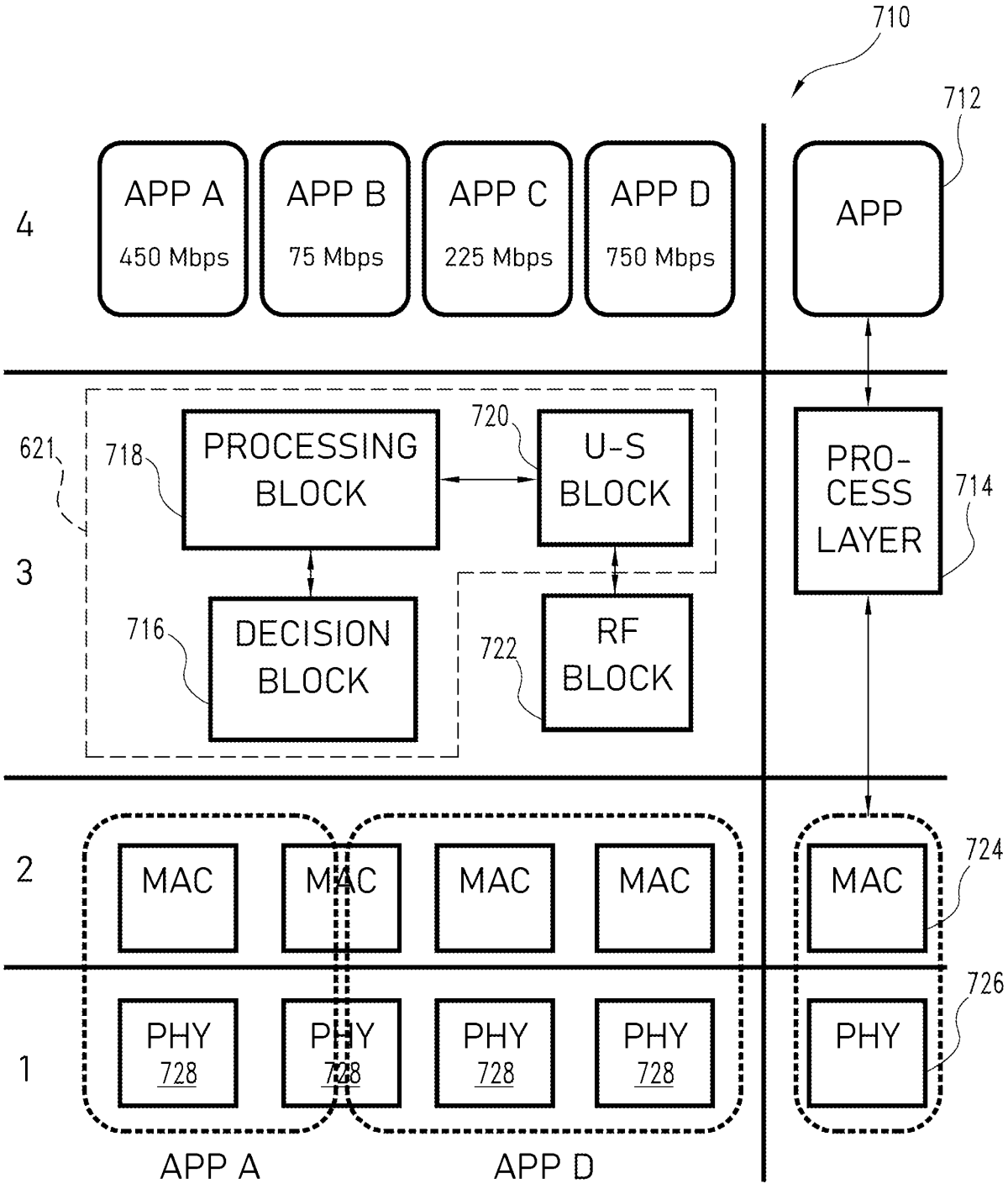

710
712
4
APP A
450 Mbps
APP B
75 Mbps
APP C
225 Mbps
APP D
750 Mbps
APP
621
718
PROCESSING BLOCK
720
U-S BLOCK
PRO-CESS LAYER
714
3
716
DECISION BLOCK
722
RF BLOCK
2
MAC
MAC
MAC
MAC
MAC
724
1
PHY 728
PHY 728
PHY 728
PHY 728
PHY
726
APP A
APP D

Fig. 8

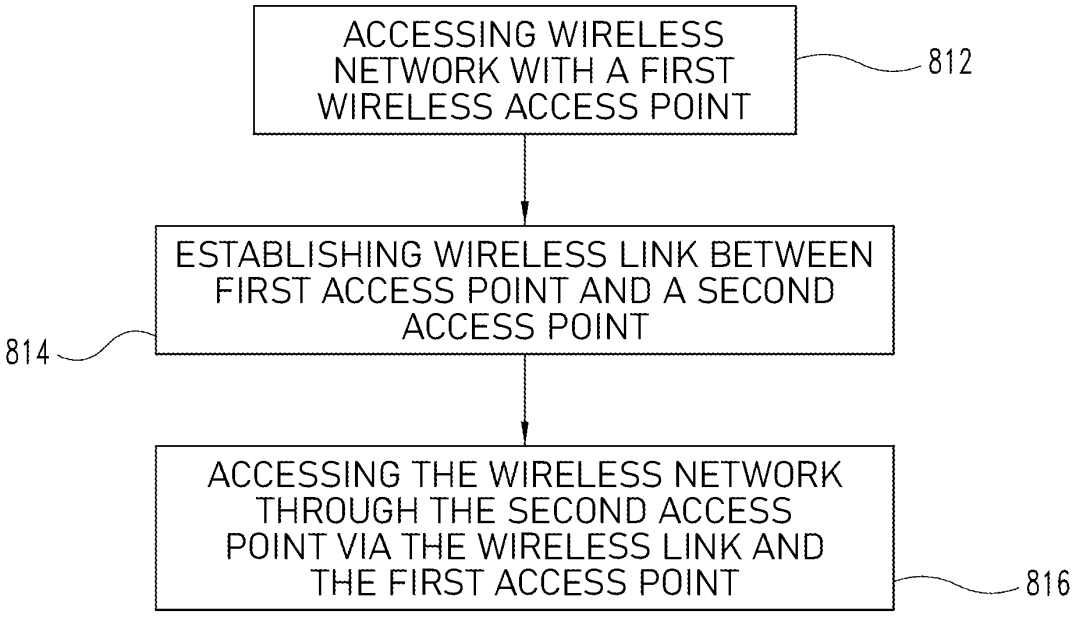

ACCESSING WIRELESS NETWORK WITH A FIRST WIRELESS ACCESS POINT
812
ESTABLISHING WIRELESS LINK BETWEEN FIRST ACCESS POINT AND A SECOND ACCESS POINT
814
ACCESSING THE WIRELESS NETWORK THROUGH THE SECOND ACCESS POINT VIA THE WIRELESS LINK AND THE FIRST ACCESS POINT
816

Fig. 9

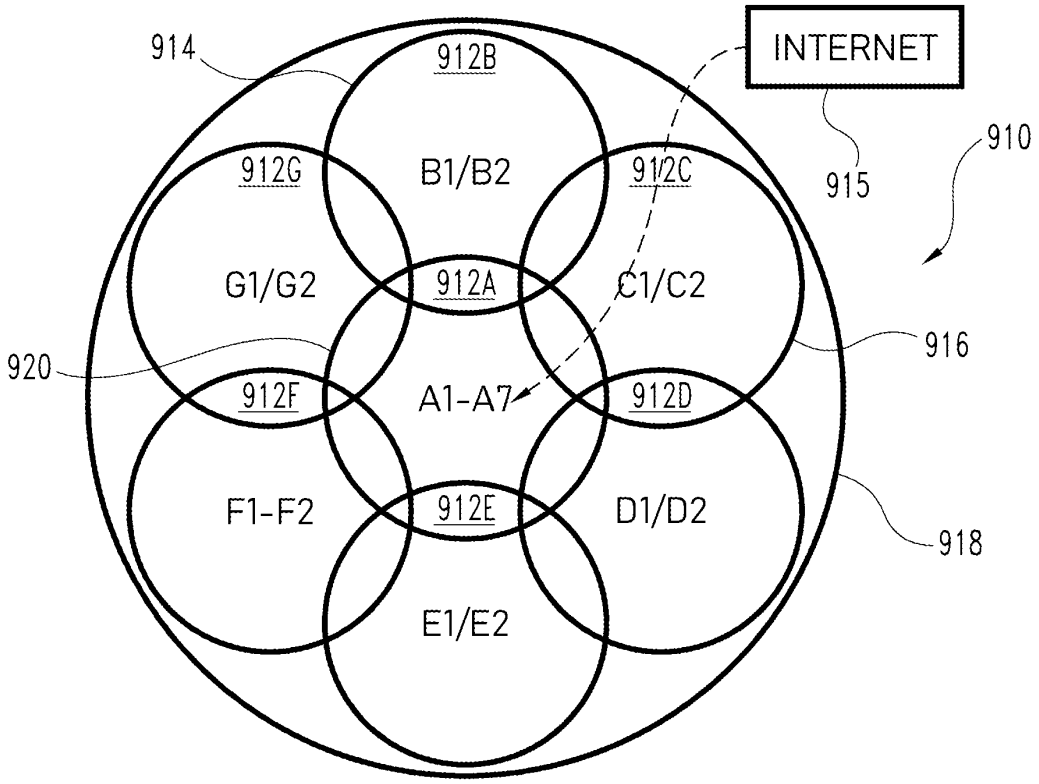


Fig. 10A

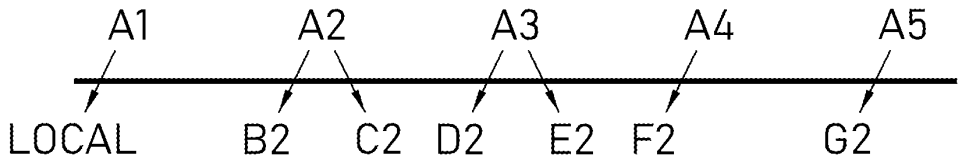


Fig. 10B

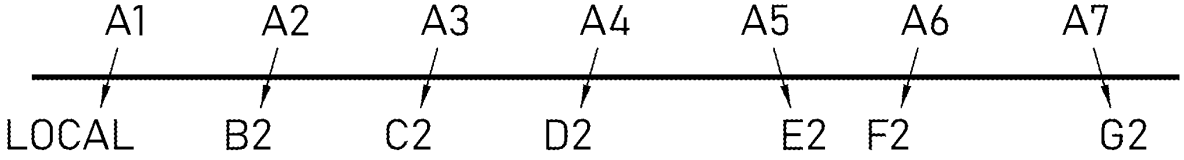


Fig. 10C

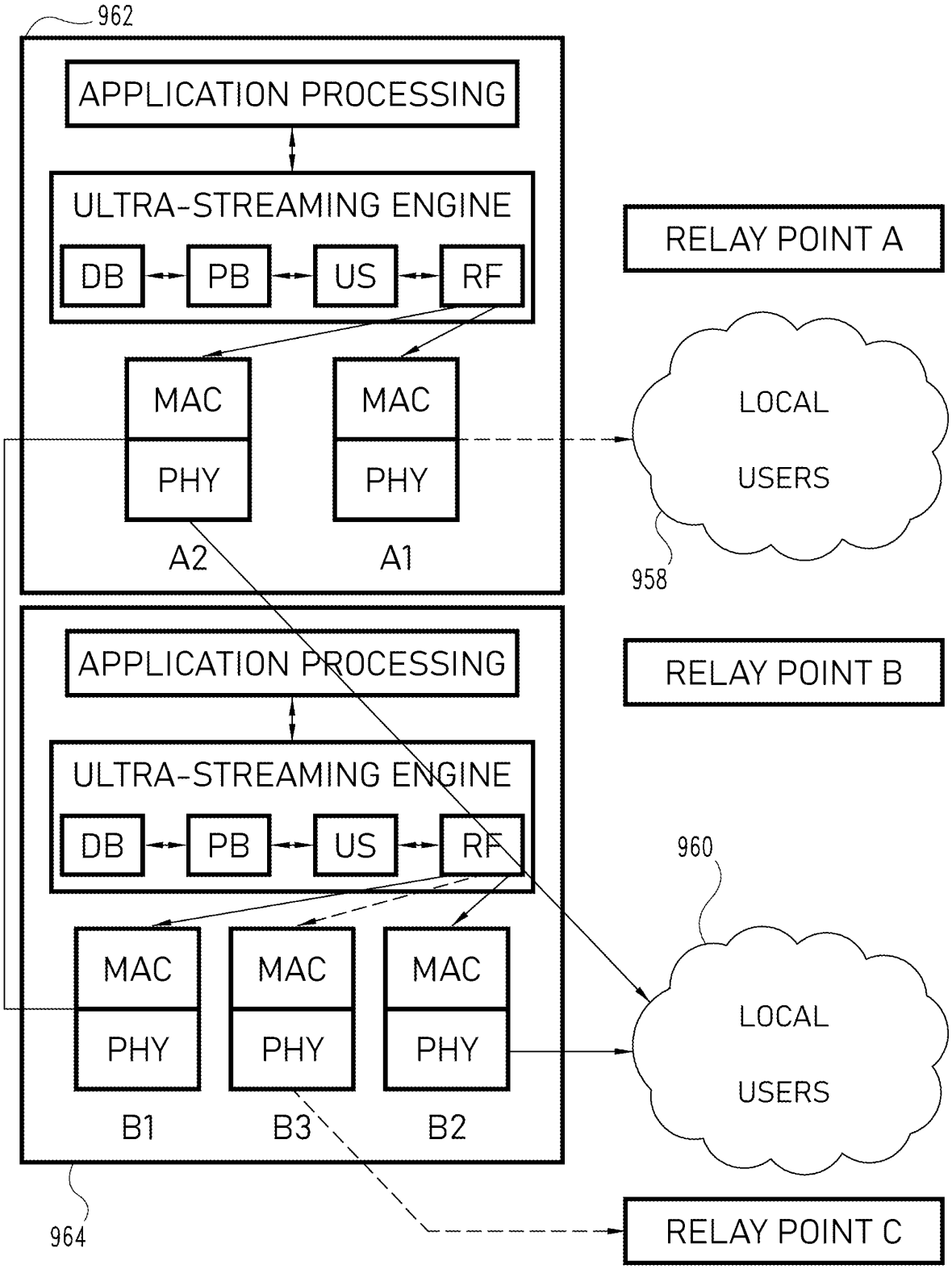

962
APPLICATION PROCESSING
ULTRA-STREAMING ENGINE
DB
PB
US
RF
MAC
PHY
MAC
PHY
A2
A1
RELAY POINT A
LOCAL
USERS
958
APPLICATION PROCESSING
ULTRA-STREAMING ENGINE
DB
PB
US
RF
RELAY POINT B
960
MAC
PHY
MAC
PHY
MAC
PHY
B1
B3
B2
LOCAL
USERS
964
RELAY POINT C

Fig. 11

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/594,375	**03/04/2024 01:44:34 PM Z ET**	**020505-000010**

Title of Invention

METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	3271	FILED BY	WALTER MOORE
PATENT CENTER #	64531364	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	**E202434D45299068**	**WALTER MOORE**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	56.00	1	56.00
2817	REQUEST FOR PRIORITIZED EXAMINATION	1680.00	1	1680.00
2111	UTILITY PATENT APPL. SEARCH FEE	280.00	1	280.00
4011	BASIC FILING FEE- UTILITY	64.00	1	64.00
2311	EXAMINATION OF ORIGINAL PATENT APPLICATION	320.00	1	320.00
2202	EACH CLAIM IN EXCESS OF 20	40.00	10	400.00
			TOTAL AMOUNT:	**$2,800.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 878 169 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
11.07.2018 Bulletin 2018/28

(21) Application number: **06733382.3**

(22) Date of filing: **02.05.2006**

(51) Int Cl.:
H04L 12/28 *(2006.01)* ***H04L 12/24*** *(2006.01)*
H04L 29/06 *(2006.01)* ***H04L 12/46*** *(2006.01)*

(86) International application number:
PCT/SE2006/000527

(87) International publication number:
WO 2006/118530 (09.11.2006 Gazette 2006/45)

(54) **OPERATOR SHOP SELECTION IN BROADBAND ACCESS RELATED APPLICATION**

BETREIBER-SHOP-AUSWAHL IN EINER DEN BREITBANDZUGANG BETREFFENDEN ANWENDUNG

SÉLECTION DE BOUTIQUE D'OPÉRATEUR DANS UNE APPLICATION RELATIVE À L'ACCÈS LARGE BANDE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **29.04.2005 PCT/SE2005/000645**

(43) Date of publication of application:
16.01.2008 Bulletin 2008/03

(73) Proprietor: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **RUNE, Johan**
  S-181 31 Lidingö (SE)
- **JÖNSSON, Ulf**
  S-169 68 Solna (SE)
- **LARSSON, Tony**
  S-194 76 Upplands Väsby (SE)
- **CAGENIUS, Torbjörn**
  S-191 34 Sollentuna (SE)

(74) Representative: **Ericsson Patent Development**
Torshamnsgatan 21-23
164 80 Stockholm (SE)

(56) References cited:
WO-A1-01/16766
WO-A2-01/41392
US-A1- 2003 037 163
US-A1- 2003 117 954
US-A1- 2003 210 671
US-A1- 2004 066 756
US-A1- 2004 165 595

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 1 878 169 B1

Description

TECHNICAL FIELD

[0001] The present invention is generally related to digital communication systems, in particular to digital communication systems in which an end user accesses the rest of the system through an Ethernet network and which include broadband access to various services, and more particularly to operator shop selection by an end user in broadband access in a digital communication system.

BACKGROUND AND PRIOR ART

[0002] Ethernet is the world's most pervasive networking technology.

[0003] Ethernet signals are transmitted from a station serially, one bit at a time, to every other station on the network. Ethernet uses a broadcast access method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD) in which every computer on the network "hears" every transmission, but each computer "listens" only to transmissions intended for it. Each computer can send a message anytime it likes without having to wait for network permission. The signal it sends travels to every computer on the network. Every computer hears the message, but only the computer for which the message is intended recognizes it. This computer recognizes the message because the message contains its address. The message also contains the address of the sending computer so the message can be acknowledged. If two computers send messages at the same moment, a "collision" occurs, interfering with the signals. A computer can tell if a collision has occurred when it does not hear its own message within a given amount of time. When a collision occurs, each of the colliding computers waits a random amount of time before resending the message. The process of collision detection and retransmission is handled by the Ethernet adapter itself and does not involve the computer. The process of collision resolution takes only a fraction of a second under most circumstances. Collisions are normal and expected events on an Ethernet network. As more computers are added to the network and the traffic level increases, more collisions occur as part of normal operation. However, if the network gets too crowded, collisions increase to the point where they slow down the network considerably.

[0004] Any system based on collision detect must control the time required for the worst round trip through the LAN. As the term "Ethernet" is commonly defined, this round trip is limited to 50 microseconds (millionths of a second). At a signaling speed of 10 million bits per second, this is enough time to transmit 500 bits. At 8 bits per byte, this is slightly less than 64 bytes.

[0005] To make sure that the collision is recognized, Ethernet requires that a station must continue transmitting until the 50 microsecond period has ended. If the station has less than 64 bytes of data to send, then it must pad the data by adding zeros at the end.

[0006] To extend the LAN farther than the 50 microsecond limit will permit, one needs a bridge or router. These terms are often confused:

- A repeater receives and then immediately retransmits each bit. It has no memory and does not depend on any particular protocol. It duplicates everything, including the collisions.
- A bridge receives the entire message into memory. If the message was damaged by a collision or noise, then it is discarded. If the bridge knows that the message was being sent between two stations on the same cable, then it discards it. Otherwise, the message is queued up and will be retransmitted on another Ethernet cable. The bridge has no address. Its actions are transparent to the client and server workstations.
- A router acts as an agent to receive and forward messages. The router has an address and is known to the client or server machines. Typically, machines directly send messages to each other when they are on the same cable, and they send the router messages addressed to another zone, department, or subnetwork. Routing is a function specific to each protocol. For IPX, the Novell server can act as a router. For SNA, an APPN Network Node does the routing. TCP/IP can be routed by dedicated devices, UNIX workstations, or OS/2 servers.

[0007] A block of data transmitted on the Ethernet is called a "frame." The first 12 bytes of every frame contain the 6 byte destination address (the recipient) and a 6 byte source address (the sender). Each Ethernet adapter card comes with a unique factory installed address (the "universally administered address"). Use of this hardware address, also called the MAC (Medium Access Control) address or the Ethernet address, guarantees a unique identity to each card. PC software can be configured to substitute a different address number. When this option is used, it is called a "locally administered address." The source address field of each frame must contain the unique address (universal or local) assigned to the sending card. The destination field can contain a "multicast" address representing a group of workstations with some common characteristic.

[0008] Each Ethernet board worldwide has a unique Ethernet-address, it is a 48 bit number (the first 24 bits indicate

the manufacturer, the last 24 bits are a unique number for each Ethernet board/controller-chip assigned by the manufacturer). This is also called the MAC-address.

[0009] In normal operation, an Ethernet adapter will receive only frames with a destination address that matches its unique address, or destination addresses that represent a multicast message.

[0010] There are three common conventions for the format of the remainder of the frame:

- Ethernet II or DIX
- IEEE 802.3 and 802.2
- SNAP

[0011] Ethernet II or DIX :

| Destination address | Source address | Type (Decnet, IPX or IP) |

[0012] Gigabit Ethernet Carrier Extension is a way of maintaining 802.3 minimum and maximum frame sizes with meaningful cabling distances. For carrier extended frames, the non-data extension symbols are included in the "collision window", that is, the entire extended frame is considered for collision and dropped. However, the Frame Check Sequence (FCS) is calculated only on the original (without extension symbols) frame. The extension symbols are removed before the FCS is checked by the receiver. So the LLC (Logical Link Control) layer is not even aware of the carrier extension.

```
| Preamble | SFD | DA | SA | Type/Length | Data | PCS | Extension |
          | 64 bytes min |
          | 512 bytes min |
          | Duration of Carrier Event |
```

SFD is a start of frame delimiter

| Preamble (7-bytes) | Start Frame Delimiter (1-byte) | Dest. MAC Address (6-bytes) | Source MAC Address (6-bytes) | Length / Type (2-bytes) | MAC Client Data (0-n bytes) | Pad (0-p bytes) | Frame Check Sequence (4-bytes) |

[0013] In 1998, the IEEE approved the 802.3ac standard that defines frame format extensions to support Virtual Local Area Network (VLAN) Tagging on Ethernet networks. The VLAN protocol permits insertion of an identifier, or "tag", into the Ethernet frame format to identify the VLAN to which the frame belongs. It allows frames from stations to be assigned to logical groups. This provides various benefits such as easing network administration, allowing formation of work groups, enhancing network security, and providing a means of limiting broadcast domains. IEEE standard 802.1Q gives the definition of the VLAN protocol. The 802.3ac standard defines only the implementation details of the VLAN protocol that are specific to Ethernet.

[0014] If present, the 4-byte VLAN tag, also called Tag Control Information field, is inserted into the Ethernet frame between the Source MAC Address field and the Length/Type field. The first 2-bytes of the VLAN tag consist of the "802.1Q Tag Type" and are always set to a value of 0x8100. The 0x8100 value is actually a reserved Length/Type field assignment that indicates the presence of the VLAN tag, and signals that the traditional Length/Type field can be found at an offset of 4-bytes further into the frame. The last 2-bytes of the VLAN tag contain the following information

[0015] The first 3-bits are a User Priority Field that may be used to assign a priority level to the Ethernet frame.

[0016] The next 1-bit is a Canonical Format Indicator (CFI) used in Ethernet frames to indicate the presence of a Routing Information Field (RIF).

[0017] The last 12-bits are the VLAN Identifier (VID) which uniquely identifies the VLAN to which the Ethernet frame belongs.

[0018] With the addition of VLAN tagging, the 802.3ac standard permitted the maximum length of an Ethernet frame to be extended from 1518-bytes to 1522-bytes. The following illustrates the format of an Ethernet frame that has been "tagged" with a VLAN identifier per the IEEE 802.3ac standard:

| Preamble (7-bytes) | Start Frame Delimiter (1-byte) | Dest. MAC Address (6-bytes) | Source MAC Address (6-bytes) | Length/Type = 802.1Q Tag Type (2-bytes) | Tag Control Information (2-bytes) | Length/Type (2-bytes) | MAC Client Data (0-n bytes) | Pad (0-p bytes) | Frame Check Sequence (4-bytes) |

[0019] With introduction of the 802.3z standard for Gigabit Ethernet in 1998, an extension field was added to the end of the Ethernet frame to ensure it would be long enough for collisions to propagate to all stations in the network. The extension field is appended as needed to bring the minimum length of the transmission up to 512 bytes (as measured from the Destination Address field through the extension field). It is required only in half-duplex mode, as the collision protocol is not used in full-duplex mode. Non data bits, referred to as "extension bits", carrying no useful information, are transmitted in the extension field extending the carrier to continue the minimum required time. The following illustrates a frame with an extension field appended:

| Preamble (7-bytes) | Start Frame Delimiter (1-byte) | Dest. MAC Address (6-bytes) | Source MAC Address (6-bytes) | Length/Type (2-bytes) | MAC Client Data (0-n bytes) | Pad (0-p bytes) | Frame Check Sequence (4-bytes) | Extension |

TCP/IP

[0020] TCP/IP uses IP addresses, which are 32-bit numbers. To make it easier to memorize such IP addresses, they are usually expressed as four 8-bit numbers (example: 192.168.10.1), where each of the four numbers is within the range of '0' to '255'. There are restrictions on using '0' and '255' for all four numbers and these values should be avoided. When setting up a small private network, you are free to use ANY IP address, however, when you are connected to a company network, you need to ask the Network-administrator to assign you an IP address. And if you are connected to the Internet, your ISP (Internet Service Provider) will assign an IP address to you.

DHCP (Dynamic Host Configuration Protocol)

[0021] On boot-up, the system sends out a call on the network to find a DHCP-server, which assigns an IP address to such a system. The IP addresses are usually assigned NOT permanently, but for a specific time (could be days, weeks, months or on Internet-connections just for the ONE connection). If the system contacts the DHCP-server again during this time, the 'lease' on the IP address is extended. But if you come back from a long vacation, your 'lease' of the IP address may have expired, that IP address may have been assigned now to somebody else, and you/your computer get now assigned a new IP address.

[0022] The systems have IP addresses, but Ethernet-boards ONLY know their Ethernet-address, so as soon as a TCP/IP configured system is switched on, it is advertising its presence onto the network: "Hey, I am alive, my Ethernet address is '08000b 0a0236' and my IP address is '192.168.10.2' " and each TCP/IP system on the network builds up a table with all this information, which is usually checked/verified in time-intervals of 15 min.

[0023] If your system needs now to communicate with a station, for which it does NOT have an entry in its table of IP/Ethernet-Addresses, it sends out a search-message to everybody ("Broadcast-Message") like: " Hey, I like to communicate with the IP address '192.168.10.4', but I do NOT know your Ethernet-Address. Please, identify yourself". This causes the system with the requested IP address to send out its advertising again.

[0024] These processes are called ARP (Address Resolution Protocol) and RARP (Reversed Address Resolution Protocol).

[0025] The Address Resolution Protocol is used to dynamically discover the mapping between a layer 3 (protocol) and a layer 2 (hardware) address. A typical use is the mapping of an IP address (e.g. 192.168.0.10) to the underlying Ethernet address (e.g. 01:02:03:04:05:06). You will often see ARP packets at the beginning of a conversation, as ARP is the way these addresses are discovered. ARP is used to dynamically build and maintain a mapping database between link local layer 2 addresses and layer 3 addresses. In the common case this table is for mapping Ethernet to IP addresses. This database is called the ARP Table. Dynamic entries in this table are often cached with a timeout of up to 15 minutes, which means that once a host has ARPed for an IP address it will remember this for the next 15 minutes before it gets time to ARP for that address again.

Gateway/Router

[0026] To connect a TCP/IP local-area-network to another TCP/IP LAN (which could be the complete Internet) or via a Wide-Area-Network (WAN), you need now a device called Gateway or Router.

EAP

[0027] IEEE 802.1x adopts the Extensible Authentication Protocol (EAP) as the mechanism for exchange of authentication messages. EAP messages are encapsulated in Ethernet LAN packets (EAP over LANs, EAPOL) to allow communication between the supplicant and the authenticator.

[0028] EAP-TLS (Transport Layer Security). EAP-TLS is defined in RFC 2716 as the security method used in the 802.1x client in Windows XP. It provides for certificate-based, mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication; and distributes dynamically generated user- and session-based encryption keys to secure the connection. Mutual authentication and distribution of dynamic encryption keys are of particular interest in shared media Ethernet environments, such as 802.11 wireless LANs.

[0029] EAP-TTLS (Tunneled Transport Layer Security). EAP-TTLS (described in an IETF draft) is an extension of EAP-TLS, which requires only server-side certificates, eliminating the need to configure certificates for each client. TTLS provides additional security for transmission of user credentials and ciphers. It also supports legacy password protocols, so that it may be deployed as a front end to existing authentication systems (such as tokens or Microsoft Active Directory Services).

[0030] The evolution towards multiple services delivered over a broadband access network to an end user using an Ethernet type connection increases the end user need and business opportunity for a player to do service bundling,

acting as a one point contact for the end user to access services from a plurality of service providers.

[0031] An access service provider (AccSP) provides the following basic services to its customers, including end users, enterprises or companies and application and content providers:

- Access, i.e. the possibility to hook in to various networks
- Connectivity, i.e. the possibility to connect to another user or service with required capabilities, speed, throughput, latency, etc.
- Reachability, i.e. to provide the possibility for others to connect to you, i.e. providing an identifier for publication together with an appropriate service logic and interconnect services
- Security from fraudulent or unwanted use of the access, including intrusion or eavesdropping.

[0032] An AccSP will also be dependent on identity and trust provisioning in order to identify and handle its customer relationships in an appropriate manner, including account handling.

[0033] From an IP and packet based perspective, AccSP basic offerings are:

- Access rights
- Connectivity
- Reachability

all with the appropriate security level. If access over multiple points is offered, mobility becomes an intrinsic part of connectivity and reachability.

[0034] In one extreme case, the AccSP, called the operator shop, provides all services. The main asset of the operator shop is its direct relation to the end users. By having direct access to all necessary knowledge about the end user, the operator shop can create good service offerings and also provide the best quality in all aspects to the customer.

[0035] This does not mean that the operator shop will be capable of producing all services needed by the market, i.e. different kinds of end users, by itself alone. It will rather offer the complete service package together with partners such as application and content providers. The operator shop then provides a single interface and acts as an integrator, or shop, towards the users, also called subscribers.

[0036] Using the terminology of today the closest you get to an operator shop is an Internet service provider (ISP). Although there may actually be significant differences between an operator shop and an ISP, the two terms may be regarded as more or less equivalent as used herein. Hence, the operator shop selection mechanisms could also be labeled ISP selection mechanisms and would work equally well with ISPs as with operator shops.

[0037] The current invention relates to a method called Flexible service selection (FSS), see the published International patent application No. WO 2005/060208, "Ethernet DSL access multiplexer and method providing dynamic service selection and end-user configuration", that is incorporated by reference herein.

[0038] FSS makes it possible to run a plurality of services from different application service providers (ASPs) simultaneously on a single personal computer (PC) or similar device in the customer premises network (CPN). Different services may be accessed through different gateways, having different media access control (MAC) addresses. It is assumed that the PC or similar device only gets one global IP (Internet Protocol) address, i.e. it may subscribe to only one ISP but to several ASPs.

[0039] The key to FSS is the use of DHCP (Dynamic Host Configuration Protocol) option 121 that allows traffic to be routed to different gateways depending on the IP address of the destination. When the PC requests an IP address through the DHCP it gets an answer according to DHCP option 121 including routing and gateway information relating to the services to which the user has subscribed. In the case where the PC does not support option 121 of the DHCP, the DSLAM (Digital Subscriber Line Access Multiplexer, Ethernet) has to snoop the information according to option 121 to be capable of mapping upstream traffic to the right virtual local area network (VLAN) and directing it to the right gateway as specified by the DHCP server. A VLAN is a logical grouping of ports and endstations such that all ports and endstations in the VLAN appear to be on the same physical (or extended) LAN segment even though they may be geographically separated. A VLAN identifier consists of the last 12 bits of the Tag Control Information field, as described above

[0040] Another related solution is the IP service engine (IPSE). Among other things it manages user traffic flows through a broadband remote access server (BRAS). IPSE can handle three levels of user authentication:

- Authenticated users. When first connected, authenticated users need to provide a login name and password that are validated by the router network element, i.e. the BRAS, typically through the RADIUS protocol with an external authentication server;
- Unauthenticated users. Unauthenticated users are granted a temporary connection and session with a minimum set of IP services. They can be authenticated at a later moment and be more officially logged-in by external business

processes. During the later confirmed login of the users, the IPSE provides more explicit services and routing policies to the managed router.

- Persistent users. Persistent users have been pre-registered in the routers (BRASs) and IPSE with the identification of the MAC addresses of their terminals. Sessions are created to manage connections that have been established without requiring any explicit authentication.

[0041] When coupled with the Ericsson Ethernet DSLAM access (EDA) network, the IPSE can register persistent users dynamically by memorizing the VMAC (Virtual MAC) identifiers or the identifiers according to option 82 of the DHCP. The VMAC address is a locally administered MAC address that is assigned to a terminal and is locally unique in the broadband access network. In frames originating from the terminal the network replaces the original source MAC address by the VMAC address assigned to the terminal, to be used within the broadband access network. In frames destined for a terminal the network uses the VMAC address assigned to the terminal as the destination address within the broadband access network, but replaces it by the MAC address of the terminal before forwarding the frame to the terminal. Hence the assigned VMAC address "belongs to" and identifies the terminal, although the terminal itself never sees the VMAC address or is not aware of its existence.

[0042] Yet another solution related to operator shop selection is the IEEE 802.1X "Port-Based Network Access Control" standard. Appendix C of this standard document describes how the standard could be used together with a VLAN aware bridge in a local area network (LAN) context. One scenario described is when users can be connected to a non-authenticated VLAN by default and then after authentication can be reassigned to another VLAN associated with authorized services. The VLAN configuration for the user's bridge port is thus changed. No VLAN mapping or VLAN de-tagging occurs.

[0043] Current solutions do not provide appropriate operator shop selection mechanisms that work in all access scenarios and for users roaming in foreign broadband access networks. A user roaming in a foreign broadband access network in this case refers to a user visiting an access network that has no direct relation to the user's home operator shop.

[0044] The FSS enables a device to access multiple services. However, it does assume that only one ISP, or single authority, e.g. the operator shop, has all knowledge about the services which the end user can access. Hence, the case where the end user may choose between several "operator shops" or ISPs is not handles by FSS. Further, the FSS method can probably not be used for users roaming in foreign broadband access networks.

[0045] The IPSE solution may be used as a platform to create operator shop selection. However, it does not describe how the authentication, authorization and accounting (AAA) architecture should be designed to support roaming users and it does not solve the problem associated with users roaming into a CPN behind a network address translator (NAT). In addition, the IPSE solution does not allow multiple users connected to the same port of a residential gateway (RG) to choose different ISPs, even when they are not connected through an NAT. Furthermore, the IPSE solution does not describe how the user login procedure is handled in conjunction with ISP selection.

[0046] The example described in the standard document IEEE 802.1X, appendix C using a non-authenticated VLAN could be used as a component in an operator shop selection solution. However, it does not describe the total solution with support for roaming users and users accessing the network from behind an NAT.

[0047] US 2004/066756 concerns a method for user equipment (UE) resident in a wireless access network (WLAN) to obtain access to at least one other network is disclosed. The method includes storing the identification (SSID) of the at least one other network (visited PLMNs and home PLMNs) in the user equipment; transmitting from the user equipment a request for connection to one of the at least one other network, which includes an identification of at least one of the at least one other network, to the wireless access network; and in response to the wireless access network receiving the identification, the user equipment is connected to the identified at least one other network through the wireless access network.

[0048] US 2003/117954 concerns a telecommunication system to interconnect end-users and comprising one or more interconnected Virtual Service Networks (VSN) each associated to a data transport network. Each Virtual Service Network provides Quality-of-Service (QoS) guarantee for aggregated dataflows and comprises a Virtual Service Network Controller (VSNC) to control the resources of the Virtual Service Network and to perform a per-user admission control on each dataflow wanting to be transferred through said associated data transport network. Furthermore, each Virtual Service Network has a reachability agreement providing Quality-of-Service guarantees between endusers of the telecommunication system. This reachability agreement comprises the location of a point of attachment (TAP) of the VSNs and corresponding to a peering point (PP) of the data transport network through which data is exchanged between virtual service networks, an agreement to exchange routing information between virtual service networks, and the location of at least one virtual service network controller (VSNC) for each VSN, this virtual service network controller being adapted to exchange resource-signaling messages between the VSNs and to perform end-to-end admission control for the end-users dataflows.

[0049] US 2003/037163 concerns, in a communication method: processing for designation of a service provider, user authentication, and IP address assignment is performed by exchanging management frames between a user terminal

and a service provider through an access network; and main-signal frames each having an IPoE form and containing a source Layer 2 address of the user terminal are exchanged between the user terminal and the service provider through the access network. The management frames have a form which can be discriminated from the main-signal frames in Layer 2, and the access network holds information on correspondences between source Layer 2 addresses and virtual private networks.; The access network recognizes one of the virtual private networks connected to the service provider, based on the source Layer 2 address contained in each main-signal frame, and transfers the main-signal frames in Layer 2 by MAC bridging.

SUMMARY

[0050] The invention is defined by claims 1, 4 and 8, with various embodiments as defined in the dependent claims. The present invention provides a solution for operator shop, or access service provider, which, in the context as used herein, can be regarded as more or less equivalent to an ISP, selection by the end user in a broadband access network with multiple operator shops connected. When multiple operator shops are connected to the same broadband network a user accessing the network may have to indicate which of the operator shops that should provide the services. This applies to dynamically established session associations, i.e. when the association with an operator shop is not permanently tied to a physical attribute, such as an access port, but is instead created as a result of a user login or service access procedure. This solution can be valid for both users in their home network and roaming users. For a user accessing his home broadband network this means that he must indicate his home operator shop. For a user accessing a foreign broadband network it means that he must indicate an operator shop with which his home operator shop has a roaming agreement.

[0051] The current invention proposes a solution for operator shop, or AccSP, selection both for a user accessing his home broadband network and for the case when a roaming user is accessing a foreign broadband network. This is an important mechanism when mobility is introduced in the broadband access networks.

[0052] The solution for operator shop selection complements FSS in that it allows an end user to select the operator shop from which to access services. FSS, i.e. DHCP option 121, may then be used by the selected operator shop to provide the end user device with routing and gateway (GW) information to the different application services.

[0053] The operator shop selection solution further adds support for a roaming end user visiting a foreign broadband access network to select the desired visited operator shop.

[0054] The invention may provide both layer 2 and layer 3 solution mechanisms. The layer 2 mechanisms are based on associations of the appropriate VLANs as triggered by a user authentication procedure, possibly complemented by manual indications on a service portal. The layer 3 mechanisms are based on IPsec (IP Security protocol suite, a set of standards used to provide security services at the IP layer) tunnels between the terminals and suitable endpoint or endpoints in the network using IKEv2 (Internet Key Exchange version 2) with the NAT traversal detection option and the extensible authentication protocol (EAP) as the integrated authentication mechanism.

[0055] The solution is comprehensive enough to cover a wide variety of access scenarios, including accessing the broadband access network through a dedicated RG port, a non-dedicated RG port, a home WLAN access point (AP), a home NAT, and a public WLAN AP, provided by the broadband access network.

[0056] Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the methods, processes, instrumentalities and combinations particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0057] While the novel features of the invention are set forth with particularly in the appended claims, a complete understanding of the invention, both as to organization and content, and of the above and other features thereof may be gained from and the invention will be better appreciated from a consideration of the following detailed description of non-limiting embodiments presented hereinbelow with reference to the accompanying drawings, in which:

- Fig. 1a is a general view illustrating a user device or user terminal accessing one of a plurality of service providing networks through a broadband access network,
- Fig. 1b is a schematic view similar to Fig. 1a illustrating also authentication entities or units,
- Fig. 1c is a schematic view of a broadband access network architecture illustrating also various units or devices used for the user device or terminal when connecting to the broadband access network,
- Fig. 2a is a more detailed view of parts of the broadband access network of Fig. 1c that are relevant for operator shop selection,
- Fig. 2b is a view similar to Fig. 2a where a WLAN AP does not support virtual APs,

Samsung Ex. 1004, Page 298 of 563

- Fig. 2c is a view similar to Fig. 2a where a terminal is connected to an RG via a router having an NAT,
- Fig. 2d is a view similar to Fig. 2a where an IPsec tunnel passes in a BRAS and ends in a local VRF of the BRAS,
- Fig. 2e is a view similar to Fig. 2a where an IPsec tunnel passes through a dedicated VRF in a BRAS, an operator shop, the Internet and ends in a BAS of another operator shop,
- Fig. 2f is a view similar to Fig. 2a where an IPsec tunnel passes through a first dedicated VRF and a second dedicated VRF up to a BAS of the operator shop associated with the second dedicated VRF,
- Fig. 2g is a view similar to Fig. 2a where an IPsec tunnel passes through a first dedicated VRF up to an IPsec tunnel endpoint server,
- Fig. 2h is a view similar to Fig. 2g where an IPsec tunnel passes from a terminal through a router connected in a customer premises network, a first dedicated VRF up to an IPsec tunnel endpoint server,
- Fig. 2i is a view similar to Fig. 2a relevant for a user roaming in a foreign broadband access network,
- Fig. 2j is a view similar to Fig. 2i relevant for a user roaming in a foreign broadband access network for the case where a WLAN AP does not support virtual APs,
- Fig. 2k is a view similar to Fig. 2a where an IPsec tunnel passes through a first dedicated VRF up to another dedicated VRF acting as an IPsec tunnel endpoint server,
- Fig. 3a is a signal diagram of procedural steps executed when a terminal accesses an operator shop through a CPN,
- Fig. 3b is a schematic block diagram of an access node used in the case of Fig. 3a,
- Fig. 4a is a signal diagram similar to Fig. 3a for a terminal accessing an operator shop through a wireless LAN access point supporting virtual APs,
- Fig. 4b is a signal diagram similar to Fig. 4a for a terminal accessing a service portal through a wireless LAN access point supporting virtual APs for obtaining information about available operator shops,
- Fig. 4c is a schematic block diagram of a wireless access node used in the case of Figs. 4a and 4b,
- Fig. 4d is a schematic block diagram of an authentication client used in the broadband access server for the case of Fig. 4a,
- Fig. 4e is a schematic block diagram of an authentication proxy server used in the broadband access server for the case of Fig. 4a,
- Fig. 4f is a flow-chart of steps performed in a modifier unit 99 in a wireless access node for the case of Fig. 4a,
- Fig. 5 is a signal diagram similar to Fig. 3a for a terminal accessing a wireless LAN access point requesting/for obtaining information on available services,
- Fig. 6a is a signal diagram similar to Fig. 4a for a terminal accessing an operator shop through a wireless LAN access point not supporting virtual APs,
- Fig. 6b is a schematic block diagram of an access node used in the case of Fig. 6a,
- Fig. 7a is a signal diagram similar to Fig. 3a for terminals accessing operator shops using IPsec tunnels having a common endpoint in the BRAS 17,
- Fig. 7b is a signal diagram similar to Fig. 7a for IPsec tunnels having dedicated endpoints in the BRAS,
- Fig. 7c is a schematic block diagram of a terminal used in the case of Fig. 7a,
- Fig. 7d is a schematic block diagram of a local virtual router function used in the case of Fig. 7a,
- Fig. 7e is a schematic block diagram of a dedicated virtual router function used in the case of Fig. 7a or 7b,
- Fig. 7f is a signal diagram similar to Fig. 7a for IPsec tunnels having tunnel endpoints in the BAS of the operator shop,
- Fig. 7g is a signal diagram similar to Fig. 7a when using a DHCP option for informing a terminal about tunnel endpoint addresses,
- Fig. 7h is a signal diagram similar to Fig. 7g in the case where the DHCP option includes FQDNs of tunnel endpoints,
- Fig. 7i is a signal diagram similar to Fig. 7g for the case where a terminal connects to a router having an NAT,
- Fig. 7j is a signal diagram similar to Fig. 7h for the case where a terminal connects to a router having an NAT,
- Fig. 8a is a signal diagram similar to Fig. 3a for a roaming user accessing a foreign operator shop with special software provided in the user's terminal,
- Fig. 8b is a schematic block diagram of an authentication proxy server used in the broadband access server for the case of Fig. 8a,
- Fig. 8c is a schematic block diagram of a terminal used in the case of Fig. 8a,
- Fig. 8d is a schematic block diagram of an authentication server used in an operator shop for the case of Fig. 8a,
- Fig. 9a is a signal diagram similar to Fig. 8a for a roaming user accessing a foreign operator shop without any special software provided in the user's terminal,
- Fig. 9b is a signal diagram similar to Fig. 9a for a procedure in which an EAP Authenticator is also used,
- Fig. 9c is a schematic block diagram of an authentication proxy server used in the broadband access server for the cases of Figs. 9a and 9b,
- Fig. 9d is a schematic block diagram of a logical unit used in the broadband access server for the cases of Figs. 9a and 9b,
- Fig. 9e is a schematic block diagram of an authentication server used in an operator shop for the cases of Figs. 9a

and 9b,

- Fig. 9f is a schematic block diagram of a service portal used in an operator shop for the cases of Figs. 9a and 9b, and
- Fig. 9g is a schematic block diagram of an authentication server that may be used in an operator shop for the cases of Figs. 9a and 9b.

DETAILED DESCRIPTION

[0058] System and methods including procedures for operator shop selection that includes both layer 2 mechanisms, i.e. basically methods, steps and devices for directly driving hardware, and layer 3 mechanisms, i.e. basically methods, steps and devices for connecting on a network level, will now be described.

Overview of the target broadband access network architecture

[0059] The network environment for the methods and devices as described herein generally includes a broadband access network 29 to which operator shops 3.1, 3.2 are connected and which is designed to serve users using their terminals 15 to connected to or through the broadband access network, see Fig. 1a. The broadband access network 29 is an access network allowing user devices to connect to it and allowing a sufficient rate of data communication between the user terminals and the operator shops, the term "broadband" referring only to the fact that communication of data or "content" should be possible between the user terminals and the operator shops. The operator shops may in the description below be considered equivalent to distinct service providing networks. Users are considered who connect only through the broadband access network of their own. Users are also considered who roam in or through other access networks. In the latter case the users are still assumed to have an operator shop 3h of their own that has some relation to one of the operator shops connected to the broadband access network 29.

[0060] Connection to or through a broadband access server requires an identification procedure and an authentication procedure that may be more or less combined with each other. Such an identification procedure may be provided by the AAA standard and is based on individual user identities in the form of network access identifiers (NAIs) having the format "name@realm", see B. Aboba, M. Beadles, "The Network Access Identifier, RFC 2486, January 1999, and B. Aboba et al., "The Network Access Identifier", RFC 4282, December 2005. An authentication procedure, that is also required for some parts of the system, may be the extensible authentication protocol (EAP), see L. Blunk, J. Vollbrecht: "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998, and L. Blunk et al.: "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004, of the EAP Working Group, IETF, and then the carrier for EAP may be assumed to be designed according to the standard IEEE 802.1X - 2001, "Port-Based Network Access Control". Some components that may be used in an identification/authentication procedure are illustrated in Fig. 1b. Thus, the broadband access network may include an access server called herein a BRAS (Broadband Remote Access Server) 17 that includes an authentication client unit such as an AAA client 23. An authentication proxy server such as an AAA proxy server 27 may be connected to or in the BRAS and can communicate with the authentication client unit. The operator shops 3.1, 3.2, 3h may each have an access server, called herein a Broadband Access Server (BAS) 19, 19h which includes an authentication client unit such as an AAA client 37, 37h. Each of these authentication client units can communicate with an authentication unit, also called authentication server, such as an AAA server 31, 31h, of the respective operator shop, and in the case where the proxy server is included, the communication is through the proxy server 27.

[0061] The legacy notion of a subscription in a broadband network is reused in the sense that a subscription can still be tied to a physical attribute of a home, e.g. a communication port to which the residential gateway 1 (RG) of the home or premises of a user is connected, see Fig. 1c. Subscribed services are delivered to the RG 1 using existing layer 2 mechanisms, i.e. per operator shop 3.1, 3.2, and possibly per service, VLAN separation, MAC forced forwarding (MAC-FF), see T. Melsen, S. Blake, "MAC-Forced Forwarding: A Method for Traffic Separation on an Ethernet Access Network", <draft-melsen-mac-forcedfwd-03.txt>, Personal Internet-Draft, IETF August 2004, Virtual MAC, see Michael Begley, "The Public Ethernet - The next-generation broadband access network", Ericsson Review No. 1 2004, or anti-spoofing address filtering, etc. A VLAN dedicated to a certain operator shop 3.1, 3.2 is hereinafter referred to as a service VLAN or an operator shop VLAN.

[0062] Overlaid on these mechanisms it is also possible for individual users to receive services based on their user identities, i.e. their NAIs. In this case the appropriate VLAN associations are dynamically established as a result of a user login procedure, whereas for services delivered to a certain RG 1, based on a physical attribute such as a communication port, these associations are permanent or semi-permanent. NAI based service delivery is required to allow roaming.

[0063] To allow volume based charging of traffic in another location than the user's home, where "home" is defined by the user's subscription, as well as to allow, for legal purposes, tracing of traffic originating from the subscribers, it is required that the source of traffic originating from a user in the broadband access network can be unambiguously

Samsung Ex. 1004, Page 300 of 563

identified. Thus, the traffic of each user has to be separated from other users' traffic. The basic method for accomplishing this in a broadband access network is a combination of the layer 2 mechanisms in VLANs, MAC-FF and virtual MAC or anti-spoofing address filtering. This applies both to connected customer premises networks 5 (CPNs) and to connected WLAN (Wireless LAN) APs 7. However, there are also a number of differences between the case where a user is connected through a conventional local area network such as a CPN 5 and the case where the user is connected through a wireless local area network 9, i.e. between the CPN case and the WLAN AP case:

- All applicable service VLANs, for different operator shops, are constantly available through the WLAN AP 7, whereas in the CPN case, appropriate service VLANs are made available when needed, dynamically for NAI based sessions and at subscription time for (semi-)permanent associations.
- For WLAN APs 7 the service VLAN separation is, normally, extended across the radio interface through associations with separate service set identifiers (SSIDs) whereas in the CPN case each RG port 11 may be associated with a service VLAN, through VLANs or ATM PVCs (Permanent Virtual Circuits) to the access node 13 (AN). However, WLAN APs 7 that do not support multiple SSIDs can also be used in the method and system as described herein.
- For WLAN APs 7 traffic separation over the radio interface is achieved using cryptographic mechanisms according to the standard document IEEE 802.11i, "Medium Access Control (MAC) Security Enhancements", 2004, whereas traffic separation in a CPN 5, when applicable, is achieved by using separate RG ports 11, i.e. one individual port for each user terminal 15 or, possibly, for each group of user terminals.

[0064] However, in a layer 2 based method for traffic separation the considered user terminal 15 must connect to a separate port 11 of the RG 1 when roaming into a CPN 5. This may be inconvenient in those cases where the terminals 15, 15' normally connect to the RG through a WLAN AP and/or an NAT, not shown in this figure. Moreover, in some cases a separate port may not even be available on the RG. Therefore, layer 3 based methods based on IPsec tunnels having source integrity and replay protection may also be used. Such methods cryptographically tie the traffic to an individual user or individual terminal 15, 15'. In the system and method as described herein two basic alternatives are considered for the remote endpoint of the IPsec tunnel, these alternatives including the broadband remote access server 17 and the broadband access server (BAS) 19.

[0065] The various methods as described herein may more specifically be performed e.g. in an architecture for a broadband access network as schematically illustrated in Fig. 1c, although the methods can also be applied to a plurality of variations of the illustrated architecture. Primarily, the location of the relevant nodes and the AAA entities in the broadband access network 29 are shown. The access node 13' between the WLAN AP 7 and the BRAS 17 may not be needed. This depends on whether the required AN functionality, e.g. mechanisms for traffic separation, can be handled by the WLAN AP 7. An alternative to having an AAA client 23 in the BRAS 17 is to have an AAA client 23' in each AN. In the general case as described herein and as seen in Figs. 1b and 1c, an AAA client 23 is located in the BRAS 17. This AAA client 23 is used for all accesses through CPNs 5 in the broadband access network. Its location in the BRAS 17 supports traffic separation on both layer 2, VLANs, MAC-FF, virtual MAC or anti-spoofing address filtering, and layer 3, IPsec tunnels. An AAA client 25 is also located in each WLAN AP 7. This location supports traffic separation on layer 2, using the proposed standard IEEE 802.11i over the radio interface and VLAN, MAC-FF and anti-spoofing address filtering between the WLAN AP 7 and the BRAS 17, employing the fact that many WLAN APs 7 intended for public access have AAA clients 25 implemented.

[0066] The BRAS 17 also has an internal AAA server 27 or is connected to an external AAA server, not shown. This AAA server 27 acts as an AAA proxy server. It facilitates the serving of multiple operator shops 3.1, 3.2 by the broadband access network 29 and allows the operator of the broadband access network to apply its own AAA policies in addition to those applied by that of the operator shop selected by a user. The AAA server 27 in the BRAS 17 or possibly only connected to the BRAS 17 has a relation to an AAA server 31 in each of the operator shops 3.1, 3.2 that the broadband access network 29 serves.

[0067] Hence, the AAA server 31 that actually authenticates and authorizes users is located in the operator shop 3.1, 3.2, since the operator shop "owns" the subscribers and manages the subscriptions.

[0068] The operator shop 3.1, 3.2 also has a broadband access server 19 (BAS) for delivery of services 33, e.g. available at servers 34 run by the operator of the operator shop or by individual service providers, and Internet traffic, see item 35. There may be an AAA client 37 in the BAS 19 for communicating with the AAA server 31 of the operator shop 3.1, 3.2 for authentication and authorization in conjunction with delivery of services to users roaming in other networks and possibly in conjunction with individualized delivery of services to users in the broadband access network 29, if a layer 3 traffic separation method is used.

[0069] The AAA protocol used between different AAA nodes, i.e. AAA servers 31 and clients 23, 23', 25, 37, is generally assumed to be RADIUS, see C. Rigney et al.: "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000, and B. Aboba, P. Calhoun: "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003. The AAA protocol can alternatively be Diameter, see P.

Samsung Ex. 1004, Page 301 of 563

Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko: "Diameter Base Protocol", RFC 3588, September 2003, and P. Eronen, Ed., T. Hiller, G. Zorn: "Diameter Extensible Authentication Protocol (EAP) Application", Internet draft <draft-ietf-aaa-eap-03.txt>, IETF, October 2003. These two protocols can both convey EAP packets. Also, any other AAA protocol that can convey EAP packets can be used. However, EAP is not required for all parts of the method and system as described herein, in which cases the AAA protocol may also be some suitable protocol that cannot convey EAP packets.

[0070] In addition to services 33 supplied through the operator shops 3.1, 3.2 the broadband access network 29 may provide local services, e.g. based on servers connected to a local service network connected to the BRAS 17, see e.g. the description of Fig. 2a below. Such local services are generally delivered for free to all users of the broadband access network, including roaming users.

Operator shop selection overview

[0071] A user is supposed to have a "home operator shop" and a "home access network", the latter also called "home broadband network" or possibly "home broadband access network", a home access network meaning a broadband access network through which the user's home operator shop can be reached directly, i.e. without using e.g. another operator shop having a roaming agreement with the user's home operator shop. The home broadband access network thus serves the user's home operator shop, by providing a connection to the home operator shop, and is assumed to have a service agreement with the user's home operator shop.

[0072] When multiple operator shops 3.1, 3.2 are connected to the same broadband access network 29 a user accessing the broadband access network must indicate that one of the available operator shops which is to provide the services.

[0073] For a user accessing his home broadband access network this means that the user must indicate his home operator shop. For a user accessing a foreign broadband access network, i.e. a broadband access network with which his home operator shop has no relation, it means that he must indicate an operator shop with which his home operator shop has a roaming agreement.

[0074] Fig. 2a is a more detailed view of those parts of the broadband access network that in a first case are relevant in conjunction with operator shop selection. It should be emphasized that the details of the architecture depicted in Fig. 2a, and also in Figs. 2b - 2k, should be seen as exemplary embodiments. Various variations are possible, while still adhering to the basic principles of the method and system as described herein. However, also Fig. 2a is a simplified illustration. E.g. the AAA server 27 of the BRAS 17 is advantageously protected by security means, such as a firewall etc., not shown.

[0075] Two service VLANs, VLAN No. 1, 41.1, and VLAN No. 2, 41. 2, each associated with an own operator shop No. 1, 3.1, and No. 2, 3.2, respectively, are depicted. The other two VLANs are local VLANs, the local default VLAN 43 and the local WLAN AP VLAN 45 that are used for user authentication, this only performed by the local default VLAN 43, for operator shop selection and for access to local services, i.e. services that are directly provided by the BRAS 17.

[0076] The VRF (Virtual Router Function) No. 1, 47.1, and the VRF No. 2, 47.2, of the BRAS 17 are each dedicated to a single operator shop 3.1, 3.2, respectively. The local VRF 49 of BRAS 17 has a central role in the operator shop selection mechanisms, e.g. in handling authentication and in some cases for handling IPsec tunnels. The VRFs are interconnected, such as being connected in an inter-VRF network 52.

[0077] The local service network 51 that is connected to or in the BRAS 17 and also may be connected to or include the inter-VRF network 52, may advantageously have a number of VLANs, not shown, configured so as to isolate VRF No. 1, 47.1, and VRF No. 2, 47.2, from each other, isolate servers, e.g. local servers 53, from each other when applicable, etc. In the simplified schematic illustration the AAA server 27 of the BRAS 17 is shown to be connected to the same local service network 51 as the local servers 53. However, it could be advantageous if this AAA server 27 is connected to a separate network surrounded by more rigorous security measures, not shown. At least, the AAA server 27 of the BRAS 17 should be isolated and protected from unauthorized access by having a separation performed by a VLAN, not shown. The local VRF 49 should preferably employ VLAN aggregation, according to D. McPherson, B. Dykes, "VLAN Aggregation for Efficient IP Address Allocation", RFC 3069, February 2001, for the local service network 51, and the VLANs in which it may be divided, so that the local VRF can be reached using the same IP address from all other VRFs across the local service network 51 and/or the inter-VRF network 52. However, these VLANs used in BRAS internal networks such as in the local service network 51 and in the inter-VRF network 52 are not illustrated in the figures.

[0078] There are two main cases which the methods for operator shop selection may handle:

- A user accessing his home broadband access network, i.e. a broadband access network that is connected to the user's home operator shop.
- A user accessing a foreign broadband access network, i.e. a broadband access network that has no relation to the user's home operator shop.

Samsung Ex. 1004, Page 302 of 563

Operator shop selection in a home broadband access network

[0079] Selection of an operator shop is not applicable for common services for all users or devices within a CPN 5 such as in the case where an RG port 11 of the CPN is permanently or semipermanently associated with the home operator shop of a user. In that case the home operator shop has already been "selected" through the permanent or semipermanent association. Only associations dynamically established per session are discussed herein.

[0080] The cases that should be considered in a home broadband access network include:

- The user accesses his home operator shop through a CPN 5 connected to/in her/his home broadband access network.
- The user accesses his home operator shop through a WLAN AP 7 connected in her/his home broadband access network.
- The user accesses his home operator shop through an IPsec tunnel established through her/his home broadband access network.

Access through a CPN

[0081] The RG port VLAN 55 of an RG port 11 of an RG 1 in a CPN 5 is, in the case discussed herein and when there is no active session activated from a user terminal 15, by default associated with the local default VLAN 43. This association is present as a logical connection internally in the AN 13 to which the RG 1 is connected. That a VLAN is associated with another VLAN generally means that the VLANs are logically connected through a node, such as by a table entry in a table in the node, so that frames in one of the VLANs are automatically transmitted into the other VLAN. Generally, there may thus be provided some indication of such associations by e.g. the contents of a memory cell, not shown, in the AN. Thus, when a user connects to an RG port 11, the local default VLAN 43 is all that the user can reach, i.e. in this case frames received in the AN 13 from the RG port 11 are automatically transmitted also into the local default VLAN. Before the user is authenticated, the procedures according to the standard document IEEE 802.1X will not allow any other communication with the user's terminal 15 than sending and receiving messages carried in EAP packets, or in other packets related to the procedure of logging in to the broadband access network 29 such as for accessing operator shop No. 1 or 2, 3.1 or 3.2, such packets being e.g. PPPoE packets, see L. Mamakos et al., "A Method for Transmitting PPP over Ethernet (PPPoE)", RFC 2516, February 1999, in the case where an authentication method different from EAP over IEEE 802.1X is used. Any Ethernet frame sent from the user's terminal 15 will trigger the local VRF 43 to initiate an EAP authentication procedure towards the terminal, in accordance with the standard document IEEE 802.1X, using some authenticator function or unit symbolically indicated at 56 in the BRAS 17 in Fig. 2a.

[0082] During the EAP procedure the local VRF 43 relays the EAP packets to the AAA client 23 of the BRAS 17, which forwards them to the AAA proxy server 27 of the BRAS. The AAA proxy server 27 examines the realm part of the NAI that the user supplies in an EAP-Identity-Response message in order to determine what to do with the EAP procedure, i.e. to determine the AAA server to which it is to be directed or if it is to be handled internally, in the case where the user wants access only to the local service network 51. A home realm is the administrative domain with which a user maintains an account relationship and a local realm is the administrative domain providing services to a user. An administrative domain may act as a local realm for some users, while being a home realm for others. The network access identifier (NAI) is used in the Diameter protocol to extract a user's identity and realm. The identity is used to identify the user during authentication and/or authorization, whereas a user's realm is used for message routing purposes. The string in the NAI that precedes the "@" character is the name part and gives the identity of the user, the "username". The string in the NAI that immediately follows the '@' character is the realm part holding an NAI realm name. NAI realm names are required to be unique. An AAA entity employing the Diameter or RADIUS protocol makes use of the realm defined by the realm part, also loosely referred to as domain, to determine whether messages from or to the user can be satisfied locally in the AAA entity, or whether they must be routed or redirected to another AAA entity. In the case considered here the user accesses his home broadband access network 29 and the realm part of the NAI indicates the user's home operator shop, i.e. either operator shop No. 1, 3.1, or operator shop No. 2, 3.2. An example of an NAI is "happy-user@op-shop1"

For this NAI the AAA proxy server 27 will relay the AAA packets between the AAA client 23 and the AAA server 31 of the operator shop indicated by the NAI, operator shop No. 1, 3.1, in the example. Hence, operator shop No. 1, 3.1, has been selected.

[0083] After a successful authentication the BRAS 17 instructs the concerned AN 13 in a suitable way, e.g. via the simple network management protocol (SNMP), see D. Harrington et al., "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", RFC 3411, December 2002, or some other protocol that the BRAS can use to control ANs, to associate the concerned RG port VLAN 55 with VLAN No. 1, 41.1, instead of the local default VLAN 43. Then the user can through his terminal 15 proceed to acquire an IP address using DHCP to enable

Samsung Ex. 1004, Page 303 of 563

subsequent IP communication. In order for the BRAS 17 to know which AN 13 to instruct, virtual MAC must be used. The EAP procedure in itself does not give the BRAS 17 any information about which AN 13 that is being involved in the procedure. Furthermore, the Ethernet network infrastructure between the AN 13 and the BRAS 17 does not allow the BRAS to trace the node from which a considered frame has arrived. Also, the (original) source MAC address of the user terminal 15 carries no location or topology information. Thus, in order for the BRAS 17 to know which AN 13 to instruct, the AN must replace the original source MAC address of the user terminal 15 with a virtual MAC address that indicates the responsible AN. To ensure that the BRAS 17 can tell to which AN 13 a virtual MAC address belongs, the different ANs are allocated different parts of the virtual MAC address range.

[0084] The AAA client can instead be located in the AN, see item 23' of Fig. 1, and then neither the local default VLAN 43 nor the virtual MAC address is needed for this purpose.

[0085] If access only to the local service network 51 is desired, the user can supply a special NAI, with a realm part belonging to the broadband access network 29, dedicated for this purpose. The user can have obtained it through off-line means or other mechanisms that are used to inform a user about available operator shops as described hereinbelow. The AN 13 can then keep its association between the concerned RG port VLAN 55 and the local default VLAN 43.

[0086] The different steps in accessing an operator shop 3.1, 3.2 for the case where the AAA client 23 is located in the BRAS 17 are summarized below with reference to the signal diagram of Fig. 3a. The user is assumed to be logged in to a CPN 5 on a terminal 15 having an MAC address and in particular connected to a specific port 11 of the RG 1, the user identified by also this specific port.

1. A user connects her/his terminal 15 to a broadband access network, e.g. by the user simply turning on his terminal device that is assumed to be connected to an RG port 11. Then, the terminal 15 sends an EAPOL-Start-packet to the multicast address of "Port Access Entity" (PAE), called the "PAE group address" in the IEEE 802.1X specification, this specification defining PAE as the unit handling the authentication procedure towards the terminal and containing the "EAP Authenticator". The EAP Authenticator is defined as the unit communicating with the terminal 15 in an EAP-procedure, and may symbolically be indicated as the unit 56 in Fig. 2. The PAE maintains a list defining in some way the frames allowed to pass. If any, these frames may be defined by certain allowed values of the Type field in the frame header or of certain allowed attributes of a higher layer packet included in the frame, such as a destination IP address or a destination UDP port number, other frames being blocked because the respective user is not authenticated. If the terminal 15 sends a frame containing something else than an EAPOL-Start packet, the EAP Authenticator 56/PAE/local VRF 49 will intercept the frame and initiate an EAP procedure towards the terminal by sending an EAP-Identity-Request packet to the terminal.
2. A frames or frames from the terminal 15 is/are received through the residential gateway 1 or switch in the AN 13 and retagged to be transmitted into local default VLAN 43, also a VMAC address being introduced in the frames, the VMAC address identifying the terminal 15 and the AN. The assigned VMAC address primarily identifies the terminal 15, but by allocating different portions of the virtual MAC address range to different ANs, as mentioned above, it can also identify the AN 13.
3. A retagged frame or retagged frames from the terminal 15 is/are received in the local VRF 49 of the BRAS 17. An EAPOL-Start packet may specifically be received by the EAP Authenticator, i.e. the PAE, in or connected to the local VRF 49. If a frame including an unauthorized MAC address or VMAC address is received, a new user is detected, the frame is intercepted and given to be processed by the EAP Authenticator such as the unit 56.
4. The EAP Authenticator in the local VRF 49 sends an EAP-Identity-Request to the terminal 15.
5. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of an NAI, as described above.
6. The EAP Authenticator 56 passes the EAP-Identity-Response to the AAA client function 23 located internally in the BRAS 17.
7. The AAA client 23 includes the EAP-Identity-Response in an AAA message and sends the AAA message to the AAA proxy server 27, which may be part of the BRAS 17 as illustrated, or may be co-located with the BRAS.
8. The AAA proxy server 27 recognizes, using the example above, that operator shop No. 1, 3.1, is wanted by retrieving and examining the realm part of the NAI, indicating the user's home operator shop, as supplied by the user in the EAP-Identity-Response packet and in the User-Name attribute in the AAA message. Thus, the AAA proxy server 27 can find the NAI in the User-Name attribute, but theoretically it could also extract it from the EAP-Identity-Request that is encapsulated in the AAA message. In addition, Diameter clients, i.e. AAA clients using the Diameter protocol, also insert the realm part of the NAI in the Destination-Realm attribute, which the AAA proxy server 27 can then use to identify the desired operator shop. The AAA proxy server 27 transmits the AAA request to the AAA server 31 in operator shop No. 1, 3.1.
9. An EAP authentication procedure between the AAA server 31 in operator shop No. 1, 3.1, and the user terminal 15 through the AAA proxy server 27 and the AAA client 23 of the BRAS 17 is performed. The EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31

Samsung Ex. 1004, Page 304 of 563

of operator shop No. 1, 3.1. Between the AAA client 23 of the BRAS 17 and the AAA server 31 the EAP packets are encapsulated in AAA messages.

10. The BRAS 17 includes a logical function unit 57 (LU) obtaining information that the AAA procedure has been completed and about the operator shop that has been selected. This is done by the AAA server 31 of the selected operator shop informing the AAA client 23, through an AAA message, after the authentication procedure has been successfully finalized, the AAA client 23 in turn informing said logical function 57, and since the AAA proxy server 27 is also informed through the same AAA message, the AAA proxy server can also be the one informing said logical function. The logical function unit 57 instructs the AN 13 to change the existing association between VLANs, using the VMAC address of the terminal 15 to find the correct AN 13. The VMAC address is a locally administered MAC address that is assigned to the terminal 15 and is locally unique in the broadband access network. Hence the assigned VMAC address "belongs to" and identifies the terminal 15, although the terminal itself never sees the VMAC address or is not aware of its existence. As mentioned above, by allocating different parts of the VMAC address range to different ANs, the VMAC address assigned to the terminal 15 can also be used to identify the AN 13 that assigned it to the terminal. The information on the selected operator shop is obviously available inside the BRAS 17 and the above procedure can be performed in various ways, such as:

a) When the AAA proxy server 27 identifies the selected operator shop, it notifies some other part of the BRAS 17, e.g. the LU 57, of the selection made and which VMAC address it concerns, the latter case requiring that the AAA client 23 includes the VMAC address of the terminal 15 in the AAA message. The LU 57 may receive the operator shop selection information in the form of the realm part of the NAI or some other BRAS internal identifier to which the AAA proxy server 27 has translated the realm part. Then the LU 57 only has to wait for a notification of a successful user authentication before instructing the AN 13 to associate certain VLANs.

b) The AAA client 23 or the EAP Authenticator, such as the unit 56, passes the realm part of the NAI and the VMAC address to some other part of the BRAS 17, e.g. the LU 57, even before transmitting the first AAA message to the AAA proxy server 27. The LU 57 then only has to wait for an indication of a successful user authentication.

c) After the AAA client 23 has received, from the AAA server 31 in the selected operator shop, via the AAA proxy server 27, the AAA message including the indication of a successful user authentication, it informs some other part of the BRAS 17, e.g. the LU 57, about the VMAC address of the terminal 15 and the selected operator shop, e.g. in the form of the realm part of the NAI, or some other BRAS internal identifier indicating the selected operator shop. The LU 57 may then, if needed or desired, translate the realm part of the NAI, or other BRAS internal identifier respectively, to some BRAS internal identifier, e.g. a VLAN ID.

d) When the AAA proxy server 27 receives, from the AAA server 31 of the selected operator shop, the AAA message including the indication of a successful user authentication, it informs e.g. the LU 57 about the VMAC address of the terminal 15, this requiring that the AAA client 23 has previously included the VMAC address in an AAA message, and about the selected operator shop associated with this VMAC address. The selected operator shop can then be indicated as an FQDN (Fully Qualified Domain Name), i.e. the realm part of the NAI, or as a BRAS internal identifier identifying the operator shop. The AAA proxy server 27 should of course also forward the AAA message to the AAA client 23.

11. The AN 13 receives an instruction message such as "Associate the RG port VLAN of VMAC X with VLAN No. 1", where the VMAC address allocated to the terminal 15 is denoted by "X", the RG port VLAN is the VLAN 55 of the RG port 11 to which the terminal identified by VMAC X is connected and it is assumed that the user wants access to operator shop No. 1, 3.1. The AN 13 accordingly changes tagging for VLANs so that frames from the concerned RG port VLAN 55 are tagged for VLAN No. 1 instead of being tagged for the local default VLAN. It can be done by e.g. the AN changing a record in a VLAN association table or generally in some data structure that the AN uses to keep track of associations between VLANs. Such a data structure can be implemented in a variety of ways obvious to one skilled in the art.

12. After the user has become authenticated, the terminal 15 can proceed to acquire an IP address. It will be an IP address from the address range of operator shop No. 1, 3.1. The IP address is supplied by a suitable address server such as an DHCP server 59 in operator shop No. 1, 3.1, e.g. located in the BAS 19. The respective address server, the DHCP server 61.1, in the BRAS 17 will act as a relay agent for performing the assigning of an address, i.e. DHCP, in this procedure. In this case the address server acting as a DHCP relay agent is associated with the VRF No. 1, 47.1, for operator shop No. 1, 3.1. Alternatively the DHCP server 61.1 in the BRAS 17 can allocate IP addresses directly to the terminal 15 from the address range of operator shop No. 1, 3.1. This requires that the DHCP server 61.1 in the BRAS 17 has been given a pool of addresses out of the address range of operator shop No. 1, 3.1.

13. After the terminal 15 has been given an IP address, the user can start traffic using TCP/IP, through VLAN No. 1, 41.1, VRF No. 1, 47.1, and the BAS 19 of operator shop No. 1. For example, the user can receive a web page

Samsung Ex. 1004, Page 305 of 563

of the BAS 19 of operator shop No. 1. Such a web page can present services that can be accessed through operator shop No. 1. This can be achieved by e.g. the user's browser having the web page of the selected operator shop set as its start page, such as configured manually by the user according to instructions from the operator shop when the subscription to this operator shop was agreed on. The services can, as illustrated in Fig. 1, include access to the Internet, and services 33 provided by specific service providers from one or more service servers 34.

[0087] The AN 13 may have at least the following modules/components/functions which may be necessary to perform the operator shop selection and access in this case, see Fig. 3b:

- A VLAN handler 71, including a submodule 73 for receiving instructions of changed association and for changing associations accordingly.
- A VLAN association table, see the example in Table 1 below, stored in a memory place 75 in a memory 77.
- A VMAC address handler 79 including a unit for translating between MAC and VMAC.
- A VMAC address table stored in a memory place 81 in the memory 77.
- An MAC address to IP address table stored in a memory place 83 in the memory 77.

[0088] An example of the structure of a VLAN association table is given in Table 1.

Table 1. VLAN association table for N different RG ports

VLAN at the customer premises side	VLAN at the network side
RG port VLAN No. 1	VLAN No. 1
RG port VLAN No. 2	VLAN No. 1
RG port VLAN No. 3	Local default VLAN
RG port VLAN No. 4	VLAN No. 2
:	:
:	:
RG port VLAN No. N	VLAN No. 1

[0089] The BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 2a:

- A BRAS internal network, such as the inter-VRF network 52, including a connection to or including the local service network 51.
- A local VRF 49 connected in the BRAS internal network.
- An EAP authenticator/PAE such as the unit 56.
- An AAA client 23 directly connected to the local VRF 49 and to the AAA proxy server 27.
- An AAA proxy server 27 connected in the BRAS internal network and to AAA servers 31 in operator shops Nos. 1 and 2, 3.1 and 3.2.
- A dedicated VRF No. 1, 47.1, connected in the BRAS internal network for routing traffic only to and from operator shop No. 1, 3.1, except for certain special cases when traffic can be routed differently. The VRF No. 1 functions as the access router of operator shop No. 1 in the broadband access network 29. From the point of view of operator shop No. 1, 3.1, VRF No. 1 appears as part of or connected in the own network of operator shop No. 1.
- A dedicated VRF No. 2, 47.2, connected in the BRAS internal network for routing traffic only to and from operator shop No. 2, 3.2, except for certain special cases when traffic can be routed differently.
- An association instruction unit or logical function unit LU 57 for monitoring AAA procedures and for instructing ANs 13 to change associations between VLANs.
- A DHCP server 61.1 for operator shop No. 1.
- A DHCP server 61.2 for operator shop No. 2.

Access through a WLAN AP supporting the virtual AP concept

[0090] It can first be assumed that the WLAN AP 7 supports the virtual AP (vAP) concept, i.e. that it has the capability or includes the function of emulating multiple logical APs in a single physical AP, see Fig. 2a. In such a case each operator shop 3.1, 3.2 connected to the broadband access network 29 is also assumed to have "its own" logical AP

63.1, 63.2 with a dedicated SSID being broadcast in beacon messages from the AP. Such a logical AP may be a unit incorporated in the WLAN AP 7, the unit including e.g. a unit for handling the virtual APs and a memory having a memory place for storing required data, such as a suitable list, not shown, see below. Furthermore, the WLAN AP 7 associates each operator shop SSID with the VLAN 41.1, 41.2 dedicated for the respective operator shop, such that all traffic, from authenticated users, pertaining to a certain SSID is passed to the associated VLAN and vice versa. The WLAN AP 7 also has an own or local logical AP 65 and a corresponding SSID associated with the local WLAN AP VLAN 45, which allows a user access to the local service network 51. In Fig. 2a the SSIDs for the operator shops Nos. 1 and 2 are denoted by "SSID 1" and "SSID 2", respectively, and the SSID for the local WLAN AP VLAN 45 is denoted by "SSID local".

[0091] When accessing the broadband access network 29 through a WLAN AP 7 supporting the virtual AP concept, the user must select the SSID associated with his home operator shop, this being one of the operator shops 3.1, 3.2 available through the WLAN AP, see the signal diagram of Fig. 4a, or the SSID associated with the local WLAN AP VLAN 45 for delivery of publicly available services, see the signal diagram of Fig. 4b. The SSID could preferably be a character string that is easily interpreted by human beings, e.g. the name of the desired operator shop or its realm-FQDN (Fully Qualified Domain Name). Then the terminal 15' can scan for broadcast SSIDs and present the result to the user of the terminal, who can then manually select the one belonging to his home operator shop. It is also possible to configure the terminal to search for and attach to (i.e. associate with) a certain SSID.

[0092] If the SSID information is not enough for the user to select an operator shop, i.e. to select one of the SSIDs, he may attach to (i.e. associate with) the SSID associated with the local WLAN AP VLAN and obtain more information, about available operator shops and their associated SSIDs, from the service portal 54 before manually selecting one of the SSIDs associated with operator shops 3.1, 3.2, see Fig. 4b. In the local WLAN AP VLAN 45 the user is allowed access and can acquire an IP address without a prior user authentication.

[0093] When the user attaches to the WLAN AP 7 using an SSID selected among those associated with available operator shops 3.1, 3.2, the AAA request resulting from the EAP authentication procedure is routed, via the BRAS AAA proxy server 27, to the operator shop 3.1 or 3.2 that is associated with the SSID, irrespective of what NAI the terminal 15' supplies. If the NAI does not indicate the operator shop associated with the selected SSID in the realm part, the WLAN AP 7 can either reject the access request or force the AAA request to be routed to the operator shop associated with the selected SSID. To force the AAA request to be routed to the operator shop 3.1 or 3.2 associated with the selected SSID, despite another realm indicated in the NAI, the WLAN AP 7 can either modify the received NAI into an extended format that includes an intermediate network realm or communicate the selected SSID in some suitable way, e.g. included in a vendor specific AAA attribute, such as using some suitable protocol extension. In the latter case, if the SSID is passed to the AAA proxy server 27 in some way such as in an AAA attribute, the AAA proxy server would use the SSID, instead of the realm part of the NAI, to direct the AAA message to the AAA server 31 of the selected operator shop, this requiring that the AAA client 25 and the AAA proxy server are provided with the corresponding additional function, see Figs. 4d and 4e. In the former case, called the extended NAI method, the extended NAI has the general format

"home-realm/name@intermediate-realm" or

"home-realm!name@intermediate-realm"

where "home-realm" is the realm of the home network/home operator shop, "intermediate-realm" is the realm of a selected intermediate network/intermediate operator shop and "name" is the user's username. A field or name separator "/" or "!" or possibly some other suitable symbol or character is used to differentiate between the "extra" realm which in this case is the original realm, and the user name. Such extended NAIs are already used by the WLAN roaming broker iPass and it is planned that they will be used in the 3GPP-WLAN interworking. In this specific case the format of the extended NAI, into which the WLAN AP may modify the received NAI, would be

"realm-supplied-in-NAI/name@op-shop-realm-associated-with-selected-SSID" or

"realm-supplied-in-NAI!name@op-shop-realm-associated-with-selected-SSID"

[0094] The modification of the NAI to an extended format can be executed by a special unit, a NAI modifier unit 99 in or connected to the respective virtual AP 63.1 or 63.2, see Fig. 4c. The procedure for modifying the NAI to an extended format is illustrated in the flow chart of Fig. 4f, where, after an EAP-Identity response message has been received in a virtual AP, see step 111, the SSID specified in a previous request for "associating" from the terminal 15' and also unique for the respective virtual AP is in a step 113 compared to the realm of the NAI included in said response message. If the result of the comparison is that two different operator shops are specified, the NAI is modified in a step 115. Finally, whatever the result of the comparison is, in a step 117 an AAA request is transmitted to the AAA proxy server 27 of the BRAS 17.

[0095] Thus, it has been described how the AAA routing can be modified to ensure that it routes according to the selected SSID, even if the user has supplied a NAI that does not indicate the operator shop associated with the selected SSID, where the SSID selection has precedence over the NAI in this case. Two ways are described: one way is to base the AAA routing explicitly on the selected SSID, which requires that the SSID is being included in an AAA attribute, and the other way is to modify the NAI in a way that makes the AAA routing direct the AAA messages to the correct operator shop 3.1 or 3.2, i.e. the one associated with the selected SSID. The user may e.g. erroneously supply a NAI that does

Samsung Ex. 1004, Page 307 of 563

not belong to the operator shop of the selected SSID, such as by a mistake made during SSID selection or during manual NAI entering. In any case it is ensured that access using the virtual AP 61.1 or 61.2, with its associated SSID, of one operator shop 3.1, 3.2 is not handled by the AAA server 31 of another operator shop.

[0096] Following a successful user authentication the user can proceed to acquire an IP address via DHCP to enable subsequent IP communication.

[0097] The different steps in accessing an operator shop in the case where the user through his terminal 15' chooses access to a WLAN virtual AP 63.1, 63.2 associated with an operator shop 3.1, 3.2 are summarized below with reference to the signal diagram of Fig. 4a.

1. The WLAN AP 7 is transmitting SSIDs for a plurality of WLAN virtual APs associated with VLANs 41.1, 41.2, 45 connected in the BRAS 17.
2. The terminal 15' transmits a request for "associating" with the WLAN virtual AP 63.1, 63.2 for a selected SSID among those associated with operator shops Nos. 1 and 2, 3.1 and 3.2.
3. The selected WLAN virtual AP 63.1 or 63.2 transmits an association response to the terminal 15'.
4. The WLAN virtual AP 63.1, 63.2 transmits, thereby starting an EAP procedure, from its EAP Authenticator, symbolically drawn as item 67 in Fig. 2a, an EAP-Identity-Request to the terminal 15'.
5. The terminal 15' responds with an EAP-Identity-Response, including the user's identity in the form of an NAI.
6. The EAP Authenticator 56 passes the EAP-Identity-Response to the AAA client function 25 of the WLAN AP 7. Before or in this step, the procedure described above for including the SSID in an AAA attribute or for a possible modification of the NAI supplied by the user can be executed.
7. The AAA client function 25 in the WLAN AP 7 transmits the AAA request, including the NAI supplied by the user in the response and possibly the SSID of the selected WLAN virtual AP 63.1, 63.2, to the AAA proxy server 27 in BRAS.
8. The AAA proxy server 27 recognizes, from the SSID that may be included in the AAA request or from the realm part of the NAI, that operator shop No. 1, 3.1, is wanted and transmits the AAA request to the AAA server 31 in operator shop No. 1.
9. An EAP authentication procedure between the AAA server 31 in operator shop No. 1 and the user terminal 15' through the AAA proxy server 27 of the BRAS 19 and the AAA client 25 of the WLAN AP 7 is executed. The EAP procedure is handled end-to-end between the terminal and the authentication server which is the AAA server. Between the AAA client 25 and the AAA server 31 the EAP packets are encapsulated in AAA messages.
10. The WLAN AP 7 is informed that the authentication has been successfully completed, through an AAA message which goes all the way to the AAA client 25 in the WLAN AP. The WLAN AP then allows frames from and to the concerned terminal 15' to be forwarded. The selected SSID already indicates to which VLAN, in this example VLAN No. 1, 41.1, the uplink frames should be forwarded. No VMAC address is needed. Source integrity protection using the mechanisms of IEEE 802.11i ensures that no other terminal can use the same MAC address for communication through the WLAN AP 7.
11. The WLAN AP 7 starts forwarding frames from and to the terminal 15' using VLAN No. 1 by tagging frames accordingly.
12. After the user has been authenticated, the terminal 15' can proceed to acquire an IP address.

[0098] This will be an IP address from the address range of operator shop No. 1. It is supplied by the DHCP server 59 in operator shop No. 1, e.g. located in the BAS 19. The respective DHCP server 61.1 in the BRAS 17 will act as a DHCP relay agent in this procedure. In this case the DHCP server acting as a DHCP relay agent is associated with the VRF No. 1, 47.1, for operator shop No. 1. Alternatively, the respective DHCP server 61.1 in the BRAS can allocate the IP address out of the address range of operator shop No. 1 without involving any DHCP server in operator shop No. 1. In that case the respective DHCP server 61.1 of the BRAS has to have been given a dedicated pool of IP addresses out of the address range of operator shop No. 1. 13. After the terminal 15' has been given an IP address, the user can start traffic using TCP/IP, through VLAN No. 1, 41.1, VRF No. 1, 47.1, and the BAS 19 of operator shop No. 1, 3.1. For example, the user can receive a web page of the BAS of operator shop No. 1. Such a web page can present services that can be accessed through operator shop No. 1.

[0099] The WLAN AP 7 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 4c:

- An RF transmitter/receiver 91 connected to an antenna 93 and including a unit 95 for transmitting broadcast messages including SSIDs and a unit 97 for receiving and transmitting frames to terminals 15' that have already established a connection with the WLAN AP and that want to establish a connection.
- A local virtual AP function 65.
- A virtual AP function 63.1 for operator shop No. 1, 3.1 holding a NAI modifier unit 99.
- A virtual AP function 63.2 for operator shop No. 2, 3.2 holding a NAI modifier unit 99.

Samsung Ex. 1004, Page 308 of 563

- An SSID-VLAN association list stored in a memory place 101 in a memory 103.
- A VLAN handler 105.
- An AAA client 25.
- An authenticator function/entity 67.

[0100] The BRAS 17 may have at least the following modules/components that may be necessary to perform the operator shop access in this case:

- A BRAS network including connection to/including the local service network 51.
- A local VRF 49 connected in the BRAS internal network.
- An AAA client 23 directly connected to the local VRF 49 and capable of communicating with the AAA proxy server 27.
- An AAA proxy server 27 connected in/to the BRAS network and capable of communicating with the AAA servers 31 in operator shops Nos. 1 and 2 when required, having security relations with them.
- A VRF No. 1, 47.1, connected in the BRAS network for routing traffic only to/from operator shop No. 1, except for certain special cases when traffic can be routed differently. The VRF No. 1 functions as the access router of operator shop No. 1 in the broadband access network 29. From the point of view of operator shop No. 1, VRF No. 1 appears as part of the own network of operator shop No. 1.
- A VRF No. 2, 47.2, connected in the BRAS network for routing traffic only to/from operator shop No. 2, except for certain special cases when traffic can be routed differently.
- A DHCP server 61.1 for operator shop No. 1.
- A DHCP server 61.2 for operator shop No. 2.

[0101] The different steps in accessing an operator shop in the case where the user chooses access to a WLAN virtual AP 65 associated with the local WLAN AP VLAN 45 are summarized below with reference to the signal diagram of Fig. 4b.

1. The WLAN AP 7 is transmitting SSIDs for a plurality of WLAN virtual APs associated with VLANs 41.1, 41.2, 45 connected in the BRAS 17.
2. The terminal 15' transmits a request for "associating" with the WLAN virtual AP 65 for the SSID associated with the local WLAN AP VLAN 45.
3. The selected WLAN virtual AP 65 transmits an association response to the terminal 15'.
4. The terminal 15' proceeds to acquire an IP address, the WLAN AP 7 forwarding frames between the terminal and the local WLAN AP VLAN 45. The IP address is acquired from a DHCP server 62 in the BRAS 17.
5. After the terminal 15' has acquired an IP address, the terminal accesses the service portal 54, via the local VRF 49. If the terminal tries to access some other web server, the terminal may be redirected to the service portal anyway by the HyperText Transfer Protocol (HTTP) redirect function.
6. The service portal 54 transmits information about available operator shops 3.1, 3.2 and their associated SSIDs to the terminal 15' to be read by the user.
7. The terminal 15' disassociates from the WLAN virtual AP 65 for local services, unless the user wanted to only access local services. The user then manually selects a new SSID, this time one that is associated with an available operator shop 3.1, 3.2, and then the same steps are used as described above when the user chooses access to a WLAN virtual AP 63.1, 63.2 associated with an operator shop 3.1, 3.2. Thus, in this case the information obtained at the service portal 54 is used in a very rudimentary way: the user reads the information and uses it for manual SSID selection. There is no automation in this reselection.

[0102] The required modules/components/functions of the WLAN AP 7 are the same as in the first case but the modules/components of the BRAS 17 have to also include a service portal 54 connected in the BRAS network and a DHCP server 62, e.g. associated with the local VRF 49.

Access through a WLAN AP not supporting the virtual AP concept

[0103] If the WLAN AP does not support the virtual AP concept and can only present a single SSID to possible users, the connection process is somewhat similar to the procedure used for access through a CPN 5, as described above. In this case an AN 13' is used that is connected between the WLAN AP 7 and the BRAS 17, see Fig. 2b. Furthermore, the VLANs 41.1, 41.2 and 43 illustrated in Fig. 2a that extend all the way to the WLAN AP, i.e. VLAN No. 1, VLAN No. 2 and the local WLAN AP VLAN, do not have to encompass the link between the AN and the WLAN AP, but instead end in the AN 13' as illustrated in Fig. 2b. No VLAN separation is needed between the WLAN AP 7 and the AN 13'. VLAN separation means that different parts of the traffic are separated from each other using VLAN tagging, but physically the traffic is mixed. Only logically the traffic is treated as belonging to different virtual LANs.

Samsung Ex. 1004, Page 309 of 563

[0104] The WLAN AP 7 is assumed to continuously broadcast an SSID belonging to or representing itself and hence also, basically, for accessing the local service network 51. The terminal 15' receives the SSID and the user selects to attach to the WLAN AP. When the user attaches to the WLAN AP 7, the AAA request resulting from the EAP authentication procedure is routed to the BRAS AAA proxy server 27, that determines from the realm part of the NAI, which should indicate either the realm of operator shop No. 1 or the realm of operator shop No. 2, whether to route the request to the AAA server 31 of operator shop No. 1 or to the AAA server 31 of operator shop No. 2. The AAA client 25 of the WLAN AP includes the MAC address of the terminal 15' in an AAA attribute, e.g. the RADIUS Calling-Station-Id attribute, which is also reused in the Diameter protocol, or a vendor specific attribute, in the AAA request sent to the AAA proxy server 27.

[0105] During, or immediately following, the authentication procedure the AAA server 31 of the respective operator shop 3.1, 3.2 provides one or more session keys, possibly produced as a byproduct of the authentication procedure, to the WLAN AP 7 to be used for the cryptographic protection mechanisms of the proposed standard IEEE 802.11i. The mechanisms of the proposed standard IEEE 802.11i cryptographically ties the MAC address of the terminal 15' that the user is currently using to the authenticated user for this particular session.

[0106] Following a successful user authentication the BRAS 17 instructs the AN 13', e.g. via SNMP or some other protocol that the BRAS 17 can use to control ANs, to associate the user's current MAC address with the service VLAN 41.1, 41.2 of the selected operator shop, e.g. VLAN No. 1 if operator shop No. 1 was selected. Then the terminal 15' can proceed to acquire an IP address using DHCP to enable subsequent IP communication.

[0107] Before associating the user's current MAC address with a VLAN, the AN 13' preferably sends packets received from the WLAN AP 7 with the user's MAC address as the source address to the local WLAN AP VLAN 45 that provides access to the local service network 51, or alternatively, it can discard such packets. The user may have indicated, at the start of the EAP procedure that access only to the local service network is desired by supplying a special NAI, including a realm part belonging to the broadband access network 29, dedicated for this purpose, and the AN 13' could keep sending, or alternatively be instructed to do so, packets received from the WLAN AP 7 with the user's MAC address as the source address to the local WLAN AP VLAN 45. Observe that for access solely to the local service network 51 via the local WLAN AP VLAN no authentication is needed and no IEEE 802.11i protection procedure would be used over the radio interface.

[0108] This procedure only requires a standard behavior of the WLAN AP 7 and can thus be used with available off-the-shelf APs.

[0109] The different steps in accessing an operator shop 3.1, 3.2 in the case where the WLAN AP 7 does not support WLAN virtual APs are summarized below with reference to the signal diagram of Fig. 6a.

1. The WLAN AP 7 is transmitting only its own SSID, denoted "SSID local" in Figs. 2b and 6a.
2. The terminal 15' transmits a request for "associating" with the WLAN AP 7.
3. The WLAN AP 7 transmits an association response to the terminal 15'.
4. The WLAN AP 7 transmits, thereby initiating EAP procedure, from its EAP Authenticator, symbolically indicated as item 67, an EAP-Identity-Request to the terminal 15'.
5. The terminal 15' responds with an EAP-Identity-Response, including the user's identity in the form of an NAI.
6. The EAP Authenticator 67 passes the EAP-Identity-Response to the AAA client function 25 of the WLAN AP 7.
7. The AAA client 25 in the WLAN AP 7 encapsulates the EAP packet with the NAI in an AAA message, including also the MAC address of the terminal 15' in the same AAA message, and sends the AAA message to the AAA proxy server 27 in the BRAS 17.
8. The AAA proxy server 27 looks at the realm part of the NAI and determines to which AAA server the AAA message is to be forwarded, in the example operator shop No. 1, 3.1. The AAA proxy server transmits the AAA request to the AAA server 31 in operator shop No. 1. The AAA proxy server 27 also retrieves the MAC address of the terminal 15' from the AAA message and stores it in the BRAS 17 for future use, such as in a memory associated with the logical function unit 57. This future use is the instructions that will be sent to the AN 7 following a successful authentication.
9. The EAP authentication procedure is executed between the user terminal 15' and the AAA server 31 in the selected operator shop, i.e. the operator shop indicated by the realm part of the NAI, in this example operator shop No. 1, through the AAA proxy server 27 and the AAA client 25 of the WLAN AP 7.
10. After the user has been successfully authenticated the respective AAA server 31 sends an AAA message indicating the successful authentication.
11. This message is received by the AAA proxy server 27 and is relayed to the AAA client 25 in the WLAN AP 7, this being a standard AAA procedure. Thus, both the BRAS 17 and the WLAN AP 7 are aware of the successful authentication. The AAA server 31 also sends, e.g. in the same message as the success indication, one or more keys to the WLAN AP 7 to be used for cryptographic protection of the traffic between the WLAN AP and the terminal 15'.
12. Then the BRAS 17 instructs the AN 7 to associate the MAC address of the terminal 15' with the VLAN 41.1, 41.2 of the selected operator shop, in the example VLAN No. 1, which is associated with operator shop No. 1. Since

Samsung Ex. 1004, Page 310 of 563

the MAC address is cryptographically tied to the authenticated user through the IEEE 802.11i mechanisms, this association is all that is needed and safe against MAC address spoofing. No VMAC address is needed in this case. Since the AAA client 25 in the WLAN AP 7 is used, the BRAS 17 already knows which WLAN AP the terminal 15' is accessing and thus which AN to instruct. The instructing of the AN 13' may be performed by a BRAS internal logical function unit 57 (LU). The information about the MAC address and the selected operator shop, and thus the VLAN to which it is to be associated is obviously available in the BRAS, since this information has been received and forwarded by the AAA proxy server 27. Typically the LU 57 obtains this information from the AAA proxy server 27. The above procedure can be performed in various ways, such as:

a) When the AAA proxy server 27 identifies the selected operator shop, it notifies some other part of the BRAS 17, e.g. the LU 57, of the selection made and which MAC address and which AN it concerns. The LU 57 may receive the operator shop selection information in the form of the realm part of the NAI or some other BRAS internal identifier to which the AAA proxy server 27 has translated the realm part, e.g. a VLAN ID. Then the LU 57 only has to wait for a notification of a successful user authentication before instructing the AN 13' to associate the MAC address that the authenticated user is currently using with the service VLAN, 41.1, 41.2, of the concerned operator shop, 3.1, 3.2, i.e., in this example, associate the MAC address with VLAN No 1, 41.1, associated with operator shop No. 1, 3.1.

b) When the AAA proxy server 27 has received, from the AAA server 31 in the selected operator shop, the AAA message including the indication of a successful user authentication, it informs some other part of the BRAS 17, e.g. the LU 57, about the MAC address of the terminal 15' and the selected operator shop, e.g. in the form of the realm part of the NAI, or some other BRAS internal identifier indicating the selected operator shop. Then, before sending the instructions to the AN 13' the LU 57 may, if needed or desired, translate the realm part of the NAI, or the other BRAS internal identifier respectively, to some BRAS internal identifier, e.g. a VLAN ID.

13. The WLAN AP 7 starts forwarding frames from and to terminal 15'.

14. The AN 13' starts forwarding frames pertaining to the concerned terminal 15'. This means forwarding uplink frames with the MAC address of the terminal as the source address to VLAN No. 1, 41.1, in the example and forwarding downlink frames with the MAC address of the terminal as the destination address from VLAN No. 1 to the WLAN AP 7.

15. After the user has been authenticated, the terminal 15' can proceed to acquire an IP address, in this case an IP address from the address range of operator shop No. 1. This is in the example supplied by a DHCP server 59 for operator shop No. 1, e.g. located in the respective BAS 19. A DHCP server 61.1, 61.2 in the BRAS 17 will act as DHCP relay agent in this procedure. In this case the DHCP server 61.1 acting as DHCP relay agent is associated with the VRF No. 1 for operator shop No. 1. Alternatively, a DHCP server 61.1 in the BRAS can allocate the IP address out of the address range of operator shop No. 1 without involving a DHCP server in operator shop No. 1. In that case the BRAS DHCP server has to have been given a dedicated pool of IP addresses out of the address range of operator shop No. 1.

16. After the terminal 15' has been given an IP address, the user can start traffic using TCP/IP, through VLAN No. 1, 41.1, VRF No. 1, 47.1, and the BAS 19 of operator shop No. 1, 3.1. For example, the user can receive a web page of the BAS of operator shop No. 1. Such a web page can present services that can be accessed through operator shop No. 1.

[0110] The AN 13' may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 6b:

- A VLAN handler 121, including a submodule or unit 123 for receiving instructions of which VLAN to be used for traffic with each connected terminal 15', a unit 125 for changing the MAC-VLAN association list and a unit 127 for tagging frames according to the respective record of said list.
- A MAC address-VLAN association list that may be designed basically as illustrated by Table 1 above but including MAC addresses instead of RG port VLANs and stored in a memory place 129 in a memory 131.

[0111] The BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case:

- A BRAS network including connection to/including the local service network 51.
- A local VRF 49 connected in the BRAS network.
- An AAA proxy server 27 connected in the BRAS network and capable of communicating with the AAA servers 31 in operator shops Nos. 1 and 2.

Samsung Ex. 1004, Page 311 of 563

- A VRF No. 1, 47.1, connected in the BRAS network for routing traffic only to/from operator shop No. 1, except for certain special cases when traffic can be routed differently.
- A VRF No. 2, 47.2, connected in the BRAS network for routing traffic only to/from operator shop No. 2, except for certain special cases when traffic can be routed differently.
- An association instruction unit or logical function unit LU 57 for monitoring the AAA procedure and for instructing ANs 13' to direct frames to a specified VLAN 41.1, 41.2.
- A DHCP server 61.1 for operator shop No. 1.
- A DHCP server 61.2 for operator shop No. 2.

[0112] A procedure in which no AN, such as 13', is used between the BRAS 17 and a WLAN AP 7 that does not support virtual APs is also conceivable, although it may be less preferable. In such a procedure, the BRAS must send its MAC address-VLAN association instructions to the WLAN AP, instead of to the non-existing AN, and the WLAN AP must be capable of associating the user's MAC address with one out of several VLANs, i.e. VLAN No. 1, VLAN No. 2 and the local WLAN AP VLAN. In this procedure the VLANs, VLAN No. 1, VLAN No. 2 and the local WLAN AP VLAN, extend all the way to the WLAN AP 7.

Access through an IPsec tunnel

[0113] A layer 3 procedure, based on IPsec tunnels, can also be used by a user/terminal accessing the broadband access network through e.g. a WLAN AP 7. Such a layer 3 procedure based on an IPsec tunnel between the terminal 15, 15' and a node in the broadband access network 29, as will now be described, can be seen as either a supplement to or a replacement of the layer 2 procedures described above.

[0114] The layer 2 procedures described above cannot be used in those cases where a plurality of users connect through the same general RG port 11, e.g. through a WLAN AP connected to or integrated with the RG 1 or in the case where there is no separate RG port available. In addition, the user may have a router 141 with an NAT 143 connected to the RG 1, so that several devices 15/users can connect to the NAT using the same IP address allocated from the local network 5, see Fig. 2c. Such a home based NAT, which is quite common, makes a layer 2 solution even less feasible. A home based WLAN AP and a router including an NAT may also be integrated in a single device. Thus, in these cases a layer 3 procedure is required. However, the layer 3 access procedure as described herein is a general solution that can be used in all cases, whether the user connects through a CPN 5 or a public WLAN AP 7.

[0115] In a basic case it can be assumed that a roaming user connects through an RG port such as 11. This is a case where a layer 3 solution is needed: the user visits a friend, hence she/he is roaming, the friend's CPN 5 being connected to a broadband access network 29 that is connected to the user's home operator shop 3.1 or 3.2. Hence this is a case where the user is accessing his "home broadband access network". It is assumed that there is no separate RG port available for the roaming user through which the user can connect using a layer 2 procedure. Instead the roaming user uses an RG port 11 which is already being used by her/his friend and which thus already is associated with a service VLAN 41.1, 41.2, i.e. VLAN No. 1 or VLAN No. 2. Since all traffic via this RG port will pass through the associated service VLAN, due to the VLAN association in the AN 13, the user/terminal 15 will have to establish the IPsec tunnel through this service VLAN, even though the IPsec tunnel may be used to associate the user/terminal with another operator shop, i.e. the roaming user's home operator shop, instead of that associated with the traversed service VLAN.

[0116] However, the user does not have to be roaming to use the IPsec tunnel procedure for establishing an IPsec tunnel through one of the service VLANs. Another case is for instance a user having subscriptions with two different operator shops, e.g. operator shops Nos. 1 and 2, 3.1 and 3.2, connected to the same broadband access network 29. In that case the user may have used a layer 2 procedure as described above to associate an RG port 11 with the service VLAN 41.1 of one of the operator shops, e.g. operator shop No. 1, and then the user decides that he also wants to access some service in another operator shop, e.g. operator shop No. 2. The user may then use the layer 3 procedure and establish an IPsec tunnel via the service VLAN 41.1 in order to access operator shop No. 2. However, this case is quite demanding for the operating system of the terminal 15, and possibly also for the applications running on the terminal, since the operating system has to be capable of handling multiple IP addresses and the applications may have to deal with source address selection.

[0117] It is also possible to establish the IPsec tunnel via an RG port 11 that is associated with the local default VLAN 43, or via a public WLAN AP 7 and one of the service VLANs 41.1, 41.2, or via a public WLAN AP 7 and the local WLAN AP VLAN 45, but the case where the IPsec tunnel is established via one of the service VLANs 41.1, 41.2 may be of greater interest, even though the mechanisms are the same or at least quite similar to each other.

[0118] In the basic case mentioned above the user is accessing the broadband access network 29 through another user's CPN 5, and hence the user is roaming. This should be distinguished from the case involving roaming to a foreign broadband access network, i.e. to a broadband access network that has no connection to the user's home operator shop, the latter case described in particular sections below.

Samsung Ex. 1004, Page 312 of 563

[0119] Thus, all the cases that will now be discussed deal with a user accessing his "home broadband access network", this defined here as a broadband access network 29 that has a connection to the user's home operator shop (3.1, 3.2). Hence, a roaming user is assumed to connect through an RG port 11 which is already associated with an authenticated connection towards one of the operator shops 3.1, 3.2, i.e. from the user terminal 15 an IPsec tunnel is in the connection operation being established through the RG port through one of the service VLANs, i.e. VLAN No. 1 or VLAN No. 2. As has already been mentioned, it is also possible to establish the IPsec tunnel through an RG port that is associated with the local default VLAN 43, or via a public WLAN AP 7 and a service VLAN or the local WLAN AP VLAN 45. When the IPsec tunnel has been established through the local default VLAN 43, it passes an RG 11, an AN 13, the local default VLAN 43 and the local VRF 49. When the IPsec tunnel has been established through a public WLAN AP 7 and a service VLAN 41.1, 41.2, it passes a WLAN AP, possibly an AN 13', depending on whether an AN is used for the WLAN AP case, a service VLAN and the VRF 47.1, 47.2 associated with the respective service VLAN. When the IPsec tunnel has been established through a public WLAN AP 7 and the local WLAN AP VLAN 45, it passes a WLAN AP, possibly an AN 13', depending on whether an AN is used for the WLAN AP case, the local WLAN AP VLAN and the local VRF 49. The end points of the IPsec tunnel may be the same in all these cases, i.e. in the local VRF 49, or possibly in a dedicated tunnel endpoint/termination device 145, in a dedicated VRF 47.1 or 47.2, or in the BAS 19 of an operator shop 3.1, 3.2, as will be discussed hereinafter.

[0120] The most straightforward layer 3 procedure is that the IPsec tunnel is established between the terminal 15, 15' and the BAS 19 in the concerned operator shop 3.1, 3.2. This procedure is one of the alternatives that will be described hereinafter, but it suffers from a number of deficiencies.

[0121] In a first case the IPsec tunnel 147' to the BAS 19 of an operator shop is established via another operator shop. For the access cases of Figs. 2a and 2c the IPsec tunnel can e.g. extend from the terminal 15 via the RG 1, the AN 13, the VRF No. 1 and the operator shop No. 1 and then across the Internet 149 to the BAS 19 of operator shop No. 2, see Fig. 2e. However, this procedure is suboptimal, both from charging and routing points of view, since the packets of the IPsec tunnel are not given any special treatment. These packets, just like any packets sent through an RG port 11 associated with operator shop No. 1, are forwarded by VRF No. 1 to operator shop No. 1 and then find their way to the BAS 19 of operator shop No. 2 across the Internet 149. Thus, the "another operator shop", via which the IPsec tunnel 147' is undesirably established, is the operator shop with which the concerned RG port is currently associated.

[0122] In a second case the IPsec tunnel 147" is extracted and routed internally in the broadband access network 29 up to the BAS 19 of the desired operator shop, see Fig. 2f, this avoiding the drawbacks of the first case. This means that the packets that are used to establish the IPsec tunnel and the packets constituting the IPsec tunnel 147" are specially treated, so that these packets are not routed through the operator shop associated with the respective VRF, in the example VRF 47.1, i.e. not through operator shop No. 1 in the above example, but instead find their way to the destination BAS 19, i.e. the BAS of operator shop No. 2 in the above example, through the BRAS 17 and the VRF dedicated for the destination operator shop, VRF No. 2, 47.2, in the above example. In practice, and in this example, this means that VRF No. 1 must have an entry in its routing table, such as a table stored at a memory place 150, see Fig. 2f, for each IP address - there may be one or multiple IP addresses for each BAS 19 - that is used for IPsec tunnel endpoints in the BAS of operator shop No. 2. The IP addresses that are used in the BAS as possible IPsec tunnel endpoint addresses are obviously included in the address range of the considered operator shop, operator shop No. 2 in the example. Such routing table entries should point towards VRF No. 2. The result is that VRF No. 1 will send packets addressed to a "tunnel endpoint address" indicating or pointing to the BAS 19 of operator shop No. 2 to VRF No. 2 instead of sending them to operator shop No. 1, this procedure executed by the routing unit/IP address handler 150', searching, for the IP address of each received packet, the matching entries in the routing table stored in memory place 150, this table having address entries such that packets destined to these addresses are routed to the respective dedicated VRF 47.1, 47.2. A routing table entry for a single IP address can also be called a "host route".

[0123] The table below is a general example of a routing table. Although the exact implementation and representation of a routing table can vary between different systems, in general the properties of the routing table may adhere to this example.

Destination	Netmask	Next hop	Interface
192.68.8.0	255.255.255.0	192.68.12.2	192.68.12.1
192.68.6.0	255.255.255.0	0.0.0.0	192.68.6.1
192.68.3.4	*255.255.255.255*	*192.68.12.3*	*192.68.12.1*
192.68.3.0	255.255.255.0	192.68.6.2	192.68.6.1
192.68.2.0	255.255.255.0	192.68.6.2	192.68.6.1

(continued)

Destination	Netmask	Next hop	Interface
192.68.1.27	*255.255.255.255*	*192.68.12.2*	*192.68.12.1*
192.68.1.0	255.255.255.0	192.68.4.1	192.68.4.2
192.44.0.0	255.255.0.0	192.68.4.1	192.68.4.2
:	:	:	:
:	:	:	:
0.0.0.0	0.0.0.0	192.68.6.2	192.68.6.1

[0124] Each row in the table represents a table entry. The contents in fields "Destination" and "Netmask" of an entry together define which addresses that match the entry. The netmask specifies how many of the bits of the destination that are valid and should be used when matching addresses for routing. A netmask of 255.255.255.0 means that the 24 first bits of the destination field are valid, because each number of the netmask represents 8 bits.

[0125] The field "Next hop" of an entry holds the IP address of the next hop router to which packets with destination addresses matching the entry should be forwarded. If the next hop field is 0.0.0.0, this indicates that the destination is located on one of the networks directly attached to the router itself, i.e. a packet matching the entry does not have to be forwarded to another or next hop router, since its destination is located on a network attached directly to the router itself to which the routing table is attached.

[0126] The field "Interface" of an entry indicates on which of the own interfaces of the router the packet is to be forwarded. The address indicated in the field "Interface" is the IP address assigned to the concerned interface.

[0127] A host route is an entry, for which the netmask is set to 255.255.255.255, i.e. all the 32 bits of the destination field are valid, indicated by italics in the table. This means that only a single address will match the entry, e.g. addresses 192.68.3.4 and 192.68.1.27 respectively for the two host route examples in the table.

[0128] When searching for an entry that matches a packet to be forwarded, the router compares the destination address of the packet with the entries in the table. Specifically, when comparing the destination address of the packet with an entry, the router compares the destination address with the destination field of the entry, but in this comparison it uses only the number of bits specified by the content of the field "Netmask" of the entry. That is, if the content of the field "Netmask", for example, is 255.255.255.0, the router compares the 24 first bits of the destination address to the 24 first bits of the content of field "Destination" of the entry, whereas if content of the field "Netmask" is 255.255.255.255, the router compares the complete destination address (32 bits) to the full 32 bits of the content of field "Destination" of the entry. The principle that the router uses for searching the table is a so-called "longest-match-first" principle. This means that if more than one entry matches the destination address of a packet, the router will choose the entry that has the largest number of matching bits, i.e. the one of the matching entries that has a content of the field "Netmask" that indicates the largest number of bits. As an example, a packet having a destination address 192.68.3.4 would match both the third and the fourth entry in the example of a routing table above. The router would then choose the third entry, because that entry matches 32, i.e. all, of the bits of the destination address, whereas the fourth entry only matches 24 bits of the destination address.

[0129] The entry at the end of the table, for which both the contents of the fields "Destination" and "Netmask" are set to 0.0.0.0, represents the default route. This is the route that is used for all packets that do not match any other entry in the table.

[0130] A routing table may contain more fields for each entry than the fields included in the example above. Such additional entries may further characterize the routes. It is for example common to have a metric field, indicating a "cost" for the route, e.g. in terms of the number of hops to the destination. The metric field may be used when choosing between alternative routes to the same destination.

[0131] The term "routing it internally" used above means in particular that the packets of the IPsec tunnel 147", as well as the packets that are used in establishing the IPsec tunnel, are routed in the BRAS 17, as described above from one VRF, VRF 47.1 in the example, through the BRAS to another VRF, VRF 47.2 in the example, and then further to the BAS 19 of the operator shop that is the endpoint of the IPsec tunnel.

[0132] However, if operator shops 3.1, 3.2 connected to the same broadband access network 29 use overlapping address spaces, which is a case that must be supported, e.g. address spaces including private addresses, the procedure according to the second case does not work, unless the endpoints of the IPsec tunnels at the operator shop are globally unique addresses, i.e. not included in or taken from any overlapping address range. A private IP address is an address from a dedicated range of addresses, assigned by the IANA (Internet Assigned Numbers Authority) that can be used in networks that are "address-wise" isolated from the global Internet. These addresses can be reused in different networks

Samsung Ex. 1004, Page 314 of 563

and are not globally unique. When connecting a network that uses private IP addresses to the global Internet, the gateway between the private network and the Internet has to be or has to include an NAT, cf. Fig. 2c. The basic operation of an NAT is to dynamically associate, i.e. "translate", a pair consisting of a private IP address and a TCP or UDP port on the private network side with a global IP address and a TCP or UDP port on the Internet side. These associations are dynamically established, and also deleted, on a per TCP/UDP connection basis. In this way multiple devices, using private IP addresses, can share a single globally unique IP address in the NAT. However, all applications cannot work across NATs.

[0133] Generally, methods in which the IPsec tunnel is established between the terminal 15, 15' and the BAS 19 in the concerned operator shop 3.1, 3.2 make informing the user/terminal 15 about the address of the remote endpoint of the IPsec tunnel more difficult than in those cases where the remote IPsec tunnel endpoint is located in the BRAS 17, because:

- There is a different remote endpoint used for each operator shop 3.1, 3.2 connected to the broadband access network 29. However, this can be handled using methods described below.
- The address of the remote endpoint is administered by an organization different from that of the broadband access network 29.

[0134] Another disadvantage of having the IPsec tunnel endpoint in the BAS 19 is that the AAA entities of the broadband access network 29, i.e. the AAA client 23 and the AAA proxy server 27 in the BRAS 17, are not involved in the AAA procedures, which may create issues associated with accounting.

[0135] The above disadvantages imply that it in some cases may be preferable to confine layer 3 access procedures to the broadband access network 29.

[0136] Locating the remote endpoint of the IPsec tunnel in the BRAS 17 is a way of confining the layer 3 access procedure to the broadband access network 29. It is still, however, possible to provide a different remote endpoint for each operator shop 3.1, 3.2 or a single common remote endpoint for all operator shops. The former alternative, i.e. having different remote endpoints of the IPsec tunnels, provides a simpler mechanism for selection of the desired operator shop, but it makes informing the user or terminal 15, 15' about endpoint addresses more complicated. The latter alternative, i.e. having a common remote endpoint, has the advantage that the same address for the remote endpoint of the IPsec tunnels can be used for all operator shops 3.1, 3.2, but, as a consequence, the selection mechanism becomes more complex, at least in the case when a foreign broadband access network is accessed, in which case this layer 3 solution is more or less reused as will be described below, because the selection mechanism cannot base its selection on or directly derive it from the remote endpoint of the IPsec tunnel.

[0137] Thus, these different variants of accessing methods using layer 3 have their respective advantages and disadvantages. They will now be described in detail.

Access through an IPsec tunnel to a common tunnel endpoint in the BRAS

[0138] In this procedure the single common remote endpoint of the IPsec tunnel 147 is located in the BRAS 17 and may belong to the local VRF 49, see Fig. 2d, and the address, the IP address, of the remote endpoint thus points to the local VRF. However, it should be pointed out that even though the description below uses the local VRF as the common remote endpoint, a dedicated tunnel endpoint device, e.g. an IPsec tunnel endpoint server 145 in the BRAS, may be used instead of the local VRF. Such a dedicated endpoint server would then also be connected in a BRAS internal network such as an inter-VRF network 52 and/or in the local service network 51, see Fig. 2g.

[0139] Methods for informing about the address of the remote tunnel endpoint will be described below, these methods also being applicable in the other cases in which IPsec tunnels are established and used.

[0140] As discussed above, in the basic case it is assumed that a roaming user connects through an RG port 11 which is already associated with an authenticated connection towards one of the operator shops 3.1, 3.2, e.g. operator shop No. 1. Before being capable of establishing an IPsec tunnel, the terminal 15 must acquire an IP address. Hence, an IP address out of the address range of operator shop No. 1 is acquired from the DHCP server 61.1 associated with VRF No. 1 in a previously described manner. Then the IPsec tunnel is established from the terminal 15 to the local VRF 49 via one of the dedicated VRFs 47.1, 47.2, e.g. VRF No. 1, assuming that the RG port through which the IPsec connection is being established is currently associated with the dedicated VRF No. 1, see the dotted line 147 in Fig. 2d, using also some BRAS internal network for the communication between the dedicated VRF and the local VRF as will be described below. The two endpoint devices execute the IKEv2 procedure that is used to establish the IPsec tunnel, i.e. the terminal 15 and the local VRF 49 execute the IKEv2 procedure in this case. The IKEv2 messages are routed via another VRF, the dedicated VRF 47.1 in this example.

[0141] The local VRF 49 has an IP address from the address range of the broadband access network 29 and this indicates to VRF No. 1 that the packets should be routed to the local service network 51, or at least to some BRAS-

Samsung Ex. 1004, Page 315 of 563

internal network such as the inter-VRF network 52, instead of being forwarded to operator shop No. 1. This is obvious from the IP routing table in VRF No. 1. In another case, the RG port 11 through which the user is connecting may be currently associated with the local default VLAN 43 and the local VRF, through the RG port VLAN 55 and the AN 13, and then the IPsec tunnel 147 will not traverse any of the other VRFs, but this case is of less interest.

[0142] The IPsec tunnel 147 is established using IKEv2 (Internet Key Exchange protocol version 2) with the NAT traversal detection option and with EAP as an integrated authentication mechanism. When the terminal 15 provides the user's regular NAI during the EAP authentication procedure, the local VRF 49 examines the realm part of the NAI and identifies the home operator shop of the user, e.g. operator shop No. 2. The local VRF forwards the EAP packets to and from the AAA client 23 in the BRAS 17 and the AAA client communicates with the AAA server 31 of operator shop No. 2 via the AAA proxy server 27.

[0143] After a successful authentication the IPsec tunnel establishment proceeds and concludes and the local VRF 49 associates the established tunnel interface with the route to VRF No. 2, 47.2. In the local VRF some data structure is used internally to associate a tunnel interface with a routing table entry, or some other internal mechanism, not involving a routing table. The data structure or mechanism can involve/use pointers, tables or similar arrangements/mechanisms. Then the local VRF 49, assisted by a DHCP server 62 in the BRAS 17, assigns an "inner" IP address, taken from the address range of operator shop No. 2, to the terminal 15 to be used for packets sent inside the IPsec tunnel 147, using the method described in B. Patel, B. Aboba, S. Kelly, V. Gupta, "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode", RFC 3456, January 2003. It is possible to implement the DHCP server 62 associated with the local VRF and the DHCP servers 61.1, 61.2 associated with VRF No. 1 and VRF No. 2 as a single entity or unit in the BRAS 17, but they may also be implemented as separate entities or units. In the latter case the DHCP server 62 associated with the local VRF 49 acts as a DHCP relay agent between the terminal 15 and the DHCP server 61.1 associated with VRF No. 1, which in turn may act as a DHCP relay agent towards a DHCP server 59 in operator shop No. 1. Alternatively, the DHCP server 62 associated with the local VRF may be given a pool of addresses out of the address range of operator shop No. 1, and possibly a similar pool of addresses from the address range of operator shop No. 2, to be used for users accessing the respective operator shop via an IPsec tunnel to the common tunnel endpoint in the BRAS. Another alternative for the inner IP address assignment is that the local VRF 49 assigns the inner IP address to the terminal 15 using a Configuration payload in one of the IKEv2 messages during the IPsec tunnel establishment, in which case no subsequent interaction between the terminal and a DHCP server is needed. Subsequently, all packets arriving to the local VRF through the IPsec tunnel will be routed to the dedicated VRF No. 2, and then optionally packets addressed to nodes in the BRAS internal network and the local service network 51 may be excluded, i.e. they may instead be routed directly from the local VRF 49 to their destination.

[0144] The VRF No. 2 and the local VRF 49 must each also establish a host route for the assigned inner address, so that packets arriving from operator shop No. 2 destined for the concerned terminal 15 are routed to the local VRF and therefrom to the remote endpoint of the IPsec tunnel. A "host route" is a route, or rather a routing table entry, for a single IP address as has been indicated above. For VRF No. 2, 41.2, an alternative to the host route is possible. The inner IP address assigned to the terminal 15 may be selected out of a special pool of addresses in the address range of operator shop No. 2, 3.2, this special pool of addresses being used only for terminals accessing operator shop No. 2 via the common IPsec tunnel endpoint in the BRAS 17. For this alternative, the VRF No. 2 can have a static configuration indicating that any packet with an IP address out of this special pool as its destination address should be forwarded to the common tunnel endpoint in the BRAS, e.g. the local VRF 49.

[0145] The IPsec tunnel 147 may also be established via the local default VLAN 43 as mentioned above, or via a public WLAN AP 7 and a service VLAN 41.1, 41.2, i.e. one of VLAN No. 1 and VLAN No. 2, or the local WLAN AP VLAN 45. If the IPsec tunnel is established via the local default VLAN or the local WLAN AP VLAN, it will not traverse any of the VRFs that are associated with operator shops.

[0146] To enable the terminal 15, 15' to establish the IPsec tunnel, it must be informed about the address of the remote endpoint of the IPsec tunnel that it is to use. This can be announced on the service portal 54, either as an FQDN or as an explicit IP address. The operating system of the terminal must have an IKEv2/IPsec protocol stack and some additional software to initiate the IKEv2 procedure, manually or from an application.

[0147] Another attractive possibility is to use a DHCP option that indicates the tunnel endpoint either as an FQDN (Fully Qualified Domain Name) or as an explicit IP address, which is possible since it is an address from the address range of the broadband access network 29, this requiring some changes in the DHCP servers 61.1, 61.2, 62 of the broadband access network 29 and the terminal 15, 15'. Then each DHCP server 61.1, 61.2, 62 of the broadband access network is arranged to include this DHCP option, including information on the tunnel endpoint, in a DHCP message, e.g. a DHCPOFFER and/or a DHCPACK message, towards the terminal, even if the DHCP server 61.1, 61.2, 62 is acting as a relay agent between the terminal and another DHCP server, e.g. a DHCP server 59 in an operator shop 3.1, 3.2.

[0148] In particular, such a DHCP option may be used in conjunction with a home NAT 143, see Fig. 2c and particularly Fig. 2h, and then the NAT is itself first configured via DHCP and then the NAT in turn configures the connecting terminals 15, 15', including the special DHCP option. The DHCP method of informing the terminals allows the mechanism, including

Samsung Ex. 1004, Page 316 of 563

informing the terminals and the subsequent establishing of tunnels, and even the user authentication depending on the authentication method, to be automated and handled by software in the terminal without user intervention. The necessary changes of the DHCP software used in the DHCP server and the terminal are obvious and can be easily implemented by a person skilled in the art using the corresponding RFCs describing the use of options in general in the DHCP protocol. Also the DHCP software in the NAT 143, or in the router 141 containing the NAT function, including both the DHCP client and the DHCP server functionality, can be modified to achieve the desired behavior by a person skilled in the art.

[0149] Such a special DHCP option can have the following format for the case where only a single endpoint address is required for all terminals such as when using a common endpoint, each small rectangle denoting a single bit octet:

Option code	Option length	IP-address

The format for the case where a plurality of endpoint addresses are used can be:

Option code	Option length	IP-address No. 1	IP-address No. 2	
		IP-address No. n		

The format for the case where an FQDN for single endpoint address is used can be:

Option code	Option length	FQDN

The format for the case where multiple FQDNs are used can be:

Option code	Option length	FQDN No. 1 length	FQDN No. 1	FQDN No. 2 length	FQDN No. 2	
		FQDN No. n length	FQDN No. n			

In the same option also there may be a mixing of IP addresses and FQDNs and then the format may be:

Option code	Option length	List item No. 1 type	List item No. 1 length	IP-addr./ FQDN No. 1	List item No. 2 type	List item No. 2 length	IP-addr./ FQDN No. 2	
		List item No. n type	List item No. n length	IP-addr./ FQDN No. n				

The list item length field may not be needed, when the preceding list item type field indicates an IP address, since IP addresses have a fixed length. This format allows inclusion of both IPv4 addresses and IPv6 addresses in the list, indicated by different list item types. It is also conceivable to make the list consist of only IPv6 and/or IPv4 addresses, but no FQDNs, in which case the list item type field is needed to indicate the type of address, but no list item length fields are needed.

[0150] The above examples of special DHCP option formats can be reused for DHCPv6, with the difference that the option-code and option-length fields are two octets each instead of one octet each. In addition, the IP addresses handled

Samsung Ex. 1004, Page 317 of 563

by DHCPv6 are 16-octet IPv6 addresses instead of 4-octet IPv4 addresses. It is also conceivable that a DHCPv6 option contains one or more IPv4 address(es) or mixes of IPv6 and IPv4 addresses, as described above.

[0151] A home NAT 143, see Fig. 2h, that uses an MAC address access control list, i.e. a list of allowed MAC addresses, may optionally use this DHCP option for additional features. It may for instance choose to use the DHCP option in messages sent only to terminals 15 having MAC addresses that are not on the list of allowed MAC addresses. Then it could apply packet filtering such that packets from these terminals are discarded unless they are sent to the address provided in the new DHCP option, i.e. the common tunnel endpoint address.

[0152] A third possible method of informing the terminal 15, 15' is to convey the information about the tunnel endpoint via off-line means. For example, each household connected to a broadband access network 29 can receive a letter from the operator of the broadband access network 29 containing general information e.g. about the broadband access network, the connected operator shops 3.1, 3.2, the available free services in the local service network 51, how to connect the equipment at home, etc. Such information could include FQDNs or IP addresses to be used for IPsec tunnel endpoints, in the case where the respective procedures are used.

[0153] The different steps in accessing an operator shop 3.1, 3.2 using an IPsec tunnel ending in a common endpoint in the BRAS 17 are summarized below, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7a.

1. A roaming user connects his terminal 15 to an RG port 11 having an already established connection with operator shop No. 1
2. The terminal 15 acquires an IP address out of the address range of operator shop No. 1, by interacting with the DHCP server 61.1 associated with VRF No. 1.
3. The user of the terminal 15, or the terminal 15 itself, receives or obtains the address of the common tunnel endpoint, such as by first obtaining a web page from the service portal 54, using a WWW browser running in the terminal and a suitable, known web address, such as "http://my-broadband-access-network-services.com", and then finding the address of the common tunnel endpoint in the displayed web page.
4. The user starts special software in the terminal 15 for starting the establishing of the IPsec tunnel. The different tasks of this software include running IKEv2 and thus establishing the security associations (SAs) for the IPsec tunnel.
5. The special software creates a message addressed to the received or obtained address for establishing an IPsec tunnel having the received or obtained address as its remote endpoint and sends the message through the connected RG port 11, in RG port VLAN 55 and in VLAN No. 1. The AN 13 only looks at the MAC address. If there is a home NAT 143 between RG port 11 and the terminal 15, the home NAT 143 examines the destination IP address of the message and forwards the message to VRF No. 1 via RG port VLAN 55 and VLAN No. 1, 41.1.
6. The VRF No. 1, 47.1, examines the address of the message and finds that the address of the message corresponds to or is an IP address that is included in the address range of the broadband access network 29 and forwards the message to the common IPsec tunnel endpoint in the BRAS 17, e.g. the local VRF 49, in the inter-VRF network 52 or the BRAS internal network.
7. The common tunnel endpoint in the BRAS 17, e.g. the local VRF 49, receives the message. The endpoint recognizes the IP address as belonging to it, starts to establish the IPsec tunnel and first uses EAP for authentication and accordingly messages start to be sent between the common tunnel endpoint and the terminal 15, the EAP Authenticator in the common tunnel endpoint (local VRF 49) sending first an EAP-Identity-Request to the terminal 15.
8. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of a regular NAI.
9. The EAP Authenticator passes the EAP-Identity-Response to the AAA client function 23 in the BRAS 17.
10. The AAA client 23 includes the EAP-Identity-Response in an AAA message and sends the AAA message to the AAA proxy server 27.
11. The AAA proxy server 27 recognizes that operator shop No. 2 is wanted by examining the realm part of the NAI. The AAA proxy server 27 transmits the AAA request to the AAA server 31 in operator shop No. 2.
12. An EAP authentication procedure between the AAA server 31 in operator shop No. 2 and the user terminal 15 through the AAA proxy server 27 and the AAA client 23 of the BRAS 17 is performed. The EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31 of operator shop No. 2. Between the AAA client 23 of the BRAS 17 and the AAA server 31 the EAP packets are encapsulated in AAA messages.
13. After successful authentication, the very procedure for establishing the IPsec tunnel is executed, the common tunnel endpoint, e.g. the local VRF, associates the established tunnel interface with the route, in the BRAS 17, to VRF No. 2.
14. The terminal 15 interacts with the DHCP server 62 associated with the local VRF to obtain an IP address to be used for packets inside the IPsec tunnel, also called an "inner IP address". As described previously, the DHCP server 62 associated with the local VRF either acts as a DHCP relay agent between the terminal 15 and the DHCP server 61.2 associated with VRF No. 2, which in turn may act as a DHCP relay agent towards a DHCP server 59

Samsung Ex. 1004, Page 318 of 563

in operator shop No. 2, 3.2, or assigns the IP address out of a pool of addresses from the address range of operator shop No. 2. It is also possible for the common tunnel endpoint, e.g. the local VRF, to assign the inner IP address to the terminal using the Configuration payload in IKEv2.

15. The inner IP address is also obtained or received by the VRF No. 2, that enters it in a table telling that packets with this IP address are to be forwarded to the common tunnel endpoint. Alternatively, the inner IP address is selected out of a special pool of addresses in the address range of operator shop No. 2, this special pool of addresses being used only for terminals accessing operator shop No. 2 via the common IPsec tunnel endpoint in the BRAS. Using this alternative procedure, the VRF No. 2, 47.1, can have a static configuration indicating that any packet with an IP address out of this special pool as its destination address should be forwarded to the common tunnel endpoint in the BRAS.

16. The IP address is also obtained or received by the common tunnel endpoint, the common tunnel endpoint enters in a table that packets with this IP address as destination address are to be forwarded into the established IPsec tunnel.

17. The user can start traffic using TCP/IP, through the IPsec tunnel 147, the common tunnel endpoint, VRF No. 2, and the BAS 19 of operator shop No. 2. For example, the user can receive a web page from the BAS. Such a web page can present available services.

[0154] Steps to be performed by the special software in the terminal 15:

1. Obtain the address of the common tunnel endpoint 49; 145.
2. Transmit into the connected network a message including the address of the common tunnel endpoint for establishing an IPsec tunnel.

[0155] Steps to be performed by the common tunnel endpoint 49; 145:

1. After receiving a request of establishing an IPsec tunnel, start an EAP authentication procedure by activating EAP Authenticator 56.

2. Receive from the EAP Authenticator 56 information about the wanted operator shop, such as by receiving the user's regular NAI obtained from the terminal 15 in the EAP authentication procedure and evaluating the realm part thereof. The EAP Authenticator can be considered a part of, or associated with, the local VRF 49 or the common tunnel endpoint server 145. In that case the information is inherently available, since the terminal supplies the NAI in the EAP-Identity-Response packet. Also the NAI analysis functionality may be used that is anyway present in the AAA proxy server 27 and the AAA proxy server may then pass the result of the analysis, in terms of which operator shop the message concerns, to the local VRF or the common tunnel endpoint server 145. Other ways may be chosen, since passing data back and forth between BRAS internal entities and, if the EAP Authenticator is regarded as a separate module in the BRAS 17, it is simply a matter of implementation and can be done in a multitude of ways obvious to one skilled in the art, depending on the preferences of the designer of the BRAS.

3. After receiving information that EAP authentication has been successfully completed, establish the IPsec tunnel to the terminal 15, creating an IPsec tunnel interface for the terminal, where such an interface is software based and can be considered a "virtual interface". Sending and receiving packets to and from the created IPsec tunnel interface includes that appropriate IPsec procedures are invoked.

4. Associate the created IPsec tunnel interface with the dedicated VRF 47.1, 47.2 of the wanted operator shop.

5. Receive the IP address assigned to the terminal 15 from the DHCP server 62, 61.1, 61.2. Optionally send the IP address to the terminal in a Configuration payload in an IKEv2 packet during the IPsec tunnel establishment procedure, in which case the common tunnel endpoint may select the IP address itself out of a dedicated pool of addresses instead of receiving it from the DHCP server.

6. After receiving or selecting the IP address, associate it with the created IPsec tunnel interface.

7. When receiving packets on the IPsec tunnel interface, route them to the VRF 47.1, 47.2 of wanted operator shop.

8. When receiving packets from VRFs 47.1, 47.2, compare their destination IP addresses to IP addresses associated with existing IPsec interfaces, and send into the respective IPsec tunnel if agreement.

9. In the case where host routes are used in the VRFs 47.1, 47.2 for routing packets to the common tunnel endpoint, inform, after having removed an IPsec tunnel and the IPsec tunnel interface thereof, the VRF associated with the IPsec tunnel interface, that routing to the assigned IP address should be stopped or closed.

[0156] If the inner IP address assigned to the terminal 15 is selected out of a dedicated pool of IP addresses that is used only for terminals accessing the operator shop via IPsec tunnels to the common tunnel endpoint, then the VRF of the selected operator shop, VRF 47.1, 47.2, does not have to perform any particular steps, except its regular IP routing, in order to support this procedure. Otherwise, the following are the additional steps to be performed by the dedicated VRF 47.1, 47.2 of the wanted operator shop:

Samsung Ex. 1004, Page 319 of 563

1. After receiving the IP address from the DHCP server 62, 61.1, 61.2, modify the routing table by entering the IP address as a new entry in the table, thus creating a host route associated with the IP address, indicating that packets with the received IP address as its destination address should be forwarded to the common tunnel endpoint, e.g. the local virtual router function 49.
2. After receiving information on stopped routing for the concerned IP address, remove the respective entry from the routing table.

[0157] The terminal 15 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 7c:

- A unit 151, typically including a suitable processor and suitable software, stored in some memory, for executing special procedures including

  -- a unit 153 for executing a procedure for obtaining or receiving addresses of common tunnel endpoints to be used for establishing IPsec tunnels and/or for storing them, if required.
  -- a unit 155 for executing a procedure for transmitting a request for establishing an IPsec tunnel.

- A memory 175 including

  -- a memory place 159 for storing special software including places 153' for the procedure for obtaining or receiving addresses and 155' for the procedure of transmitting an IPsec tunnel request, and
  -- a memory place/memory places 161 for storing addresses of common tunnel endpoints.

[0158] The BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case:

- A BRAS network, also called the BRAS internal network, including a connection to/including the local service network 51 and/or the inter-VRF network 52.
- A local VRF 49 connected in the BRAS network.
- An AAA client 23.
- An authenticator unit 56.
- An AAA proxy server 27 connected in the BRAS network and to AAA servers 31 in operator shops Nos. 1 and 2.
- A VRF No. 1, 47.1, connected in the BRAS network for routing traffic only to/from operator shop No. 1, except for certain special cases when traffic can be routed differently.
- A VRF No. 2, 47.2, connected in the BRAS network for routing traffic only to/from operator shop No. 2, except for certain special cases when traffic can be routed differently.
- A DHCP server 62 associated with the local VRF 49.
- A DHCP server 61.1 associated with VRF No. 1, 47.1.
- A DHCP server 61.2 associated with VRF No. 2, 47.2.
- Optionally a service portal 54.
- Optionally a dedicated IPsec tunnel server 145, optionally also having DHCP server functionality.

[0159] The local VRF 49 of the BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 7d:

- An AAA client 27 that may only be connected to the local VRF.
- An authenticator function 56 that may be a component of or connected to the local VRF.
- An IPsec tunnel handler 173 including

  -- a unit 175 for initiating authentication,
  -- a unit 177 for establishing IPsec tunnels and creating corresponding tunnel interfaces, and
  -- a unit 179, possibly integrated with the unit 177, for removing IPsec tunnels and corresponding tunnel interfaces.

- A unit 181 for finding the wanted operator shop as a consequence of having received a request for establishing an IPsec tunnel. This unit may evaluate the realm part of the user's regular NAI received in the EAP authentication procedure.
- A unit 183 for associating created tunnel interfaces with wanted operator shops 3.1, 3.2 connected to the broadband

Samsung Ex. 1004, Page 320 of 563

access network 29, such as by storing corresponding entries.

- A DHCP server 62 that may be a component of or connected to the local VRF 49.
- An optional unit 185 for sending requests for IP addresses to the DHCP server 62.
- A unit 187 for associating IP addresses with respective IPsec tunnel interfaces.
- A comparator 189 for comparing IP addresses of packets received in BRAS internal network.
- A unit 191 for forwarding packets to a selected IPsec tunnel interface and tunnel after having received required information from the comparator 189.
- A unit 193 for routing packets from IPsec tunnels to respective VRFs, information about the correct VRFs taken from an association table.
- A unit 195 for sending information about IP addresses that no longer require special routing to the respective VRFs, this unit provided only if dynamically established host routes are used in the dedicated VRFs 47.1, 47.2.
- A memory 197 including

  -- a memory place 199 for a table, which may be a part of the routing table, listing associations between IPsec tunnels/tunnel interfaces and dedicated VRFs 47.1, 47.2, and
  -- a memory place 201 for a table, which may be a part of the routing table, listing associations between IP addresses and IPsec tunnel interfaces.

[0160] If a dedicated IPsec tunnel endpoint server 145 is used, it may require most of the same or corresponding components.

[0161] The dedicated VRFs 47.1, 47.2 of the BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case, see Fig. 7e:

- A VLAN handler 171.
- A unit 203 for handling IP addresses requiring special routing including

  -- a unit 205 for identifying received IP addresses as requiring special routing and entering such IP addresses in a routing table, and
  -- a unit 207 for receiving information on non-current addresses and removing corresponding entry from routing table.

- A unit 209 for routing according to routing table including

  -- a comparator 211 for comparing IP addresses of packets received from the BAS 19 of associated operator shop 3.1, 3.2 to entries in routing table, and
  -- a unit 213 for routing, according to the comparing operation executed in the comparator 211, in the case where the IP addresses agree with the dynamically created routing table entries indicating the common tunnel endpoint, to the common tunnel endpoint, e.g. the local VRF 49.

- A memory 215 including

  -- a memory place 217 for storing a routing table.

[0162] The different steps in accessing an operator shop 3.1, 3.2 using a common IPsec tunnel endpoint in the BRAS 17 and the special DHCP option for the case of a terminal connecting directly to an RG port 11 are almost the same as in the cases where the special DHCP option is not used. The way in which the terminal 15 obtains the IP address of the common IPsec tunnel endpoint is the only part that differs. There are two cases to consider. In the first case the special DHCP option includes an IP address of the common tunnel endpoint. In the second case the special DHCP option includes a FQDN that can be translated into an IP address of the common tunnel endpoint. In both cases the BRAS DHCP server 61.1, 61.2, 62, as in regular DHCP operation, also provides the terminal 15 with the IP address of a DNS (Domain Name System) server 148 that can translate FQDNs into IP addresses. This DNS server may be located in the BRAS 17, dedicated for a certain VRF or serving the entire broadband access network 29, or it may be located in the operator shops 3.1, 3.2. The different steps involved in this procedure when the special DHCP option contains an IP address are summarized below, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7g. The first steps performed when using the special DHCP option are:

1. A roaming user connects his terminal 15 to an RG port 11 having an already established connection with operator shop No. 1 and acquires an IP address out of the address range of operator shop No. 1, by interacting with the

Samsung Ex. 1004, Page 321 of 563

DHCP server 61.1 associated with VRF No. 1.
2. From the same DHCP server 61.1 the terminal 15 receives a special DHCP option that includes an IP address of the common tunnel endpoint (49; 145).

[0163] The remaining steps are the same as steps 3 - 16 described above for the case when the terminal, connecting directly to an RG port 11, accesses an operator shop 3.1, 3.2 using a common IPsec tunnel endpoint in the BRAS 17 without the use of the special DHCP option.

[0164] The first steps involved in this procedure when the special DHCP option contains an FQDN are summarized below, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7h.

1. A roaming user connects her/his terminal 15 to an RG port 11 having an already established connection with operator shop No. 1 and acquires an IP address out of the address range of operator shop No. 1, as well as a DNS server address, by interacting with the DHCP server 61.1 associated with VRF No. 1, 47.1.
2. From the DHCP server 61.1 the terminal 15 receives a special DHCP option that includes a FQDN of the common tunnel endpoint (49; 145).
3. The terminal 15 includes the FQDN in a request message and sends the request message to the DNS server 148, the address of which it has previously received.
4. The DNS server 148 examines the request and translates the FQDN into an IP address, or possibly a list of IP addresses, belonging to the common tunnel endpoint (49; 145), in accordance with regular DNS server operation.
5. The DNS server 148 sends the IP address, or the list of IP addresses respectively, resulting from the translation to the terminal 15.

[0165] The remaining steps are the same as steps 3 - 16 described above for the case where the terminal 15, connecting directly to an RG port 11, accesses an operator shop 3.1, 3.2 using a common IPsec tunnel endpoint in the BRAS 17 without the use of a special DHCP option.

[0166] The first steps in accessing an operator shop 3.1, 3.2 using a common tunnel endpoint in the BRAS 17 and the special DHCP option for the case of a terminal 15 connecting to an NAT 143 and the special DHCP option containing an IP address are summarized below, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7i.

1. An NAT 143 connects to an RG port 11.
2. The NAT 143 is authenticated and a VLAN association is created, connecting the NAT to operator shop No. 1, in the manner previously described for the case of a terminal 15 accessing an operator shop 3.1, 3.2 through a CPN 5.
3. The NAT 143 interacts with the DHCP server 61.1 associated with VRF No. 1, 47.1, and acquires an IP address out of the address range of operator shop No. 1, as well as the address of a DNS server 148.
4. From the DHCP server 61.1, the NAT 143 receives a special DHCP option that includes an IP address of the common tunnel endpoint, this special DHCP option actually included in the same message as the IP address assigned to the NAT and the DNS server address.
5. A roaming user connects her/his terminal 15 to the NAT 143.
6. The terminal 15 interacts with a DHCP server in the NAT 143 to acquire a private IP address.
7. From the DHCP server in the NAT 143 the terminal receives a special DHCP option that includes an IP address of the common tunnel endpoint (49; 145).

[0167] The remaining steps are the same as steps 3 - 16 described above for the case where the terminal, connecting directly to an RG port 11, accesses an operator shop 3.1, 3.2 using a common IPsec tunnel endpoint in the BRAS 17 without the use of a special DHCP option.

[0168] The different steps in accessing an operator shop 3.1, 3.2 using a common tunnel endpoint in the BRAS 17 and the special DHCP option for the case of a terminal 15 connecting to an NAT 143 and the special DHCP option containing an FQDN are summarized below, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7j.

1. An NAT 143 connects to an RG port 11.
2. The NAT 143 is authenticated and a VLAN association is created, connecting the NAT to operator shop No. 1, 3.1, in the manner previously described for the case of a terminal accessing an operator shop through a CPN 5.
3. The NAT 143 interacts with the DHCP server 61.1 associated with VRF No. 1 and acquires an IP address out of the address range of operator shop No. 1, as well as the address of a DNS server 148.
4. From the DHCP server 61.1 the NAT 143 receives a special DHCP option that includes an FQDN of the common tunnel endpoint (49; 145).

Samsung Ex. 1004, Page 322 of 563

5. Optionally, if the special DHCP option contains an FQDN, the NAT 143 includes the FQDN in a request message, which it sends to the DNS server 148, the address of which it has previously received.
6. If the NAT 143 sent the FQDN in a request message to the DNS server 148, the DNS server examines the request, translates the FQDN into an IP address, or possibly a list of IP addresses), belonging to the common tunnel endpoint (49; 145) and returns it to the NAT.
7. A roaming user connects her/ his terminal 15 to the NAT 143.
8. The terminal 15 interacts with a DHCP server in the NAT 143 to acquire a private IP address, as well as the IP address of a DNS server 148.
9. From the DHCP server in the NAT 143 the terminal 15 receives a special DHCP option that includes an IP address, if the NAT has chosen to have the FQDN translated, or an FQDN of the common tunnel endpoint (49; 145).
10. If the special DCHP option received from the DHCP server in the NAT 143 contains an FQDN, the terminal 15 includes the FQDN in a request message, which it sends to the DNS server 148, the address of which it has previously received. 11. If the terminal 15 sent the FQDN in a request message to the DNS server 148, the DNS server examines the request, translates the FQDN into an IP address, or possibly a list of IP addresses, belonging to the common tunnel endpoint (49; 145) and returns it to the terminal.

[0169] The remaining steps are the same as steps 3 - 16 described above for the case where the terminal 15, connecting directly to an RG port 11, accesses an operator shop 3.1, 3.2 using a common IPsec tunnel endpoint (49; 145) in the BRAS 17 without the use of a special DHCP option.

[0170] Steps to be performed by the special software in the terminal 15 and in the NAT 143 in the case where the special DHCP option contains one or more IP addresses of a common IPsec tunnel endpoint in the BRAS 17:

1. When a NAT 143 receives configuration data, e.g. an IP address and a DNS server address, from the DHCP server 61.1, 61.2 associated with the VRF 47.1, 47.2 of the operator shop 3.1, 3.2 that the NAT has connected to, it also receives and recognizes from the DHCP server a special DHCP option.
2. The NAT 143 extracts and stores the IP address(es) contained in the special DHCP option.
3. When a terminal 15 of a roaming user has connected to the NAT 143 and requests configuration data from the DHCP server of the NAT, the DHCP server sends a special DHCP option, in which it includes the IP address(es) of a common IPsec tunnel endpoint in the BRAS 17, to the terminal in addition to the regular configuration data.
4. When the terminal 15 receives the configuration data, e.g. an IP address and a DNS server address, from the DHCP server of the NAT, it also receives and recognizes the special DHCP option.
5. The terminal 15 extracts and stores the IP address(es) contained in the special DHCP option.
6. The terminal 15 uses a received IP address of a common IPsec tunnel endpoint (49; 145) in the BRAS 17 to establish an IPsec tunnel towards the common tunnel endpoint.

[0171] Steps to be performed by the special software in the terminal 15 and in the NAT 143 in the case where the special DHCP option contains an FQDN of a common IPsec tunnel endpoint in the BRAS and the NAT chooses to have the FQDN translated:

1. When a NAT 143 receives configuration data, e.g. an IP address and a DNS server address, from the DHCP server 61.1, 61.2 associated with the VRF 47.1, 47.2 of the operator shop 3.1, 3.2 that the NAT has connected to, it also receives and recognizes from the DHCP server a special DHCP option.
2. The NAT 143 extracts the FQDN from the special DHCP option and sends the FQDN in a DNS query to the DNS server 148, the address of which it received in step 1.
3. The NAT 143 receives one or more IP addresses in the response from the DNS server 148.
4. The NAT 143 extracts and stores the IP address(es) contained in the response from the DNS server 148.
5. When a terminal 15 of a roaming user has connected to the NAT 143 and requests configuration data from the DHCP server of the NAT, the DHCP server sends a special DHCP option, in which it includes the IP address(es) of a common IPsec tunnel endpoint (49; 145) in the BRAS 17, to the terminal in addition to the regular configuration data.
6. When the terminal 15 receives the configuration data, e.g. IP address and DNS server address, from the DHCP server of the NAT, it also receives and recognizes the special DHCP option.
6. The terminal 15 extracts and stores the IP address(es) contained in the special DHCP option.
7. The terminal 15 uses a received IP address of a common IPsec tunnel endpoint (49; 145) in the BRAS 17 to establish an IPsec tunnel towards the common tunnel endpoint.

[0172] Steps to be performed by the special software in the terminal 15 and in the NAT 143 in the case where the special DHCP option contains an FQDN of a common IPsec tunnel endpoint (49; 145) in the BRAS 17 and the NAT

Samsung Ex. 1004, Page 323 of 563

does not have to have the FQDN translated:

1. When a NAT 143 receives configuration data, e.g. an IP address and a DNS server (148) address, from the DHCP server 61.1, 61.2 associated with the VRF 47.1, 47.2 of the operator shop 3.1, 3.2 that the NAT has connected to, it also receives and recognizes from the DHCP server a special DHCP option.
2. The NAT 143 extracts and stores the FQDN contained in the special DHCP option.
3. When a terminal 15 of a roaming user has connected to the NAT 143 and requests configuration data from the DHCP server of the NAT, the DHCP server sends a special DHCP option, in which it includes the FQDN of a common IPsec tunnel endpoint (49; 145) in the BRAS 17, i.e. the FQDN that it stored in step 2, to the terminal in addition to the regular configuration data.
4. When the terminal 15 receives the configuration data, e.g. an IP address and a DNS server address, from the DHCP server of the NAT 143, it also receives and recognizes the special DHCP option.
5. The terminal 15 extracts the FQDN from the special DHCP option and sends the FQDN in a DNS query to the DNS server 148, the address of which it received in step 4.
6. The terminal 15 receives one or more IP addresses in response from the DNS server 148.
7. The terminal 15 extracts and stores the IP address(es) contained in the response from the DNS server.
8. The terminal 15 uses a received IP address of a common IPsec tunnel endpoint (49; 145) in the BRAS 17 to establish an IPsec tunnel towards the common tunnel endpoint.

[0173] The BRAS 17, the local VRF 49 of the BRAS 17 and the VRFs 47.1, 47.2 may have the same modules/components/functions as described above.

Access through an IPsec tunnel to an operator shop specific endpoint in the BRAS

[0174] In this procedure each operator shop 3.1, 3.2 connected to the broadband access network 29 has a dedicated tunnel endpoint in the BRAS 17. The following alternatives for dedicated tunnel endpoints may be considered:

1. The dedicated tunnel endpoints are given as dedicated addresses of the local VRF 49, i.e. special IP addresses pointing to the local VRF and possibly only used for the purpose of serving as tunnel endpoints. The local VRF could use only a subset, e.g. one, of its addresses for this purpose, but it could as well be all of its addresses, in which case they are not special at all. When an IP packet containing an IKE message is received in the local VRF 49, the contents of the packet is passed to the IKE software in the local VRF. This functionality may be available irrespective of which one of the addresses of the local VRF that is used. It is also possible that the local VRF 49 has only one address in the BRAS internal network, in which case this address will obviously be used for all purposes, including termination of IPsec tunnels. This also applies to the case where the tunnel endpoints are located in the BASs 19.
2. The dedicated tunnel endpoints are given as dedicated addresses of a dedicated tunnel endpoint device, such as an IPsec tunnel endpoint server 145. In the case where a dedicated tunnel endpoint device is used it must, as in cases described above, "have access to" an EAP Authenticator and an AAA client. The BRAS 17 may, in principle, be regarded a monolithic device. It may therefore be assumed that the internal entities thereof, comprising VRFs, EAP Authenticator(s), AAA client(s), etc. have means for possible communication with each other. Such communication may be implemented in a variety of ways obvious to one skilled in the art. Due to this property of the BRAS 17, it may e.g. be possible to let all BRAS internal entities that need an EAP Authenticator use the same EAP Authenticator entity. It may also be possible to arrange that each such entity has its own EAP Authenticator. The same applies to the AAA client.
3. The dedicated tunnel endpoints are given as dedicated addresses of each of the VRFs 47.1, 47.2 that are associated with an operator shop 3.1, 3.2.

[0175] As above, it may be assumed that a roaming user connects through an RG port 11 which is already associated with an authenticated connection towards one of the operator shops 3.1, 3.2, e.g. operator shop No. 1. In case 1 mentioned above the IPsec tunnel extends as illustrated in Fig. 2d for the common tunnel endpoint case and the tunnel establishment mechanisms are also basically the same as in the case using a common tunnel endpoint. The only difference is that the operator shop selection is not solely based on the realm part of the NAI, but also on the selected tunnel endpoint. If the supplied realm and the selected tunnel endpoint do not indicate or do not belong to the same operator shop, the tunnel establishment may optionally be rejected.

[0176] In the steps executed for the case of a common tunnel endpoint described with reference to Fig. 7a, step 6. is modified so that the local VRF 49, such as in a unit 219, recognizes the IP address of the request for an IPsec tunnel as being an address that it has to handle or is linked to it by comparing the IP address to entries in a table stored in a memory place 221 in the memory 103, see Fig. 7d. It then starts to establish the IPsec tunnel as described above. In

Samsung Ex. 1004, Page 324 of 563

the above listed steps to be performed by the common tunnel endpoint a new step may be executed before step 1 in which IP addresses of packets sent in the internal BRAS network are compared to all IP addresses handled by the local VRF. In step 2 the local VRF 49 receives from the EAP Authenticator 56 information on the user's regular NAI, as obtained in the EAP authentication procedure, in particular the realm part of the NAI, but this step may be modified to also include that this information is be compared to the address of the tunnel endpoint as obtained in the request for setting up the IPsec tunnel. This procedure is suitably executed by the unit 181, see Fig. 7d.

[0177] If the dedicated tunnel endpoints are distributed to the different dedicated VRFs 47.1, 47.2, i.e. in case 3. mentioned above, a tunnel endpoint does not have to be associated with a route to another VRF, see Fig. 2k. Instead the respective dedicated VRF routes the packets coming out of the IPsec tunnel like all other uplink packets, i.e. to the operator shop to which the VRF is dedicated, unless the packets have destination addresses from the address range of the broadband access network, indicating e.g. the local service network 51. However, in the downlink direction, the dedicated VRF 47.1, 47.2 of the wanted operator shop still has to establish a host route for the "inner" IP address of the terminal 15, 15', pointing to the tunnel interface, so that downlink packets addressed to the terminal 15 are sent through the tunnel to the terminal instead of being routed to the service VLAN 41.1, 41.2 associated with the VRF, like other downlink packets. Also in this case the realm part of the NAI should indicate the same operator shop as that for which the dedicated VRF is arranged.

[0178] For the example illustrated by the signal diagram of Fig. 7a, in this third case, the signal instance "Local virtual router function" may be substituted with "Virtual router function for op shop 2", the signal instance "BRAS DHCP server" substituted with "Dedicated DHCP server" and the signal instance "Virtual router function for op shop 2" deleted, see Fig. 7b. The AAA client and the EAP Authenticator used by the dedicated VRF may be the same BRAS internal entities as used by the local VRF, i.e. AAA client 23 and authenticator 56, but they may also be entities that are integrated in or associated with only the concerned VRF, 47.1, 47.2, see Fig. 7e. The units 219, 173, 175, 177, 179, 189, 185, 187 and optionally the unit 191 and the table in the memory place 201 used in the local VRF for the case of a common tunnel endpoint in the local VRF, as illustrated in Fig. 7d, must be moved to the dedicated VRF illustrated in Fig. 7e.

[0179] The IPsec tunnel may also be established via the local default VLAN 43, or via a WLAN AP 7 and a service VLAN 41.1, 41.2, or the local WLAN AP VLAN 45.

[0180] The methods of informing the terminals 15, 15' about the available potential tunnel endpoints may basically be the same as in the case where a single common endpoint is used, as described above. A difference is that the new possible DHCP option in this case contains a list of tunnel endpoints, each identified by the realm, and/or possibly the name, of the associated operator shop followed by an FQDN or one or more explicit IP addresses, compare the format examples given above. Alternatively, the new possible DHCP option may contain a single tunnel endpoint, but instead appear a plurality of times in the DHCP message, once for each dedicated tunnel endpoint. Generally, a message field, like a DHCP option, may be specified as including one or more, i.e. a list, of a certain type of information, such as the tunnel endpoint reference in our case. Alternatively, the message field may be specified as always including one and only one instance of a certain piece of data, such as the tunnel endpoint reference in the case described herein. In the former case a single instance of the message field, i.e. the special DHCP option in this case, is enough to convey a list. In the latter case a list is instead conveyed by including multiple instances of the message field, together, in essence, constituting a list. Obviously the same information is conveyed by the message in both cases.

[0181] In the previously illustrated examples of possible special DHCP option formats a realm length field and a realm field is in this case inserted before or after each item, where an "item" refers to a field containing an IP address or two associated fields consisting of an FQDN length field and an FQDN field. The two examples below illustrate how this "transformation" of the previously illustrated special DHCP option format examples is performed.

[0182] Format of option including a list of realms and associated FQDNs:

Option code	Option length	Realm No. 1 length	Realm No. 1	FQDN No. 1 length	FQDN No. 1	
		Realm No. n length	Realm No. n	FQDN No. n length	FQDN No. n	

The realm may be the same for several FQDNs, e.g. Realm No. 1 = Realm No. 2, such that several FQDNs consequently belong to the same operator shop 3.1, 3.2, each FQDN representing a potential IPsec tunnel endpoint in the BAS 19 of the operator shop.

[0183] Format of option including a single IP address and associated realm:

Samsung Ex. 1004, Page 325 of 563

Option code	Option length	Realm length	Realm			IP address			

[0184] The above examples of special DHCP option formats can be reused for DHCPv6, with the difference that the option-code and option-length fields are two octets each instead of one octet each. In addition, the IP addresses handled by DHCPv6 are 16-octet IPv6 addresses instead of 4-octet IPv4 addresses.

Access through an IPsec tunnel to a broadband access server

[0185] The simplest way to establish an IPsec tunnel from the terminal to the BAS 19 of a selected operator shop 3.1, 3.2 is to use the regular IPsec establishment mechanisms and make no difference between this IPsec tunnel and other IPsec tunnels that a terminal 15 may establish. However, it would mean that the IPsec tunnel is routed through the operator shop that is associated with the RG port 11, unless the RG port is currently associated with the local default VLAN 43. As a consequence, the resources of that operator shop, e.g. operator shop No. 1, and possibly other resources on the Internet, would have to be used, resulting in suboptimal routing and unnecessary charges for the subscriber of operator shop No. 1. In the case illustrated in Fig. 2e, it is assumed that the RG port 11 is associated with operator shop No. 1, whereas the terminal 15 wishes to access operator shop No. 2 through an IPsec tunnel to the BAS 19 of operator shop No. 2. The IPsec tunnel 147' then extends from the terminal 15 via the RG 1, the AN 13, VLAN No. 1, VRF No. 1, the BAS 19 of operator shop No. 1, the Internet 149 and ending in the BAS of operator shop No. 2.

[0186] A more attractive method is to establish host routes in all VRFs, including the local VRF 49, to tunnel endpoints in the BASs 19 of all operator shops 3.1, 3.2 connected to the broadband access network 29, compare the discussion of Fig. 2f above. Then, instead of going through operator shops and external networks, the IPsec tunnels are routed internally between the VRFs in the BRAS 17. For example, the dedicated VRF No. 1 may have a host route for the tunnel endpoint in the BAS 19 of operator shop No. 2, i.e. a routing table entry for the IP address of this tunnel endpoint, pointing to VRF No. 2 through the BRAS internal network. However, as mentioned above, if multiple operator shops connected to a broadband access network use overlapping address spaces, e.g. private addresses, then this method does not work, unless the tunnel endpoints at the operator shops are globally unique addresses, i.e. not taken from any overlapping private range.

[0187] The host routes to the BAS tunnel endpoints of the other operator shops control the routing of the uplink tunnel packets - and IKEv2 packets for establishment of the tunnels - but not the routing of the corresponding downlink packets. Using as an example an IPsec tunnel established between a terminal 15 communicating via the VRF No. 1 and the BAS 19 of operator shop No. 2, 3.2, the tunnel will pass through both VRF No. 1 and VRF No. 2 between the terminal and the BAS. The host route in VRF No. 1 ensures that uplink packets pertaining to the tunnel, or packets in the tunnel establishment procedure, are forwarded internally in the BRAS 17 to the VRF No. 2 and the regular routing in the VRF No. 2 forwards the packet to the BAS of operator shop 2. However, a corresponding downlink packet from the BAS 19 received by the VRF No. 2 has a destination address from the address range of operator shop No. 1. Hence, the regular routing table of VRF No. 2 would indicate that the packet should be forwarded towards the BAS of operator shop No. 2, although in this case the desired treatment of the packet would be to forward it to the VRF No. 1.

[0188] Hence, VRF No. 2 must be capable of handling a packet having a destination address out of the address range of operator shop No. 1 in different ways depending on whether it arrives from inside the broadband access network 29 or from its dedicated operator shop. If the packet arrives from the broadband access network, or from another VRF, the VRF No. 2 should forward it towards the BAS 19 of its dedicated operator shop, i.e. operator shop No. 2, whereas if the packet arrives at the interface towards the BAS of its dedicated operator shop, the VRF No. 2 should forward it to the VRF No. 1.

[0189] This behavior can be achieved, e.g. by having a separate routing table for packets arriving at the interface towards the BAS 19 of the dedicated operator shop. When the VRF uses different routing tables depending on the interface on which the concerned packet arrives, the different routing tables can be configured differently to incur the desired routing behavior. In the case of this example the routing table for packets arriving at the interface towards the BAS of operator shop No. 2 would indicate VRF No. 1 as the next hop for packets with a destination address out of the address range of operator shop No. 1. The routing table(s) for packets arriving at the other interfaces of VRF No. 2 would instead indicate the BAS of operator shop No. 2, or a router in the path towards the BAS of operator shop No. 2, as the next hop for packets with a destination address belonging to the address range of operator shop No. 1.

[0190] When the VRF No. 1 receives the downlink packet from the VRF No. 2, its regular routing ensures that the packet is forwarded in the broadband access network 29 towards the terminal 15.

[0191] Using the method of BRAS internal routing, the IPsec tunnel establishment becomes rather straightforward using IKEv2 with the NAT traversal detection option. The BAS 19 and the AAA devices/modules 37, 31 of the operator

Samsung Ex. 1004, Page 326 of 563

shop 3.1, 3.2 handle the user authentication.

[0192] As discussed above, the IPsec tunnel can also be established via a service VLAN 41.1, 41.2 or the local default VLAN 43, whichever is currently associated with the concerned RG port 11. In addition, the IPsec tunnel may be established via a WLAN AP 7 and a service VLAN or the local WLAN AP VLAN 45.

[0193] The ways of informing the terminal 15, 15' about the available potential tunnel endpoints are the same as for the procedure using multiple operator shop specific tunnel endpoints in the BRAS 17.

[0194] The different steps in accessing an operator shop 3.1, 3.2 using internal routing in the BRAS 17 to the BAS of a wanted operator shop are summarized below for the same example as above, i.e. it is assumed that a roaming user connects through an RG port 11 which is already associated with an authenticated connection towards operator shop No. 1 and that the user wants to connect to operator shop No. 2, the steps involving transmission of information also illustrated in the signal diagram of Fig. 7f.

1. A roaming user connects his terminal 15 to an RG port 11 having an already established connection with operator shop No. 1
2. The terminal 15 acquires an IP address out of the address range of operator shop No. 1, by interacting with the DHCP server 61.1 associated with VRF No. 1.
3. The user or terminal 15 receives or obtains the address of a tunnel endpoint in the BAS 19 of operator shop No. 2, such as by obtaining a web page from service portal 54 and finding the
) address therein, as illustrated in Fig. 7f, or by receiving a special DHCP option including an FQDN or one or more IP addresses of the tunnel endpoint in the BAS. If the terminal obtains an FQDN of the tunnel endpoint, it has it translated into one or more IP addresses, assisted by a DNS server 148, as previously described in the descriptions of IP sec tunnel establishment to a tunnel endpoint in the BRAS 17.
4. The users starts special software in the terminal 15 for starting the establishing of the IPsec tunnel, the special software adapted to in particular run IKEv2 and thus establish the security associations (SAs) for the IPsec tunnel.
5. The special software creates a message addressed to the received or obtained address for establishing an IPsec tunnel having the received or obtained address as its remote endpoint and) sends the message through the connected RG port 11, in RG port VLAN 55 and in VLAN No. 1, 41.1.
6. The dedicated VRF No. 1, 47.1, examines the address of the message by searching a routing table and finds that the address of the request message corresponds to an entry in the table indicating VRF No. 2, 47.2, as the next hop and forwards the message to VRF No. 2 through the inter-VRF network 52 or the BRAS internal network.
7. The message is received by VRF No. 2, the VRF No. 2 recognizing that the IP address of the endpoint is an address belonging to the operator shop to which it itself is dedicated, and it then forwards the request to the BAS 19 of operator shop No. 2.
8. The request is received by the BAS 19 of operator shop No. 2, the BAS recognizing that the) destination IP address of the message is an address belonging to or associated with it, then starting to establish the IPsec tunnel and first, using EAP for authentication, activating the AAA client 37 integrated in, or associated with, the BAS, which AAA client 37 in turn communicates with the AAA server 31 of operator shop No. 2.
9. In the case where an EAP Authenticator, not shown, integrated in, or associated with, the BAS 19 has sent an EAP-Identity-Request to the terminal 15, messages start to be sent between the AAA server 31 and the terminal 15, the AAA client 37 in the BAS also being involved.
10. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of a regular NAI.
11. An EAP authentication procedure between the AAA server 31 in operator shop No. 2 and the user terminal 15, via the AAA client 37 integrated in, or associated with, the BAS 19 of operator shop No. 2 3.2 is performed. The EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31 of operator shop No. 2. Between the AAA client 37 of the BAS 19 and the AAA server 31 the EAP packets are encapsulated in AAA messages.
12. After successful authentication, the very procedure for establishing the IPsec tunnel is executed.
13. The terminal 15 interacts with the DHCP server 59 associated of operator shop No. 2 to obtain an IP address to be used for packets inside the IPsec tunnel, also called an "inner IP address". It is also possible for the BAS to assign the inner IP address to the terminal using the Configuration payload in IKEv2.
14. The IP address is sent to the BAS 19, the BAS enters in a table that packets with this IP address as destination address are to be forwarded into the established IPsec tunnel. If the DHCP server 59 is integrated in the BAS, the passing of the IP address between the DHCP server and other parts of the BAS is simply BAS internal data handling. If the DHCP server is external to the BAS, the BAS may obtain the IP address, either by snooping the DHCP messages being passed between the DHCP server and the terminal 15 or by receiving it from the DHCP server via operator shop internal communications means, e.g. an operator shop internal network.
15. The user can start traffic using TCP/IP through the BAS 19 of operator shop No. 2. For example, the user can receive a web page from the BAS. Such a web page can present services available in operator shop No. 2.

Samsung Ex. 1004, Page 327 of 563

[0195] The special software in the terminal 15 may perform the same steps and be configured as described above.

[0196] The dedicated VRFs 47.1, 47.2 of the BRAS 17 may have at least the following modules/components/functions that may be necessary to perform the operator shop access in this case in addition to the modules/components/functions described in conjunction with access via an IPsec tunnel to a common tunnel endpoint in the BRAS, see Fig. 7e:

- A unit 250 for selecting a route or a routing table based on the incoming interface.
- Separate routing tables Nos. 1 and 2 stored at memory places 217, 217' for packets arriving at the interface towards the BAS 19 of the operator shop 3.1, 3.2 for which the VRF 47.1, 47.2 is dedicated and for packets arriving at other interfaces, respectively.

Operator shop selection in a foreign broadband access network

[0197] In a foreign broadband access network, which herein is taken to refer to a broadband access network that has no relation or connection to the home operator shop of a user, the operator shop selection is a much more complex matter than in the home broadband access network. The reason is that a regular NAI cannot be used to indicate the operator shop that the user desires to visit, this shop called herein the selected visited or selected desired operator shop. The NAI indicates the home operator shop 3h of the subscriber, i.e. the considered user, see Fig. 2i, but it provides no indication of the operator shop that is the desired visited operator shop. As described above, the user can from the terminal only access her/his home operator shop or an operator shop with which her/his home operator shop has a roaming agreement. In the operator shops involved, lists of other operator shops with which such agreements are stored, such as in memories 64 in or connected to their AAA servers 31, 31h.

[0198] The main cases that should be considered in a foreign broadband access network include:

- The user accesses the broadband access network through a CPN.
- The user accesses the broadband access network through a WLAN AP.
- The user accesses the broadband access network through an IPsec tunnel.

Access through a CPN

[0199] In this case it may be easier to achieve operator shop selection, if there is specific support for the selection process in the client software in the terminal 15, i.e. extra or modified software in addition to the support for EAP. However, the roaming architecture becomes more general and can easier encompass roaming users from other types of networks, if no specific support is required in the client software. Both these cases are considered below.

Access through a CPN with support in software of terminal

[0200] The procedure for this case relies on the concept of a modified NAI of the previously described general extended format. In this case the NAI is extended to include the realm of the selected operator shop 3.1, 3.2 that the user wants to visit. Thus, in this case the extended NAI has the format

"home-op-shop/name@visited-op-shop" or

"home-op-shop!name@visited-op-shop"

where "home-op-shop" is the realm of the home operator shop 3h of the user, see Fig. 2i, "visited-op-shop" is the realm of the selected operator shop that the user wants to visit, i.e. the one of the operator shops connected to the foreign broadband access network 29 that is selected to act as the visited operator shop, i.e. as illustrated in the drawings one of operator shops 3.1 and 3.2, and "name" is the user's username.

[0201] For producing such an extended NAI the software of the terminal 15 may e.g. allow

- manual selection, i.e. that the user enters his choice into the terminal, and/or
- automatic selection, i.e. the terminal software includes a function arranged to select an operator shop from a configured list of preferred visited operator shops.

[0202] As previously described, the communication from/with a user or a terminal 15 who/which is connecting to an RG port 11, without a previously active session, is by default directed to the local default VLAN 43, where the EAP authentication procedure is initiated by the Authenticator 56 and the AAA client 23 of the BRAS 17. If the terminal is to supply an extended NAI of the format described above during the authentication procedure, the terminal requires information about the operator shops that are available, i.e. about the operator shops 3.1, 3.2 that are connected to the broadband access network 29 to which the RG port is connected through an AN 13. The broadband access network can provide this information in different ways:

Samsung Ex. 1004, Page 328 of 563

a) A first way for the broadband access network 29 to advertise available operator shops is the method suggested to be used in 3GPP-WLAN interworking. This method is described in Farid Adrangi (Ed.), "Mediating Network Discovery and Selection", Internet draft, <draft-adrangi-eap-network-Discovery-and-Selection-01.txt>, February 2004. The basic concept is that the operator shop information is provided to the terminal 15 via EAP, in the case where the broadband access network receives from the terminal an NAI with an unrecognized realm part, i.e. a realm for which there is no available AAA route. The user or terminal then selects one of the advertised operator shops and provides a second NAI to the broadband access network, this time an extended NAI of the format described above.

b) A second way for the broadband access network 29 to advertise the available operator shops is to use a new link layer protocol to broadcast the information in the local default VLAN 43.

c) A third way is to let the user retrieve the operator shop information through off-line means.

d) Alternative methods that do not rely on information provided by the broadband access network 29 have been described and in these methods either the terminal 15 is designed to transfer a list of preferred visited operator shops to the broadband access network, and the network is made do the very selection, as described in the published International patent application WO 2006/038843, "Terminal controlled selection of intermediary network for roaming UMTS/WLAN subscribers", or they rely on support from a central Diameter redirect agent, as described in the published International patent application WO 2006/038844, "Home network controlled selection of intermediary network for roaming UMTS/WLAN subscribers".

[0203] In any case, the AAA proxy server 27 recognizes the realm of the selected visited operator shop in the modified NAI and routes the AAA message containing the EAP-Identity-Request to the AAA server 31 of the selected visited operator shop 3.1 or 3.2. Before forwarding the AAA message, the AAA proxy server may or may not remove the realm of the selected visited operator shop from the modified NAI and turn the NAI into its regular format. When the AAA server 31 of the selected visited operator shop receives the AAA message containing the EAP-Identity-Request, it recognizes the realm of the home operator shop as belonging to an operator shop with which it has a roaming agreement and routes the AAA message to the AAA server 31h of the home operator shop 3h. If the AAA proxy server 27 did not turn the NAI into its regular format, then the AAA server of the selected visited operator shop turns the extended NAI into its regular format before forwarding it to the AAA server of the home operator shop. Then a user authentication procedure is performed between the user/terminal 15 and the home AAA server 31h of the user, the AAA requests routed through the AAA client 23 of the BRAS, the AAA proxy server 27, the AAA server 31 of the selected one of the operator shops 3.1, 3.2 to the home AAA server 31h. After a successful user authentication the BRAS 17 instructs the concerned AN 13, e.g. via SNMP or some other protocol that the BRAS can use in the control of ANs, to associate the concerned RG port VLAN 55 with the service VLAN 41.1, 41.2, associated with the selected visited operator shop, e.g. VLAN No. 2 if operator shop No. 2 is selected, instead of the local default VLAN 43. Then the user can proceed to acquire an IP address via DHCP, in the example from the DHCP server 59 of operator shop 3.2, to enable subsequent IP communication with the selected visited operator shop and also with networks beyond the selected visited operator shop. In order for the BRAS 17 to know which AN to instruct virtual MAC addresses must be used.

[0204] In the description above the AAA client 23 is assumed to be located in the BRAS 17, closely connected to the local VRF 49. However, if the AAA client is instead located in the AN 13, neither the local default VLAN 43 nor virtual MAC addresses are needed for achieving the above described VLAN association in this access case.

[0205] If the user/terminal 15 only desires access to the local service network 51, the user/terminal may supply, just as in the case of access through the home broadband access network, a special NAI, having a realm part belonging to the broadband access network 29 that is dedicated for this purpose. Then, the AN 13 can keep its association between the concerned RG port VLAN 55 and the local default VLAN 43.

[0206] The different steps necessary for a roaming user to access a foreign operator shop 3.1, 3.2 for the case of the AAA client 23 located in the BRAS 17, special software provided in the user's terminal and the method a) described above for informing the user, are summarized below with reference to the signal diagram of Fig. 8a. The user is assumed to be logged in to a CPN 5 on a specific port 11 of the RG 1 from a terminal 15. Steps 1 - 7 are identical to the previously described steps 1 - 7, unless otherwise is explicitly stated, for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in her/his home broadband access network and the AAA client 23 is located in the BRAS 17. Similarly, steps 16 - 19 are the same as the previously described steps 10 - 13 for the same case, the only difference being that when the user is accessing a foreign broadband access network, the selected one of the operator shops 3.1, 3.2 that are connected to the broadband access network 29 acts as a visited operator shop instead of a home operator shop. For ease of understanding, these steps are repeated below, but in a more summarized manner. In addition, a general difference is that in the example used to illustrate the previously described steps for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network and the AAA client 23 is located in the BRAS 17 operator shop No. 1, 3.1, is assumed to be selected, whereas in the example used to illustrate the steps below operator shop No 2, 3.2, is assumed to be selected, i.e. it is the visited operator shop, but this difference is of little

Samsung Ex. 1004, Page 329 of 563

significance to the procedures as such.

1. The user connects her/his terminal to a broadband access network 29, e.g. by simply turning on the terminal device that is assumed to be connected to an RG port 11.
2. A frame or frames from the terminal 15 is/are received in the AN 13, retagged and forwarded into the local default VLAN 43.
3. A retagged frame or retagged frames from the terminal 15 is/are received in the local VRF 49 of the BRAS 17 and specifically received by the Authenticator symbolically indicated at 56.
4. The Authenticator 56 sends an EAP-Identity-Request to the terminal 15.
5. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of a regular NAI such as described above.
6. The Authenticator passes the EAP-Identity-Response to AAA client function 23 in BRAS 17.
7. The AAA client 23 sends the EAP-Identity-Response in an AAA message to the AAA proxy server 27.
8. The AAA proxy server 27 examines the NAI and recognizes a realm part for which it has no available AAA route.
9. The AAA proxy server 27 sends a message, typically an EAP-Identity-Request, containing information about available operator shops via EAP to the terminal 15. Between the AAA proxy server 27 and the AAA client 23 the message is carried in an AAA message.
10. The terminal 15 receives information about available operator shops and selects one thereof, which has a roaming agreement with the home operator shop.
11. The terminal 15 sends a new EAP-Identity-Response including an NAI having the extended format such as described above.
12. The message is received by the AAA proxy server 27 that forwards the AAA request to the AAA server 31 of the wanted visited operator shop, in the example operator shop No. 2, 3.2.
13. The AAA server 31 in the wanted visited operator shop examines the NAI and finds the realm of the home operator shop 3h of the user.
14. The AAA server 31 in the wanted visited operator shop, in the example operator shop 3.2, forwards the message to the AAA server 31h of the home operator shop 3h.
15. An EAP authentication procedure between the AAA server 31h of the home operator shop 3h and the user terminal 15 through the AAA server 31 of operator shop No. 2, 3.2 in the example, the AAA proxy server 27 and the AAA client 23 of the BRAS 17 is performed. The EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31h of the home operator shop 3h. Between the AAA client 23 of the BRAS 17 and the home AAA server 31h the EAP packets are encapsulated in AAA messages.
16. The logical function unit 57 in the BRAS 17 obtains information that the EAP/AAA procedure, in particular the identification and authentication procedures, has been completed and about the operator shop that has been selected. Out of the four alternatives for this in step 13 for the case described above where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network and the AAA client 23 is located in the BRAS 17 only alternatives a and d are relevant in this case. In addition, it would be possible for the AAA client and the AAA proxy server to supply one part each of the information to the LU 57. The AAA client 23 would then supply the VMAC address of the terminal 15 together with the session identifier of the AAA session. The AAA client could do this as it receives the EAP-Identity-Request or after it has received, from the AAA server 31h in the home operator shop 3h, via the AAA server 31 in the selected visited operator shop, in the example operator shop No. 2, 3.2, via the AAA proxy server 27, the AAA message including the indication of a successful user authentication. The AAA proxy server would supply an FQDN equal to the realm of the selected visited operator shop, or possibly some other BRAS internal identifier of the selected visited operator shop, together with the session identifier of the AAA session. The logical function unit 57 would associate the VMAC address and the FQDN, or the other BRAS internal identifier, respectively, by matching the session identifiers received from the AAA client 23 and the AAA proxy 27 server respectively. The logical function unit instructs the AN 13 to change the existing association between VLANs, using the VMAC address of the terminal 15 to find the correct AN 13.
17. The AN 13 receives an association instruction message and changes tagging for VLANs accordingly.
18. After the user has become authenticated, the terminal 15 can proceed to acquire an IP address supplied by the DHCP server 59 in desired visited operator shop, operator shop No. 2, 3.2, in the example, using the respective DHCP server 61.2 in the BRAS 17 as a DHCP relay agent. Alternatively the DHCP server 61.1 in the BRAS 17 can allocate, if assigned a predetermined address range, IP addresses directly to the terminal 15 from the address range of the desired visited operator shop such as operator shop No. 2, 3.2.
19. After the terminal 15 has been given an IP address, the user can start traffic using TCP/IP, through the VLAN 41.2, the VRF 47.2 and the BAS 19 of the desired visited operator shop such as operator shop No. 2, 3.2.

[0207] The AN 13 and the BRAS 17 may have the same components and functions as in the case of a user accessing

Samsung Ex. 1004, Page 330 of 563

through his home broadband access network. In addition, the AAA proxy server 27 may have a unit 223, see Fig. 8b, for responding to NAIs having an unrecognizable realm part, and a unit 225 for handling extended NAIs. Such a handling unit may then be arranged to analyze received extended NAIs, extracting the realm of the home operator shop and the realm of the operator shop that the source of the NAI desires to use as the visited operator shop. It may compare the realm of the desired visited operator shop to those connected to the BRAS, such as by referencing a table or list stored in a memory place 227, and if the realm of the desired operator shop agrees with an entry in the list, route AAA messages, some of them including EAP packets, to the AAA server 31 of the respective operator shop 3.1, 3.2. The terminal 15 must have some special software, see Fig. 8d, such as e.g. a unit 231 for receiving, in a suitable EAP packet, information about available operator shops, and a unit 233 for preparing and supplying extended NAIs. The AAA servers 31 of the operator shops 3.1, 3.2 may use, as described above, lists of operator shops with which they have roaming agreements, stored in memory places 64. Furthermore, they may include, see Fig. 8e, a unit 235 for handling extended NAIs, such a unit arranged to analyze extended NAIs, to extract the realm of the home operator shop of the source of the extended NAI, to compare extracted realms to entries in the table and to route AAA messages, some of which including EAP packets, to the AAA server 31h of the home operator shop 3h in the case where an agreement with an entry is detected.

Access through a CPN without support in software of terminal

[0208] As previously described, when a user or terminal 15 connects to an RG port 11, without a previously active session, she/he/it is for the communication by default directed to the local default VLAN 43, where the EAP authentication procedure is initiated by the Authenticator 56 of the BRAS 17. This is obviously also valid for a user wanting access to an operator shop through a foreign broadband access network.

[0209] Since the software of the terminal 15 in this case is assumed to have no support for the operator shop selection procedure, the terminal cannot receive operator shop information advertised by the broadband access network 29, irrespective of whether it is advertised using EAP or a new link layer protocol, i.e. alternatives a) and b) as described above. Thus, the terminal will supply the user's regular NAI to the broadband access network, unless the user has acquired operator shop information off-line, i.e. in some suitable way not using the services of the broadband access network, and has manually extended the NAI.

[0210] When faced with a non-routable NAI, the broadband access network 29, in particular the BRAS 17 thereof, is in this case arranged to bypass the actual authentication procedure, by immediately sending an EAP-Success packet, granting the user access to the local service network 51 and keeping the default association between the RG port VLAN 55 and the local default VLAN 43. Before sending the EAP-Success packet the broadband access network may optionally send an EAP-Notification-Request packet to the terminal 15 with a displayable message instructing the user to start her/his browser to select an operator shop, or publicly available services in the local service network 51. The EAP-Success packet and the optional preceding EAP-Notification-Request packet can be sent by the Authenticator 56 or the AAA proxy server 27. In the latter case, the Authenticator passes the EAP-Identity-Response packet from the terminal to the AAA client 23, which forwards it, included in an AAA message, to the AAA proxy server 27. Then, the AAA proxy server discovers that the packet is non-routable. In the former case, the Authenticator 56 itself discovers that the realm part of the NAI in the EAP-Identity-Response received from the terminal 15 does not belong to any of the operator shops 3.1, 3.2 that are connected to the broadband access network 29 and hence does not pass the packet to the AAA client 23.

[0211] Thereupon, when the user uses her/his browser, after acquiring an IP address from the address space of the broadband access network 29, in a procedure between the DHCP client of the terminal 15 and the general DHCP server 62 of the BRAS 17, she/he is redirected to a web page on the service portal 54 of the broadband access network, unless she/he attempts to access a specific web page in the local service network 51. On the web page obtained from the service portal the user can select between the available operator shops as well as services from the local service network.

[0212] If the user selects access to local services, the VLAN association, i.e. the association between the RG port VLAN 55 and the local default VLAN 43, as handled by the access node 13, and the IP address can remain as they are.

[0213] If the user clicks on a symbol for one of the available operator shops, this triggers, by a routine coupled to the displayed web page, the BRAS 17 to start executing the following steps, such as controlled by the logical function unit 57:

1. The BRAS 17 stores information on the selected operator shop and associates it with the virtual MAC address that is used for the concerned terminal 15 or, if no virtual MAC address is used, the actual MAC address of the terminal 15.
2. The BRAS 17 forces the DHCP client in the user's terminal 15 into the INIT state using a DHCP force renew procedure and a subsequent rejection of a possible request from the client to prolong its IP address lease from the address space of the broadband access network 29.
3. The BRAS 17 initiates a new EAP procedure towards the terminal 15, but this time with the user's selected operator shop stored.

Samsung Ex. 1004, Page 331 of 563

- This new EAP procedure will start in the same way as the previous one, i.e. with the EAP Authenticator 56 or the AAA proxy server 27 sending an EAP-Identity-Request packet to the terminal 15, but this time the BRAS 17 knows to which operator shop 3.1, 3.2 the resulting AAA request is to be routed. Thus it is ensured that the AAA request ends up in the selected operator shop 3.1, 3.2, i.e. in the AAA server 31 thereof, irrespective of which NAI the user provides. One way to achieve this is to let some unit in the BRAS 17, e.g. the EAP Authenticator unit 56, modify the NAI into the previously described extended format before handing it over to the AAA client 23 of the BRAS, but the AAA request may also be routed to the selected operator shop without any NAI modification, since the BRAS, that holds the knowledge about the selected operator shop, comprises both the EAP Authenticator unit 56, the AAA client 23 and the AAA proxy server 27.
- If the BRAS 17 fails to initiate the second EAP procedure, or if the authentication fails, the operator shop selection information, which was associated with the virtual MAC address used for the concerned user, or the MAC address of the user's terminal 15 if virtual MAC is not used, eventually times out and is deleted.
- Another method that may be used in this case is a method that relies on support from a central Diameter redirect agent, which is described in the cited published International patent application WO 2006/038844. That method is based on a central Diameter redirect agent that aggregates information about roaming agreements and visited network, i.e. visited operator shop, priority lists from operators, i.e. basically from home operator shops. The Diameter redirect agent information can be obtained through real-time operations, non-real-time - semi-manual - operations or manual off-line operations. In the case where this method is used, the terminal of a roaming user would supply a NAI having a realm part that has a specific ending, following a part that indicates the user's home operator shop that indicates the domain of the central Diameter agent. Thus, the AAA proxy server 27 of the broadband access network 29 will route the first AAA message pertaining to the user to the central Diameter redirect agent. The Diameter redirect agent returns a prioritized list of AAA servers of potential intermediary, i.e. visited, operator shops. The AAA proxy server searches the received list for a AAA server of an operator shop with which it has an association, i.e. one of the operator shops that are connected to the broadband access network, and selects the one of those that has the highest priority indicated. Then the AAA proxy server routes the initial AAA message to the AAA server 31 of the selected visited operator shop 3.1, 3.2.

4. Following a successful user authentication the BRAS 17 instructs the concerned AN 13, e.g. via SNMP, or some other protocol that the BRAS can use to control ANs, to associate the concerned RG port VLAN 55 with the service VLAN 41.1, 41.2 associated with the selected operator shop 3.1, 3.2, e.g. VLAN No. 1 if operator shop No. 1 is selected, instead of the local default VLAN 43. Then the terminal 15 may proceed to acquire an IP address via DHCP to enable subsequent IP communication. In order for the BRAS 17 to know which AN 13 to instruct virtual MAC must be used.

[0214] In the description above the AAA client 23 is assumed to be located in the BRAS 17, connected to the local VRF 49, but if the AAA client located most adjacent to the terminal is located in the AN 13, virtual MAC is not needed for this purpose, but the BRAS then has to be capable of triggering the AN to reinitiate the EAP procedure towards the terminal 15, and possibly inform the AN about the selected operator shop, e.g. using SNMP or some other protocol that the BRAS can use to control ANs.

[0215] If access only to the local service network 51 is desired, the user may supply, as in the case of access through the user's home broadband access network, a special NAI having a realm part belonging to the broadband access network 29, dedicated for this purpose. The AN 13 may then keep its association between the concerned RG port VLAN 55 and the local default VLAN 43. However, the communication from the terminal 15 of a roaming user will anyway be restricted to the local default VLAN 43 and the local service network 51 before the second EAP procedure is concluded. Hence, the terminal of a roaming user may, as well as using the above mentioned special NAI, supply the user's regular NAI and then select to access only services from the local service network, in which case the second EAP procedure is not initiated.

[0216] The different steps necessary for a roaming user to access an operator shop 3.1, 3.2 for the case of the AAA client 23 located in the BRAS 17 and no special software provided in the terminal 15 are summarized below with reference to the signal diagrams of Figs. 9a and 9b illustrating different cases. The user is assumed to be logged in to a CPN 5 on a specific port 11 of the RG 1 from a terminal 15. Steps 1 - 7 are identical, unless an exception is explicitly stated, to the previously described steps 1 - 7 for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network and where the AAA client 23 is located in the BRAS 17. Similarly, steps 25 - 28 for the case illustrated in Fig. 9a and steps 26 - 29 for the case illustrated in Fig. 9b are the same as the previously described steps 10 - 13 for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network and where the AAA client 23 is located in the BRAS 17, with the only difference being that when the user is accessing a foreign broadband access network, the selected one of the operator shops 3.1, 3.2 that are connected to the broadband access network acts as a visited operator shop instead of a home operator shop. For

Samsung Ex. 1004, Page 332 of 563

ease of understanding, these steps are repeated below, but in a more summarized manner. In addition, a general difference is that in the example used to illustrate the previously described steps for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network and where the AAA client 23 is located in the BRAS 17 operator shop No. 1 3.1 is selected, whereas in the example used to illustrate the steps below operator shop No 2 3.2 is selected, as the visited operator shop, but this difference is of no significance to the procedures as such. Of the above described two alternatives for which entity that discovers that the NAI does not belong to any of the operator shops that are connected to the broadband access network, i.e. the AAA proxy server 27 or the EAP Authenticator 56, the AAA proxy server 27 is assumed in the description of the steps below.

[0217] First the steps for the case illustrated in Fig. 9a will be described.

1. The user connects his terminal 15 to a broadband access network 29, e.g. by simply turning on his terminal device that is assumed to be connected to an RG port 11.
2. A frame or frames from the terminal 15 is/are through the residential gateway 1 or switch received in the AN 13, is/are retagged therein and forwarded into the local default VLAN 43.
3. A retagged frame or retagged frames from the terminal 15 is/are received in the local VRF 49 of the BRAS 17.
4. From the local VRF 49 an EAP-Identity-Request is sent to the terminal 15.
5. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of a regular NAI such as described above.
6. The local VRF 49 passes the EAP-Identity-Response to AAA client function 23 in the BRAS 17.
7. The AAA client 23 sends the EAP-Identity-Response in an AAA message to the AAA proxy server 27.
8. The AAA proxy server 27 examines the NAI and recognizes a realm part for which it has no available AAA route.
9a. In this optional step, the AAA proxy server 27 may send an EAP-Notification-Request packet to the terminal 15, including a displayable text string instructing/recommending the user to start her/his browser and select an operator shop.
9b. In this optional step, performed only if step 9a is performed, the AAA proxy server 27 receives an EAP-Notification-Response in return from the terminal. Such a response is mandatory according to the EAP specification.
10. The AAA proxy server 27 sends an EAP-Success packet to the terminal.
11. The terminal 15 receives the EAP-Success packet and acquires an IP address from the BRAS DHCP server 62.
12. The terminal 15 connects through its browser to the service portal 54 in the local service network 51, either directly or after being redirected during an attempt to connect to a server outside the local service network.
13. The terminal 15 receives a web page from the service portal 51 including information about available operator shops.
14. The user, using the browser of her/his terminal 15, selects one of the available operator shops which has a roaming agreement with the user's home operator shop 3h.
15. Information about the selection made is transferred to the BRAS 17, such as first to the service portal 54.
16. Information about the selection made is stored in the BRAS 17 such as first transferred from the service portal 54 to the logical function unit 57 and then stored by this unit in a suitable memory, the information stored e.g. in the form of the realm part of the NAI or some other BRAS internal indicator of the selected operator shop, coupled to e.g. the virtual MAC address used for the terminal 15 or some other suitable information identifying the user terminal. The coupling of these stored data to each other may be executed by e.g. storing them together, storing them separately with a reference, such as a pointer, between them, storing them in a mutual software "object", such as in object oriented programming languages.
17. The BRAS 17 transmits a message, e.g. a DHCP FORCERENEW message, such as commanded by its logical function unit 57 sending a message to the DHCP server 62, to the terminal 15, forcing it into the INIT state according to DHCP to make the IP address of the terminal no longer usable. If the terminal subsequently requests the DHCP server to renew or prolong the lease of the old IP address of the terminal, the DHCP server will reject such a request.
18. The BRAS 17, e.g. the AAA proxy server 27, such as commanded by a message received from the logical function unit 57, sends an EAP-Identity-Request to the terminal 15.
19. The terminal 15 sends an EAP-Identity-Response, including the user's identity in the form of a regular NAI.
20. The EAP-Identity-Response is received by the BRAS AAA client 23, which includes it in an AAA message and sends it to the AAA proxy server 27.
21. The message is received by the AAA proxy server 27, as described above for the initial EAP-Identity-Response in steps 6 and 7. The AAA proxy server examines the NAI and compares it to stored entries, finds in the example that operator shop No. 2, 3.2 is selected as the visited operator shop and forwards the AAA request to the AAA server 31 in operator shop No. 2, 3.2.
22. The AAA server 31 in the wanted visited operator shop, in the example operator shop No. 2, 3.2, examines the NAI of the AAA request and finds the realm of the home operator shop 3h of the user.
23. The AAA server 31 in the wanted visited operator shop forwards a message to the AAA server 31h of the home

Samsung Ex. 1004, Page 333 of 563

operator shop 3h, see also Fig. 2j.

24. An EAP authentication procedure between the AAA server 31h of the home operator shop 3h and the user terminal 15 through the AAA server 31 of operator shop No. 2, 3.2 in the example, the AAA proxy server 27 and the AAA client 23 of the BRAS 17 is performed. This EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31h of the home operator shop 3h. Between the AAA client 23 of the BRAS 17 and the home AAA server 31h the EAP packets are encapsulated in AAA messages.

25. The logical function unit 57 in BRAS 17 obtains information that the EAP/AAA procedure has been completed and about the operator shop that has been selected if it has not been informed thereof in step 16 above. Out of the four alternatives for this in step 13 for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network for the case where the AAA client 23 is located in the BRAS 17 only alternatives a) and d) are relevant in this case. In addition, it would also be possible for the AAA client 23 and the AAA proxy server 27 to supply one part each of the information to the LU 57. The AAA client would then supply the VMAC address of the terminal 15 together with the session identifier of the AAA session. The AAA client 23 could do this as it receives the EAP-Identity-Request or after it has received, from the AAA server 31h in the home operator shop, via the AAA server 31 in the selected visited operator shop, via the AAA proxy server 27, the AAA message including the indication of a successful user authentication. The AAA proxy server would supply an FQDN equal to the realm of the selected visited operator shop, or some other suitable BRAS internal identifier of the selected visited operator shop, together with the session identifier of the AAA session. The logical function unit 57 would associate the VMAC address and the FQDN, or another BRAS internal identifier respectively, by matching the session identifiers received from the AAA client 23 and the AAA proxy server 27, respectively. The logical function unit instructs the AN 13 to change the existing association between VLANs, using the VMAC address of the terminal 15 to find the correct AN 13.

26. The AN 13 receives an association instruction message and changes tagging for VLANs accordingly.

27. After the user has become authenticated, the terminal 15 can proceed to acquire an IP address supplied by the DHCP server 59 in the selected visited operator shop No. 2, 3.2 in the example, using the respective DHCP server 61.2 in the BRAS 17 as a DHCP relay agent. Alternatively the DHCP server 61.2 in the BRAS 17 can allocate, if assigned a predetermined address range, an IP address directly to the terminal 15 from the address range of the selected visited operator shop, operator shop No. 2, 3.2, in the example.

28. After the terminal 15 has been given an IP address, the user can start traffic using TCP/IP, through the VLAN 41.2, the VRF 47.2 and the BAS 19 of the selected visited operator shop, in the example operator shop No. 2, 3.2.

[0218] Second, the steps for the case illustrated in Fig. 9b will be described.

1. The user connects his terminal 15 to a broadband access network 29, e.g. by simply turning on his terminal device that is assumed to be connected to an RG port 11.

2. A frame or frames from the terminal 15 is/are through the residential gateway 1 or switch received in the AN 13, is/are retagged therein and forwarded into the local default VLAN 43.

3. A retagged frame or retagged frames from the terminal 15 is/are received in the local VRF 49 of the BRAS 17 responding by forwarding them to the EAP Authenticator symbolically indicated at 56. The EAP Authenticator 56 may be associated with, connected to or integrated with the local VRF 49.

4. The EAP Authenticator 56 sends an EAP-Identity-Request to the terminal 15.

5. The terminal 15 responds with an EAP-Identity-Response, including the user's identity in the form of a regular NAI such as described above.

6. The EAP Authenticator 56 passes the EAP-Identity-Response to AAA client function 23 in the BRAS 17.

7. The AAA client 23 sends the EAP-Identity-Response in an AAA message to the AAA proxy server 27.

8. The AAA proxy server 27 examines the NAI and recognizes a realm part for which it has no available AAA route.

9a. In this optional step, the AAA proxy server 27 may send an EAP-Notification-Request packet to the terminal 15, including a displayable text string instructing/recommending the user to start her/his browser and select an operator shop.

9b. In this optional step, performed only if step 9a is performed, the AAA proxy server 27 receives an EAP-Notification-Response in return from the terminal. Such a response is mandatory according to the EAP specification.

10. The AAA proxy server 27 sends an EAP-Success packet to the terminal 15.

11. The terminal 15 receives the EAP-Success packet and acquires an IP address from BRAS DHCP server 62.

12. The terminal 15 connects through its browser to the service portal 54 in the local service network 51, either directly or after being redirected during an attempt to connect to a server outside the local service network.

13. The terminal 15 receives a web page from the service portal 51 including information about available operator shops.

14. The user, using the browser of her/his terminal 15, selects one of the available operator shops which has a roaming agreement with the user's home operator shop 3h.

Samsung Ex. 1004, Page 334 of 563

15. Information about the selection made is transferred to the BRAS 17, such as first to the service portal 54.
16. Information about the selection made is stored in the BRAS 17 such as first transferred from the service portal 54 to the logical function unit 57 and then stored by this unit in a suitable memory, the information stored e.g. in the form of the realm part of the NAI or some other BRAS internal indicator of the selected operator shop, coupled to e.g. the virtual MAC address used for the terminal 15 or some other suitable information identifying the user terminal.
17. The BRAS 17 transmits a message, e.g. a DHCP FORCERENEW message, such as commanded by its logical function unit 57 sending a message to the DHCP server 62, to the terminal 15, forcing it into the INIT state according to DHCP to make the IP address of the terminal no longer usable. If the terminal subsequently requests the DHCP server to renew or prolong the lease of the old IP address of the terminal, the DHCP server will reject such a request.
18. The BRAS 17, e.g. the EAP Authenticator 56, such as commanded by a message received from the logical function unit 57, sends an EAP-Identity-Request to the terminal 15.
19. The terminal 15 sends an EAP-Identity-Response, including the user's identity in the form of a regular NAI, to the EAP Authenticator 56.
20. The EAP Authenticator 56 passes the EAP-Identity-Response to the AAA client function 23 in the BRAS 17.
21. The EAP-Identity-Response is received by the BRAS AAA client 23, which includes it in an AAA message and sends it to the AAA proxy server 27.
22. The AAA message is received by the AAA proxy server 27 that examines the NAI and compares it to stored entries, finds in the example that operator shop No. 2, 3.2 is selected as the visited operator shop and forwards the AAA request to AAA server 31 in the selected visited operator shop, operator shop No. 2, 3.2 in the example.
23. The AAA server 31 in the wanted visited operator shop, in the example operator shop No. 2, 3.2, examines the NAI of the AAA request and finds the realm of the home operator shop 3h of the user.
24. The AAA server 31 in the wanted visited operator shop forwards a message to the AAA server 31h of the home operator shop 3h, see also Fig. 2).
25. An EAP authentication procedure between the AAA server 31h of the home operator shop 3h and the user terminal 15 through the AAA server 31 of operator shop No. 2, 3.2 in the example, the AAA proxy server 27 and the AAA client 23 of the BRAS 17 is performed. This EAP authentication procedure is handled end-to-end between the terminal 15 and the authentication server which is the AAA server 31h of the home operator shop 3h. Between the AAA client 23 of the BRAS 17 and the home AAA server 31h the EAP packets are encapsulated in AAA messages.
26. The logical function unit 57 in BRAS 17 obtains information that the EAP/AAA procedure has been completed and about the operator shop that has been selected if it has not been informed thereof in step 16 above. Out of the four alternatives for this in step 13 for the case where a user is accessing an operator shop 3.1, 3.2 via a CPN 5 in his home broadband access network for the case where the AAA client 23 is located in the BRAS 17 only alternatives a) and d) are relevant in this case. In addition, it would also be possible for the AAA client 23 and the AAA proxy server 27 to supply one part each of the information to the LU 57. The AAA client would then supply the VMAC address of the terminal 15 together with the session identifier of the AAA session. The AAA client 23 could do this as it receives the EAP-Identity-Request or after it has received, from the AAA server 31h in the home operator shop, via the AAA server 31 in the selected visited operator shop, via the AAA proxy server 27, the AAA message including the indication of a successful user authentication. The AAA proxy server would supply an FQDN equal to the realm of the selected visited operator shop, or some other suitable BRAS internal identifier of the selected visited operator shop, together with the session identifier of the AAA session. The logical function unit 57 would associate the VMAC address and the FQDN, or another BRAS internal identifier respectively, by matching the session identifiers received from the AAA client 23 and the AAA proxy server 27, respectively. The logical function unit instructs the AN 13 to change the existing association between VLANs, using the VMAC address of the terminal 15 to find the correct AN 13.
27. The AN 13 receives an association instruction message and changes tagging for VLANs accordingly.
28. After the user has become authenticated, the terminal 15 can proceed to acquire an IP address supplied by the DHCP server 59 in the selected visited operator shop No. 2, 3.2 in the example, using the respective DHCP server 61.2 in the BRAS 17 as a DHCP relay agent. Alternatively the DHCP server 61.2 in the BRAS 17 can allocate, if assigned a predetermined address range, an IP address directly to the terminal 15 from the address range of the selected visited operator shop, operator shop No. 2, 3.2, in the example.
29. After the terminal 15 has been given an IP address, the user can start traffic using TCP/IP, through the VLAN 41.2, the VRF 47.2 and the BAS 19 of the selected visited operator shop, in the example operator shop No. 2, 3.2.

[0219] The AN 13 and the BRAS 17 may have the same components and functions as in the case of a user accessing through his home broadband access network.

[0220] In addition the AAA proxy server 27 may have a unit 237, see Fig. 9c, for analyzing NAIs and comparing the realm parts thereof to available operator shops and a unit 238 for responding to NAIs having an unrecognizable realm part, including an optional subunit for transmitting a message urging the user to start a browser and a subunit for transmitting an EAP-Success message to a terminal. For the comparing it may reference a table or list stored in a memory

Samsung Ex. 1004, Page 335 of 563

place 227. Alternatively, the EAP Authenticator 56 may have such additional units, see Fig. 9g. The AAA proxy server 27, or the EAP Authenticator, respectively, may further include a unit 239 for receiving instructions to force a new authentication process and to send a message to the terminal 15 for starting such a new authentication process. The AAA proxy server may have a unit 241 for comparing NAIs or similar information to entries in a stored list and for routing, for NAIs for which the information agrees with an entry, to the AAA server 31 of an operator shop 3.1, 3.2, for which there is an identification stored associated with said entry.

[0221] The logical unit 57, see Fig. 9d, that can be collocated with or included in some other unit in the BRAS 17, may include a unit 243 for receiving, when a user clicks an appropriate symbol on web page, information from the service portal 54 on the selected operator shop, a unit 245 for storing this information together with necessary information to identify the user's terminal, such as the VMAC address thereof, in a memory place 247, and a unit 249 for sending instructions to the AAA proxy server 27 or the EAP Authenticator 56 to force a new authentication process and/or sending instructions to force renewal of the IP address of a terminal.

[0222] The AAA servers 31 of the operator shops 3.1, 3.2 may use, as described above, lists of operator shops with which they have roaming agreements, stored in memory places 64. Furthermore, they may include, see Fig. 9e, a unit 251 for handling NAIs, such a unit arranged to analyze NAIs, extract the realm part thereof, compare realms to entries in the table and route AAA messages, some of which may include EAP packets, to the AAA server 31h of the home operator shop in the case where an agreement with an entry is detected.

[0223] The service portal 54 may, as illustrated in Fig. 9f, include a unit for sending web pages, such as a web page including information about available operator shops, a unit for receiving information from web pages when they are displayed on a user device, or more specifically for receiving information in HTTP messages from terminals accessing such web pages or links on such web pages, such as information about a selected operator shop, and a unit for responding to such received information, forwarding the information to some suitable recipient such as the logical function unit 57 or possibly the EAP Authenticator 56.

Access through a public WLAN AP supporting the virtual AP concept

[0224] For a public WLAN AP 7 that supports the virtual AP concept the access procedure is substantially similar to that described above for a user accessing through her/his home broadband access network, only the authentication procedure being executed from the AAA server of the home operator shop 31h instead of that of an operator shop connected to the broadband access network 29, and may in particular include at least the following steps.

[0225] As described above, when a user or terminal 15' accesses the broadband access network 29 through a public WLAN AP 7, she/he/it must use the SSID associated with the operator shop 3.1, 3.2 that she/he has selected. Guiding information, in addition to the contents of the SSIDs themselves, may be obtained beforehand from the service portal 54 that can be reached by the user/terminal first attaching to the WLAN AP 7 using the SSID associated with the local WLAN AP VLAN 45.

[0226] The WLAN AP will then ensure that the AAA request resulting from the EAP procedure is routed to the selected operator shop 3.1, 3.2, either

- by modifying the NAI into the extended format, such as
  "home-op-shop/name@op-shop-realm-associated-with-selected-SSID" or
  "home-op-shop!name@op-shop-realm-associated-with-selected-SSID",

or by conveying in some suitable way the corresponding information, such as the used SSID, to the AAA proxy server 27.

[0227] However, the authentication procedure must be made from the AAA server 31h of the home operator shop 3h of the user. Thus, when the AAA proxy server 27 receives the AAA message containing the EAP-Identity-Request, it forwards the AAA request to the AAA server 31 of the wanted visited operator shop, as indicated by the extended NAI or other equivalent information. Before forwarding the AAA message the AAA proxy server removes the "equivalent information", e.g. the used SSID, if any, from the AAA message. If an extended NAI is used, the AAA message is handled in the same way as described for the case where a roaming user accesses a foreign broadband access through a CPN using the extended NAI method to indicate the wanted visited operator shop. That is, either the AAA proxy server or the AAA sever of the selected operator shop turns the modified NAI into its regular format before forwarding the AAA message. The AAA server 31 in the wanted visited operator shop 3.1 or 3.2 examines the NAI, finds the realm of the home operator shop 3h of the user, checks that there is a roaming agreement, and forwards the AAA request to the appropriate authentication server, i.e. the AAA server 31h of the home operator shop of the user. Then, the EAP authentication procedure is executed end-to-end between the AAA server 31h of the home operator shop 3h and the user terminal 15' through the AAA server 31 of the selected visited operator shop 3.1, 3.2, the AAA proxy server 27 and the AAA client 25 of the WLAN AP 7. Between the AAA client 25 and the AAA server 31h the EAP packets are encapsulated in AAA messages.

[0228] The remaining steps may be the same as those described for a non-roaming user.

Access through a public WLAN AP not supporting the virtual AP concept

[0229] If the public WLAN AP 7 does not support the virtual AP concept, the access procedure for a roaming user is similar to that described for access through a CPN 5 for a roaming user. In this case an AN 13' is used between the WLAN AP and the BRAS 17, see Fig. 2j. Furthermore, the VLANs 41.1, 41.2, 43 illustrated in Fig. 2a that extend all the way to the WLAN AP, i.e. VLAN No. 1, VLAN No. 2 and the local WLAN AP VLAN, do not encompass the link between the AN 13' and the WLAN AP 7, but instead ends in the AN 13'. No VLAN separation is be needed between the WLAN AP 7 and the AN 13'.

Access through a WLAN AP not supporting the virtual AP concept with special software in terminal

[0230] If there is specific support for operator shop selection in the client software in the terminal 15', the access procedure is substantially the same as described for the case of access through a CPN 5 using extended NAIs. Informing the terminal about the available operator shops 3.1, 3.2 may be done in the same way and the above-mentioned methods plurality of service providing networks described respectively in the cited published International patent applications WO 2006/038844 and WO 2006/038843 can also be used.

[0231] A difference is that the AAA client 25 is located in the WLAN AP 7 instead of in the BRAS 17. The AAA request resulting from the EAP-Identity-Response during the EAP authentication procedure is routed to the BRAS AAA proxy server 27 and the AAA client of the WLAN AP includes the MAC address of the terminal 15' in the AAA request, e.g. in the RADIUS Calling-Station-Id attribute, which is also reused in the Diameter protocol, or a vendor specific attribute. During, or immediately following, the authentication procedure the AAA server 31h of the home operator shop 3h provides one or more session keys, possibly produced as a byproduct in the authentication procedure, to the WLAN AP 7 to be used for the cryptographic protection mechanisms of IEEE 802.11i. As before, following a successful user authentication the BRAS 17 instructs the AN 13', e.g. using SNMP or some other protocol that the BRAS can use to control ANs, to associate the current MAC address of the terminal 15' with the service VLAN 41.1, 41.2 of the selected visited operator shop 3.1, 3.2, e.g. VLAN No. 2 if operator shop No. 2 was selected as the visited operator shop. Then the terminal may proceed to acquire an IP address via DHCP to enable subsequent IP communication.

Access through a public WLAN AP not supporting the virtual AP concept without special software in terminal

[0232] If there is no support for the operator shop selection in the client software in the terminal 15', extended NAIs cannot be used. Instead the BRAS AAA proxy server 27 may be arranged to immediately approve of the user authentication, when it is faced with a non-routable AAA request, i.e. an AAA request including a destination realm for which the AAA proxy server has no route. The BRAS 17 instructs the AN 13' to associate the MAC address of the user's terminal, which was received in the AAA request, with the local WLAN AP VLAN 45. The result is of course the same if the BRAS 17 sends no instructions at all to the AN. Optionally the AAA proxy server 27 may send an EAP-Notification-Request to the terminal 15' with a displayable string encouraging the user to start her/his browser to be used for operator shop selection.

[0233] The user now has access to the local service network 51 and the service portal 54. On the service portal, to which the browser running in the user's terminal 15' is redirected if trying to access an external web page, i.e. from a server located outside the local service network, the user can find information about available operator shops. The user selects an operator shop, or local services, by clicking on a symbol for one of them. The current MAC address of the terminal is then associated with the choice and both the MAC address and an indication of the choice are stored in the BRAS 17. Then, unless the user has selected access to local services, the terminal 15' is forced to abandon its IP address, as described for the case of access through a CPN 5 for a roaming user.

[0234] If the AAA protocol is Diameter, the next step is for the AAA proxy server 27 to request the WLAN AP 7 to re-authenticate the terminal 15' through a Re-Auth-Request AAA message. The AAA client 25 of the WLAN AP 7 initiates a new EAP authentication procedure towards the terminal by sending an EAP-Identity-Request packet and receives an EAP-Identity-Response in return. The AAA proxy server matches the subsequent AAA request with the stored visited operator shop selection through the terminal MAC address that the AAA client 25 in the WLAN AP 7 includes in the AAA request, e.g. in the RADIUS Calling-Station-Id attribute, which is also reused in the Diameter protocol, or a vendor specific attribute. This time the AAA messages carrying the EAP procedure are routed between the WLAN AP 7 and the AAA server 31h of the user's home operator shop 3h via the AAA server 31 of the selected visited operator shop 3.1, 3.2. The re-authentication triggers IEEE 802.11i mechanisms to be initiated and after that the AAA client 25 in the WLAN AP 7 initiates a new accounting subsession, which clearly distinguishes any accounting data preceding the re-authentication from accounting data subsequent to the re-authentication procedure. Possibly, the same method can be

used, if the AAA protocol is RADIUS. In the worst case the terminal 15' would have to re-connect and initiate a new EAP procedure itself.

[0235] This procedure leaves the WLAN AP 7 unaffected and may thus be used with available off-the-shelf APs.

[0236] If no AN 13' is used between the WLAN AP 7 and the BRAS 17, the BRAS must send its instructions to the WLAN AP and the WLAN AP must include a unit for receiving such instructions and for associating the MAC address of the user's terminal 15' with one out of several VLANs 41.1, 41.2, 43, these VLANs in this case extending all the way to the WLAN AP, according to the received instructions.

Access through an IPsec tunnel

[0237] The layer 3 solution, based on IPsec tunnels, can also be used by a roaming user accessing the broadband access network 29 from the terminal 15' through a WLAN AP 7, considering the fact that the authentication of the user must always be executed between the user and the AAA server 31h of the user's home operator shop 3h instead of between the user and the AAA server of the wanted operator shop 3.1, 3.2, the latter AAA server actually serving as a relay agent in the authentication procedure.

[0238] The variants of the IPsec tunnel based layer 3 solution are the same as for the case of a user accessing his home broadband access network.

Access through an IPsec tunnel to a common tunnel endpoint in the BRAS

[0239] The procedure described above for a user accessing an operator shop through his home broadband access network using a single common tunnel endpoint for all connected operator shops 3.1, 3.2 has to be modified as follows.

[0240] The IPsec tunnel to the local VRF 49 in the BRAS 17, or a dedicated tunnel endpoint device 145, is established in the same way as described for a user accessing his home broadband access network. However, since neither the tunnel endpoint itself nor the regular NAI provided by the terminal 15' indicates to which of the connected operator shops 3.1, 3.2 the AAA requests, and subsequent user data, are to be routed, extensions to the procedure are needed. During the EAP procedure the user can instead indicate the selected visited operator shop through an extended NAI, of the format described above

"home-op-shop/name@visited-op-shop" or

"home-op-shop!name@visited-op-shop"

[0241] If the user does not supply an extended NAI, the EAP based advertising of operator shop information may be used to let the user or terminal 15' select one of the available operator shops 3.1, 3.2 and include the realm thereof in a subsequently transferred extended NAI, as described in the cited standard text Farid Adrangi (Ed.), "Mediating Network Discovery and Selection", Internet draft, <draft-adrangi-eap-network-Discovery-and-Selection-01.txt>.

[0242] Before forwarding an AAA request the AAA proxy server 27 may turn the extended NAI into a regular NAI, having the format

"name@home-op-shop"

by deleting the "visited-op-shop" realm, moving the "home-op-shop" realm to the right of the "@" character and deleting the "/" or "!" character before the "name" part. Otherwise the AAA server 31 in the selected visited operator shop 3.1, 3.2 turns the extended NAI into a regular NAI.

[0243] The above mentioned method that is described in the cited International patent application WO 2006/038844 and relies on support from a central Diameter relay agent is also applicable to this case.

Access through an IPsec tunnel to an operator shop specific endpoint in the BRAS

[0244] The procedures using a dedicated tunnel endpoint for each connected operator shop 3.1, 3.2 can be almost entirely reused from the home broadband access network case. It is the task of the AAA server 31 of the selected one of the visited operator shops 3.1, 3.2 to route the AAA requests to the home AAA server 31h of the user, based on the realm part of the NAI that the terminal 15 supplies, the NAI indicating the realm of the home operator shop of the user of the terminal.

Access through an IPsec tunnel to a broadband access server

[0245] The procedures using an IPsec tunnel to the BAS 31 of the selected visited operator shop 3.1, 3.2 can be almost entirely reused from the home broadband access network case. It is the task of the AAA server 31 of the selected visited operator shop 3.1, 3.2 to route the AAA requests to the home AAA server 31h of the user, based on the realm part of the NAI that the terminal supplies and indicates the realm of the user's home operator shop.

[0246] Hence, methods and procedures as described herein allow a user/terminal 15, 15' that accesses a broadband

access network 29 to select an operator shop out of multiple operator shops 3.1, 3.2 connected to the broadband access network. This is possible for users accessing their home broadband access networks as well as for users roaming in foreign broadband access networks.

[0247] Both layer 2 and layer 3 methods are provided in order to cope with a variety of access scenarios, including accessing the broadband access network 29 through a dedicated RG port, a non-dedicated RG port, a home WLAN AP, a home NAT, and a public WLAN AP, provided by the broadband access network.

[0248] Hence, the methods and procedures as described herein and the accordingly modified components in a broadband access network as described herein are parts of a multi-operator (shop) mobile broadband access network environment.

[0249] Methods and associated devices/nodes have been described for supporting users, both in home and foreign broadband access networks, in a broadband access network context with multiple operator shops. Two main areas are identified:

- Layer 2 methods that are used to associate a user/terminal with the service VLAN of a selected operator shop. Mechanisms used for users roaming in foreign broadband access networks may be particularly important.
- Layer 3 methods using IPsec tunnels that are handled internally in the BRAS. DHCP may be used to inform terminals about available potential tunnel endpoints.

[0250] The specific division and assigning of method steps to different components as described have been used for illustration purposes, in order to provide a clear and understandable description and claiming of the invention.

[0251] Therefore, the invention in its broader aspects is not limited to the specific details, representative devices and illustrated examples shown and described herein.

Claims

1. An access node (13) adapted to be connected in an Ethernet type network between an access point (1) of user devices (15, 15') and a broadband remote access server (17) for providing broadband access to a plurality of service providing networks (3.1, 3.2), the access node including

   - a handling unit for handling virtual local area networks, the handling unit including a memory,
   the access node being **characterized in that**
   - the access node has a first virtual local area network function for implementing a first virtual local area network (43) including the access node and a local virtual router function unit (49) of the broadband remote access server,
   - for each one of said plurality of service providing networks, the access node has a second virtual local area network function, each second virtual local area network function being for implementing a respective second virtual local area network (41.1, 41.2) including the access node and a respective one of dedicated virtual router function units (47.1, 47.2) of the broadband remote access server, the respective one of the dedicate virtual router function units being for communication with the respective one of said plurality of service providing networks, the respective dedicated virtual router function unit being adapted to directly transfer Ethernet frames from and to a broadband access server (19) of the respective one of the service providing networks,
   - the memory stores identifications of Ethernet frames transmitted in

     -- the first virtual local area network and
     -- the second virtual local area networks, and

   - the access node comprises a control unit connected to the handling unit, the control unit being

     - - for commanding the handling unit to transmit frames from a new user device that has connected itself to the access point into the first virtual local area network,
     - - for receiving information from the broadband remote access server in respect of routing of frames, and
     -- for commanding the handling unit to transmit frames from a user device which is connected to the access point into one of the second virtual local area networks as given by information received from the broadband remote access server, instead of into the first virtual local area network, the frames thereby being transmitted to the broadband access server of the respective service providing network.

2. An access node according to claim 1, wherein the control unit is adapted to receive information including a Medium Access Control, MAC, address of the user device connected to the access point and to command the handling unit

Samsung Ex. 1004, Page 339 of 563

to transmit frames from this address into said one of the second virtual local area networks.

3. An access node according to claim 2, wherein the MAC address is a Virtual MAC address and that the access node includes a translating unit for translating the virtual MAC address into a MAC address of the user device.

4. A method for a user device (15, 15') to connect to one of a plurality of service providing networks (3.1, 3.2) through a broadband access network (29), the method including the following steps :

- the user device connects to the broadband access network,
- an access node (13) receives a frame or frames sent from the user device and forwards the frame or frames into a first virtual local area network (43),
- a local virtual router function unit (49) receives the frame or frames received in the first virtual local area network,

the method being **characterized in that** the method further comprises the following steps:

- the local virtual router function unit starts an identification and authentication procedure for the user device,
- the user device sends in the identification and authentication procedure selection information indicating one of the plurality of service providing networks,
- after a successful identification and authentication procedure the access node receives an instruction from a broadband remote access server (17) to associate an address of the user device with one of second virtual local area networks (41.1, 41.2), each of said virtual local area networks including the access node and one of dedicated virtual router function units (47.1, 47.2) of the broadband remote access server, said one of dedicated virtual router function units corresponding to the selection information, and based on said instruction, forwards frames received from the user device into said one of second virtual local area networks instead of into the first virtual local area network, each of said virtual router function units being adapted to directly transfer Ethernet frames from and to a broadband access server (19) of a respective one of the service providing networks (3.1, 3.2), and
- the broadband remote access server forwards frames from the user device received in said one of second virtual local area networks into said respective one of the plurality of service providing networks.

5. A method according to claim 4, wherein in the step of the user device connecting to the broadband access network it connects to the access point of the broadband access network.

6. A method according to claim 4, wherein in the step of receiving the frame or frames in the first virtual local area network, the frame or frames are received by the local virtual router function unit starting the identification and authentication procedure.

7. A method according to claim 4, wherein in the identification and authentication procedure the user device starts by sending identification information including said selection information of one of the plurality of service providing networks.

8. A broadband remote access server (17) for providing, for user devices (15, 15') connected to the broadband remote access server through an access node (13) or access point (7), broadband access to a plurality of service providing networks (3.1, 3.2) different from home service providing networks of users of the user devices, the broadband remote access server including:

- a service unit for storing and providing information about said plurality of service providing networks, the broadband remote access server being **characterized in that** the broadband remote access server is adapted to:

- connect a user device to the service unit, the service unit being adapted to send to the user device information about said plurality of service providing networks,
- receive from a user device information about a selected one of said plurality of service providing networks,
- thereafter forward information about a selected one of said plurality of service providing networks, as received from the user device, to said selected one of the service providing networks,
- thereafter pass authentication information between said selected one of said plurality of service providing networks and the user device,
- thereafter receive information, about the success or lack of success of the authentication procedure, and
- finally, using the received information, when indicating success, to route data, from the user device towards

said selected one of the plurality of service providing networks and to route data from said selected one of the plurality of service providing networks to the user device,
wherein the broadband remote access server includes
- a local virtual router function unit (49),
wherein the broadband remote access server is adapted to include the local virtual router function unit in a first virtual local area network (43) also including the access node or access point, and
- dedicated virtual router function units (47.1, 47.2), wherein each dedicated virtual router function unit is adapted to communicate with a corresponding one of a plurality of second virtual local area networks (41.1, 41.2), each of said second virtual local area networks including said access node or access point,

each of said dedicated virtual router function units being adapted to directly transfer data, from the respective one of the service providing networks to said access node or access point, and from said access node or access point to the respective one of the service providing networks, the broadband remote access server being adapted, to provide a command to said access node or access point,
said command instructing the access node or access point to send data from the user device into that one of second virtual local area networks in which there is a virtual router function unit associated with the selected one of the service providing networks, and to send to the user device data from the one of second virtual local area networks in which there is a virtual router function unit associated with the selected one of the service providing networks,
thereby routing data from the user device towards said selected one of the plurality of service providing networks and routing data from said selected one of the plurality of service providing networks to the user device.

9. A broadband remote access server according to claim 8, wherein the broadband remote access server further includes:

- an authentication arrangement including an authentication client (23) and an authentication server (27), wherein the local virtual router function unit is arranged, when receiving data from a previously unconnected user device, to initiate an identifying procedure with the user device and to forward a response received from the user device to the authentication arrangement, wherein the authentication arrangement is arranged to compare, when receiving a forwarded response from the user device, information in the response to stored information about said service providing networks, and

wherein the service unit is arranged, in a case where the result of the comparison is that the user device or the user of the user device has no agreement with any of the service providing networks to connect to them, to transfer said information about said service providing networks to the user device.

10. A broadband remote access server according to claim 9, adapted to pass to a dynamic host configuration protocol, DHCP server, messages from the user device,
to pass a message from the DHCP server assigning an address to the user device,
using the assigned address, to connect the user device to the service unit, and
using the assigned address, to transfer from the service unit to the user device said information about said service providing networks.

11. A broadband remote access server according to claim 10, arranged, after receiving from the user device information about a selected one of the service providing networks, to cancel said address and to initiate an authentication procedure with the user device.

Patentansprüche

1. Zugangsknoten (13), der angepasst ist, um in einem Ethernettyp-Netzwerk zwischen einem Zugangspunkt (1) von Benutzervorrichtungen (15, 15') und einem Breitband-Fernzugangsserver (17) verbunden zu sein zum Bereitstellen von Breitbandzugang für eine Mehrzahl von Dienst bereitstellenden Netzwerken (3.1, 3.2), wobei der Zugangsknoten aufweist

- eine Handhabungseinheit zum Handhaben von virtuellen lokalen Netzwerken, wobei die Handhabungseinheit einen Speicher aufweist,

Samsung Ex. 1004, Page 341 of 563

wobei der Zugangsknoten **dadurch gekennzeichnet ist, dass**

- der Zugangsknoten eine erste virtuelle lokale Netzwerkfunktion zum Implementieren eines ersten virtuellen lokalen Netzwerks (43) aufweist, das den Zugangsknoten und eine lokale virtuelle Router-Funktionseinheit (49) des Breitband-Fernzugangsservers aufweist,
- für jedes einzelne der Mehrzahl von Dienst bereitstellenden Netzwerken, der Zugangsknoten eine zweite virtuelle lokale Netzwerkfunktion aufweist, wobei jede zweite virtuelle lokale Netzwerkfunktion dem Implementieren eines entsprechenden zweiten virtuellen lokalen Netzwerks (41.1, 41.2) dient, das den Zugangsknoten und eine entsprechende von zugeordneten virtuellen Router-Funktionseinheiten (47.1, 47.2) des Breitband-Fernzugangsservers aufweist, wobei die entsprechende der zugeordneten virtuellen Router-Funktionseinheiten der Kommunikation mit dem entsprechenden von der Mehrzahl von Dienst bereitstellenden Netzwerken dient, wobei die entsprechende zugeordnete virtuelle Router-Funktionseinheit angepasst ist, um Ethernet-Rahmen direkt von und zu einem Breitband-Zugangsserver (19) des entsprechenden der Dienst bereitstellenden Netzwerke zu übertragen,
- der Speicher Identifizierungen von Ethernet-Rahmen speichert, die in

  -- dem ersten virtuellen lokalen Netzwerk und
  -- den zweiten virtuellen lokalen Netzwerken übertragen werden,

und
- der Zugangsknoten eine mit der Handhabungseinheit verbundene Steuereinheit umfasst,

wobei die Steuereinheit vorgesehen ist, zum

-- Befehlen der Handhabungseinheit, Rahmen von einer neuen Benutzervorrichtung, die sich selbst mit dem Zugangspunkt verbunden hat, in das erste virtuelle lokale Netzwerk zu übertragen,
-- Empfangen von Information von dem Breitband-Fernzugangsserver in Bezug auf ein Routen von Rahmen, und
-- Befehlen der Handhabungseinheit, Rahmen von einer Benutzervorrichtung, die mit dem Zugangspunkt verbunden ist, anstelle von in das erste virtuelle lokale Netzwerk in eines der zweiten virtuellen lokalen Netzwerke zu übertragen, wie durch von dem Breitband-Fernzugangsserver erhaltene Information angegeben wird, wobei die Rahmen dadurch zu dem Breitband-Zugangsserver des entsprechenden Dienst bereitstellenden Netzwerks übertragen werden.

2. Zugangsknoten nach Anspruch 1, wobei die Steuereinheit angepasst ist, um Information zu empfangen, die eine Medium Access Control, MAC, Adresse eines mit dem Zugangspunkt verbundenen Benutzervorrichtung aufweist, und um der Handhabungseinheit zu befehlen, Rahmen von dieser Adresse in das eine der zweiten virtuellen lokalen Netzwerke zu übertragen.

3. Zugangsknoten nach Anspruch 2, wobei die MAC-Adresse eine virtuelle MAC-Adresse ist und der Zugangsknoten eine Übersetzungseinheit zum Übersetzen der virtuellen MAC-Adresse in eine MAC-Adresse der Benutzervorrichtung aufweist.

4. Verfahren für eine Benutzervorrichtung (15, 15'), zum Verbinden mit einem von einer Mehrzahl von Dienst bereitstellenden Netzwerken (3.1, 3.2) durch ein Breitband-Zugangsnetzwerk (29), wobei das Verfahren die folgenden Schritte aufweist:

- die Benutzervorrichtung verbindet mit dem Breitband-Zugangsnetzwerk,
- ein Zugangsknoten (13) empfängt einen Rahmen oder mehrere Rahmen von der Benutzervorrichtung und leitet den Rahmen oder die Rahmen in ein erstes virtuelles lokales Netzwerk (43) weiter,
- eine lokale virtuelle Router-Funktionseinheit (49) empfängt den Rahmen oder die Rahmen, die in dem ersten virtuellen lokalen Netzwerk empfangen wurden,
- wobei das Verfahren **dadurch gekennzeichnet ist, dass** das Verfahren weiter die folgenden Schritte umfasst:
- die lokale virtuelle Router-Funktionseinheit beginnt einen Identifizierungs- und Authentifizierungsvorgang für die Benutzervorrichtung,
- die Benutzervorrichtung sendet in dem Identifizierungs- und Authentifizierungsvorgang Auswahlinformation, die eines von einer Mehrzahl von Dienst bereitstellenden Netzwerken anzeigt,
- nach einem erfolgreichen Identifizierungs- und Authentifizierungsvorgang empfängt der Zugangsknoten eine Anweisung von einem Breitband-Fernzugangsserver (17), um eine Adresse der Benutzervorrichtung einem der

Samsung Ex. 1004, Page 342 of 563

zweiten virtuellen lokalen Netzwerke (41.1, 41.2) zuzuordnen, wobei jedes der virtuellen lokalen Netzwerke den Zugangsknoten und eine von zugeordneten virtuellen Router-Funktionseinheiten (47.1, 47.2) des Breitband-Fernzugangsservers aufweist, wobei die eine der zugeordneten virtuellen Router-Funktionseinheiten der Auswahlinformation entspricht, und basierend auf der Anweisung die von der Benutzervorrichtung empfangenen Rahmen in das eine der zweiten virtuellen lokalen Netzwerke weiterleitet anstelle von in das erste virtuelle lokale Netzwerk, wobei jede der virtuellen Router-Funktionseinheiten angepasst ist, um Ethernet-Rahmen direkt von und zu einem Breitband-Zugangsserver (19) eines entsprechenden von den Dienst bereitstellenden Netzwerken (3.1, 3.2) zu übertragen, und

- der Breitband-Fernzugangsserver leitet Rahmen von der Benutzervorrichtung, die in dem einen der zweiten virtuellen lokalen Netzwerke empfangen wurden, in das entsprechende eine von der Mehrzahl von Dienst bereitstellenden Netzwerken weiter.

5. Verfahren nach Anspruch 4, wobei in dem Schritt, in dem die Benutzervorrichtung mit dem Breitband-Zugangsnetzwerk verbindet, diese mit dem Zugangspunkt des Breitband-Zugangsnetzwerks verbindet.

6. Verfahren nach Anspruch 4, wobei in dem Schritt, in dem der Rahmen oder die Rahmen in dem ersten virtuellen lokalen Netzwerk empfangen werden, der Rahmen oder die Rahmen von der lokalen virtuellen Router-Funktionseinheit, die den Identifizierungs- und Authentifizierungsvorgang beginnt, empfangen werden.

7. Verfahren nach Anspruch 4, wobei bei dem Identifizierungs- und Authentifizierungsvorgang die Benutzervorrichtung durch Senden von Identifizierungsinformation, die die Auswahlinformation von einem von der Mehrzahl von Dienst bereitstellenden Netzwerken aufweist, beginnt.

8. Breitband-Fernzugangsserver (17) zum Bereitstellen, für Benutzervorrichtungen (15, 15'), die mit dem Breitband-Fernzugangsserver durch einen Zugangsknoten (13) oder einen Zugangspunkt (7) verbunden sind, von Breitbandzugang zu einer Mehrzahl von Dienst bereitstellenden Netzwerken (3.1, 3.2), die von Dienst bereitstellenden Heimnetzwerken von Benutzern der Benutzervorrichtungen verschieden sind, wobei der Breitband-Fernzugangsserver aufweist:

- eine Diensteinheit zum Speichern und Bereitstellen von Information über die Mehrzahl von Dienst bereitstellenden Netzwerken, wobei der Breitband-Fernzugangsserver **dadurch gekennzeichnet ist, dass** der Breitband-Fernzugangsserver angepasst ist, um:
- eine Benutzervorrichtung mit der Diensteinheit zu verbinden, wobei die Diensteinheit angepasst ist, um Information über die Mehrzahl von Dienst bereitstellenden Netzwerken an die Benutzervorrichtung zu senden,
- von einer Benutzervorrichtung Information über ein ausgewähltes von der Mehrzahl von Dienst bereitstellenden Netzwerken zu empfangen,
- anschließend Information über ein ausgewähltes von der Mehrzahl von Dienst bereitstellenden Netzwerken, wie von der Benutzervorrichtung empfangen, an das ausgewählte eine von den Dienst bereitstellenden Netzwerken weiterzuleiten,
- anschließend Authentifizierungsinformation zwischen dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken und der Benutzervorrichtung auszutauschen,
- anschließend Information über den Erfolg oder mangelnden Erfolg des Authentifizierungsvorgangs zu empfangen, und
- schließlich die empfangene Information zu verwenden, wenn Erfolg angezeigt wird, um Daten von der Benutzervorrichtung zu dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu routen und um Daten von dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu der Benutzervorrichtung zu routen,

wobei der Breitband-Fernzugangsserver aufweist

- eine lokale virtuelle Router-Funktionseinheit (49),

wobei der Breitband-Fernzugangsserver angepasst ist, um die lokale virtuelle Router-Funktionseinheit in einem ersten virtuellen lokalen Netzwerk (43) aufzuweisen, das auch den Zugangsknoten oder den Zugangspunkt aufweist, und

- zugeordnete virtuelle Router-Funktionseinheiten (47.1, 47.2), wobei jede zugeordnete virtuelle Router-Funktionseinheit angepasst ist, um mit einem entsprechenden einen von einer Mehrzahl von zweiten virtuellen

Samsung Ex. 1004, Page 343 of 563

lokalen Netzwerken (41.1, 41.2) zu kommunizieren, wobei jedes der zweiten virtuellen lokalen Netzwerke den Zugangsknoten oder den Zugangspunkt aufweist,

wobei jede der zugeordneten virtuellen Router-Funktionseinheiten angepasst ist, um Daten direkt von dem entsprechenden einen der Dienst bereitstellenden Netzwerke zu dem Zugangsknoten oder dem Zugangspunkt und von dem Zugangsknoten oder dem Zugangspunkt zu dem entsprechenden einen der Dienst bereitstellenden Netzwerke zu übertragen,
wobei der Breitband-Fernzugangsserver angepasst ist, um einen Befehl zu dem Zugangsknoten oder dem Zugangspunkt bereitzustellen,
wobei der Befehl den Zugangsknoten oder den Zugangspunkt anweist, Daten von der Benutzervorrichtung in das eine von zweiten virtuellen lokalen Netzwerken zu senden, in dem sich eine virtuelle Router-Funktionseinheit, die dem ausgewählten einen von den Dienst bereitstellenden Netzwerken zugeordnet ist, befindet, und Daten von dem einen von zweiten virtuellen lokalen Netzwerken, in dem sich eine virtuelle Router-Funktionseinheit, die dem ausgewählten einen von den Dienst bereitstellenden Netzwerken zugeordnet ist, befindet, zu der Benutzervorrichtung zu senden,
wodurch Daten von der Benutzervorrichtung zu dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken geroutet werden und Daten von dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu der Benutzervorrichtung geroutet werden.

9. Breitband-Fernzugangsserver nach Anspruch 8, wobei der Breitband-Fernzugangsserver weiter umfasst:

- eine Authentifizierungsanordnung, die einen Authentifizierungsklienten (23) und einen Authentifizierungsserver (27) aufweist,

wobei die lokale virtuelle Router-Funktionseinheit angeordnet ist, um, wenn Daten von einer zuvor nicht verbundenen Benutzervorrichtung empfangen werden, einen Identifizierungsvorgang mit der Benutzervorrichtung einzuleiten und eine von der Benutzervorrichtung empfangene Antwort zu der Authentifizierungsanordnung weiterzuleiten,
wobei die Authentifizierungsanordnung angeordnet ist, um, wenn eine von der Benutzervorrichtung weitergeleitete Antwort empfangen wird, Information in der Antwort mit gespeicherter Information über die Dienst bereitstellenden Netzwerke zu vergleichen, und
wobei die Diensteinheit angeordnet ist, um, in dem Fall, in dem das Ergebnis des Vergleichs das ist, das die Benutzervorrichtung oder der Benutzer der Benutzervorrichtung keine Vereinbarung mit einem von den mit ihnen verbundenen Dienst bereitstellenden Netzwerken hat, die Information über die Dienst bereitstellenden Netzwerke an die Benutzervorrichtung zu übertragen.

10. Breitband-Fernzugangsserver nach Anspruch 9, der angepasst ist, um Nachrichten von der Benutzervorrichtung an einen Dynamic Host Configuration Protocol, DHCP, Server zu übergeben, um eine Nachricht von dem DHCP-Server zu übergeben, die der Benutzervorrichtung eine Adresse zuordnet, um die zugeordnete Adresse zu verwenden, um die Benutzervorrichtung mit der Diensteinheit zu verbinden, und um die zugeordnete Adresse zu verwenden, um die Information über die Dienst bereitstellenden Netzwerke von der Diensteinheit zu der Benutzervorrichtung zu übertragen.

11. Breitband-Fernzugangsserver nach Anspruch 10, der angeordnet ist, um nach dem Empfangen, von der Benutzervorrichtung, von Informationen über ein ausgewähltes der Dienst bereitstellenden Netzwerke, die Adresse zu löschen und einen Authentifizierungsvorgang mit der Benutzervorrichtung zu starten.

Revendications

1. Noeud d'accès (13) conçu pour être connecté à un réseau de type Ethernet entre un point d'accès (1) de dispositifs utilisateur (15, 15') et un serveur d'accès distant à large bande (17) pour fournir un accès à large bande à une pluralité de réseaux fournissant des services (3.1, 3.2), le noeud d'accès incluant

- une unité de traitement pour traiter des réseaux locaux virtuels, l'unité de traitement incluant une mémoire,

le noeud d'accès étant **caractérisé en ce que**

- le noeud d'accès a une première fonction de réseau local virtuel pour mettre en oeuvre un premier réseau

Samsung Ex. 1004, Page 344 of 563

local virtuel (43) incluant le noeud d'accès et une unité faisant fonction de routeur virtuel local (49) du serveur d'accès distant à large bande,
- pour chacun de ladite pluralité de réseaux fournissant des services, le noeud d'accès a une seconde fonction de réseau local virtuel, chaque seconde fonction de réseau local virtuel servant à mettre en oeuvre un second réseau local virtuel respectif (41.1, 41.2) incluant le noeud d'accès et une unité respective d'unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2) du serveur d'accès distant à large bande, l'unité respective des unités faisant fonction de routeurs virtuels dédiés servant à la communication avec le réseau respectif de ladite pluralité de réseaux fournissant des services, l'unité faisant fonction de routeur virtuel dédié respective étant conçue pour transférer directement des trames Ethernet en provenance et vers un serveur d'accès à large bande (19) du réseau respectif des réseaux fournissant des services,
- la mémoire stocke des identifications de trames Ethernet transmises dans

-- le premier réseau local virtuel, et
-- les seconds réseaux locaux virtuels,

et
- le noeud d'accès comprend une unité de commande connectée à l'unité de traitement,

l'unité de commande servant à

-- commander l'unité de traitement pour transmettre des trames depuis un nouveau dispositif utilisateur qui s'est connecté au point d'accès dans le premier réseau local virtuel,
-- recevoir des informations à partir du serveur d'accès distant à large bande en ce qui concerne l'acheminement de trames,
et
-- commander l'unité de traitement pour transmettre des trames depuis un dispositif utilisateur qui est connecté au point d'accès dans un des seconds réseaux locaux virtuels comme donné par des informations reçues en provenance du serveur d'accès distant à large bande, au lieu du premier réseau local virtuel, les trames étant de ce fait transmises au serveur d'accès à large bande du réseau respectif fournissant des services.

2. Noeud d'accès selon la revendication 1, dans lequel l'unité de commande est conçue pour recevoir des informations incluant une adresse de Commande d'Accès au Support, MAC, du dispositif utilisateur connecté au point d'accès et pour commander l'unité de traitement afin de transmettre des trames en provenance de cette adresse jusque dans ledit réseau des seconds réseaux locaux virtuels.

3. Noeud d'accès selon la revendication 2, dans lequel l'adresse MAC est une adresse MAC Virtuelle et le noeud d'accès inclut une unité de translation pour faire subir une translation à l'adresse MAC virtuelle en une adresse MAC du dispositif utilisateur.

4. Procédé pour connecter un dispositif utilisateur (15, 15') à un réseau d'une pluralité de réseaux fournissant des services (3.1, 3.2) par l'intermédiaire d'un réseau d'accès à large bande (29), le procédé incluant les étapes suivantes :

- le dispositif utilisateur est connecté au réseau d'accès à large bande,
- un noeud d'accès (13) reçoit une trame ou des trames envoyées depuis le dispositif utilisateur et fait suivre la trame ou les trames jusque dans un premier réseau local virtuel (43),
- une unité faisant fonction de routeur virtuel local (49) reçoit la trame ou les trames reçues dans le premier réseau local virtuel,

le procédé étant **caractérisé en ce que** le procédé comprend en outre les étapes suivantes :

- l'unité faisant fonction de routeur virtuel local démarre une procédure d'identification et d'authentification pour le dispositif utilisateur,
- le dispositif utilisateur envoie dans la procédure d'identification et d'authentification des informations de sélection indiquant un réseau de la pluralité de réseaux fournissant des services,
- après une procédure d'identification et d'authentification couronnée de succès, le noeud d'accès reçoit une instruction en provenance d'un serveur d'accès distant à large bande (17) pour associer une adresse du dispositif utilisateur à l'un de seconds réseaux locaux virtuels (41.1, 41.2), chacun desdits réseaux locaux virtuels incluant

Samsung Ex. 1004, Page 345 of 563

le noeud d'accès et l'une desdites unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2) du serveur d'accès distant à large bande, ladite unité des unités faisant fonction de routeurs virtuels dédiés correspondant aux informations de sélection, et sur la base desdites instructions, fait suivre les trames reçues en provenance du dispositif utilisateur jusque dans ledit réseau de seconds réseaux locaux virtuels au lieu du premier réseau local virtuel, chacune desdites unités faisant fonction de routeurs virtuels étant conçue pour directement transférer des trames Ethernet en provenance et vers un serveur d'accès à large bande (19) d'un réseau respectif des réseaux fournissant des services (3.1, 3.2), et
- le serveur d'accès distant à large bande fait suivre des trames provenant du dispositif utilisateur reçues dans ledit réseau de seconds réseaux locaux virtuels dans ledit réseau respectif de la pluralité de réseaux fournissant des services.

5. Procédé selon la revendication 4, dans lequel dans l'étape du dispositif utilisateur se connectant au réseau d'accès à large bande, il se connecte au point d'accès du réseau d'accès à large bande.

6. Procédé selon la revendication 4, dans lequel, dans l'étape de réception de la trame ou des trames dans le premier réseau local virtuel, la trame ou les trames sont reçues par l'unité faisant fonction de routeur virtuel local démarrant la procédure d'identification et d'authentification.

7. Procédé selon la revendication 4, dans lequel, dans la procédure d'identification et d'authentification, le dispositif utilisateur démarre en envoyant des informations d'identification incluant lesdites informations de sélection d'un réseau de la pluralité de réseaux fournissant des services.

8. Serveur d'accès distant à large bande (17) pour fournir, pour des dispositifs utilisateur (15, 15') connectés au serveur d'accès distant à large bande par l'intermédiaire d'un noeud d'accès (13) ou point d'accès (7), un accès à large bande à une pluralité de réseaux fournissant des services (3.1, 3.2) différents de réseaux fournissant des services domestiques d'utilisateurs des dispositifs utilisateur, le serveur d'accès distant à large bande incluant :

- une unité de service pour stocker et fournir des informations concernant ladite pluralité de réseaux fournissant des services,

le serveur d'accès distant à large bande étant
caractérisé en ce que le serveur d'accès distant à large bande est conçu pour :

- connecter un dispositif utilisateur à l'unité de service, l'unité de service étant conçue pour envoyer au dispositif utilisateur des informations concernant ladite pluralité de réseaux fournissant des services,
- recevoir en provenance d'un dispositif utilisateur des informations concernant un réseau sélectionné de ladite pluralité de réseaux fournissant des services,
- après cela faire suivre des informations concernant un réseau sélectionné de ladite pluralité de réseaux fournissant des services, lorsque reçues en provenance du dispositif utilisateur, audit réseau sélectionné des réseaux fournissant des services,
- après cela faire passer des informations d'authentification entre ledit réseau sélectionné de ladite pluralité de réseaux fournissant des services et le dispositif utilisateur,
- après cela recevoir des informations, concernant le succès ou l'absence de succès de la procédure d'authentification, et
- finalement, en utilisant les informations reçues, lorsqu'elles indiquent un succès, acheminer des données, en provenance du dispositif d'utilisateur vers ledit réseau sélectionné de la pluralité de réseaux fournissant des services et acheminer des données en provenance dudit réseau sélectionné de la pluralité de réseaux fournissant des services au dispositif utilisateur,

dans lequel le serveur d'accès distant à large bande inclut

- une unité faisant fonction de routeur virtuel local (49),

dans lequel le serveur d'accès distant à large bande est conçu pour inclure l'unité faisant fonction de routeur virtuel local dans un premier réseau local virtuel (43) incluant également le noeud d'accès ou le point d'accès, et

- des unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2), dans lesquelles chaque unité faisant fonction de routeur virtuel dédié est conçue pour communiquer avec un réseau correspondant d'une pluralité de seconds

Samsung Ex. 1004, Page 346 of 563

réseaux locaux virtuels (41.1, 41.2), chacun desdits seconds réseaux locaux virtuels incluant ledit noeud d'accès ou point d'accès,

chacune desdites unités faisant fonction de routeurs virtuels dédiés étant conçue pour transférer directement des données, en provenance du réseau respectif des réseaux fournissant des services audit noeud d'accès ou point d'accès, et en provenance dudit noeud d'accès ou point d'accès au réseau respectif des réseaux fournissant des services,
le serveur d'accès distant à large bande étant conçu pour fournir une commande audit noeud d'accès ou point d'accès, ladite commande ordonnant au noeud d'accès ou point d'accès d'envoyer des données en provenance du dispositif utilisateur dans ce réseau de seconds réseaux locaux virtuels dans lequel il y a une unité faisant fonction de routeur virtuel associée au réseau sélectionné des réseaux fournissant des services, et d'envoyer au dispositif utilisateur des données en provenance du réseau de seconds réseaux locaux virtuels dans lequel il y a une unité faisant fonction de routeur virtuel associée au réseau sélectionné des réseaux fournissant des services, acheminant de ce fait des données en provenance du dispositif utilisateur vers ledit réseau sélectionné de la pluralité de réseaux fournissant des services et en acheminant des données en provenance dudit réseau sélectionné de la pluralité de réseaux fournissant des services au dispositif utilisateur.

9. Serveur d'accès distant à large bande selon la revendication 8, dans lequel le serveur d'accès distant à large bande inclut en outre :

- un agencement d'authentification incluant un client d'authentification (23) et un serveur d'authentification (27),

dans lequel l'unité faisant fonction de routeur virtuel local est agencée, lors de la réception des données en provenance d'un dispositif utilisateur précédemment non connecté, pour amorcer une procédure d'identification avec le dispositif d'utilisateur et pour faire suivre une réponse reçue en provenance du dispositif utilisateur vers l'agencement d'authentification,
dans lequel l'agencement d'authentification est agencé pour comparer, lors de la réception d'une réponse réexpédiée en provenance du dispositif utilisateur, des informations dans la réponse à des informations stockées concernant lesdits réseaux fournissant des services, et
dans lequel l'unité de service est agencée, dans un cas où le résultat de la comparaison est que le dispositif utilisateur ou l'utilisateur du dispositif utilisateur n'a aucun accord avec l'un quelconque des réseaux fournissant des services pour se connecter à eux, pour transférer lesdites informations concernant lesdits réseaux fournissant des services au dispositif utilisateur.

10. Serveur d'accès distant à large bande selon la revendication 9, conçu pour passer à un serveur de protocole de configuration d'hôte dynamique, DHCP, des messages en provenance du dispositif utilisateur, pour passer un message en provenance du serveur DHCP attribuant une adresse au dispositif utilisateur, en utilisant l'adresse attribuée, pour connecter le dispositif utilisateur à l'unité de service, et en utilisant l'adresse attribuée, pour transférer depuis l'unité de service au dispositif utilisateur lesdites informations concernant lesdits réseaux fournissant des services.

11. Serveur d'accès distant à large bande selon la revendication 10, agencé, après réception en provenance du dispositif d'utilisateur d'informations concernant un réseau sélectionné des réseaux fournissant des services, pour annuler ladite adresse et amorcer une procédure d'authentification avec le dispositif utilisateur.

Samsung Ex. 1004, Page 347 of 563

Fig. 1a

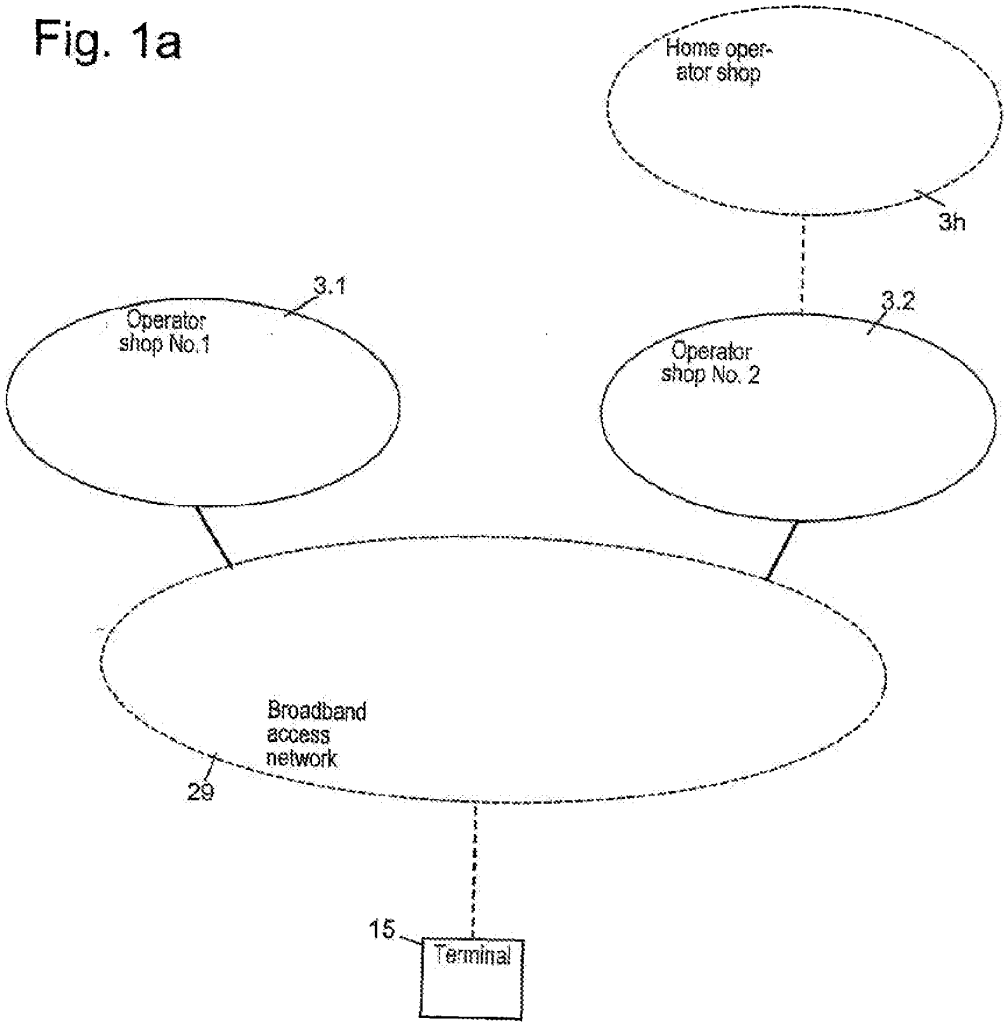

Home operator shop
3h
3.1
Operator shop No.1
3.2
Operator shop No. 2
Broadband access network
29
15
Terminal

Fig. 1b

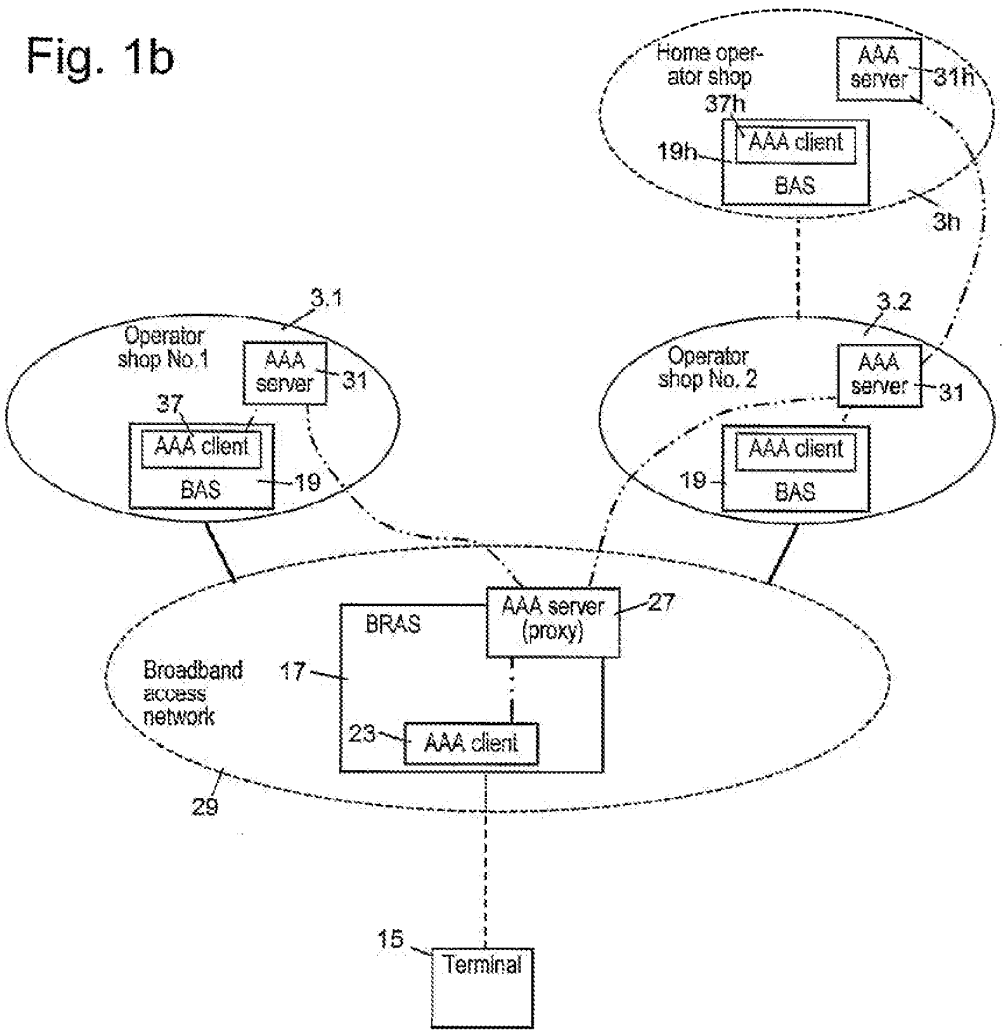

Home operator shop
37h
AAA server
31h
19h
AAA client
BAS
3h
3.1
Operator shop No.1
AAA server
31
37
AAA client
BAS
19
3.2
Operator shop No. 2
AAA server
31
AAA client
19
BAS
BRAS
AAA server (proxy)
27
Broadband access network
17
23
AAA client
29
15
Terminal

Fig. 1c

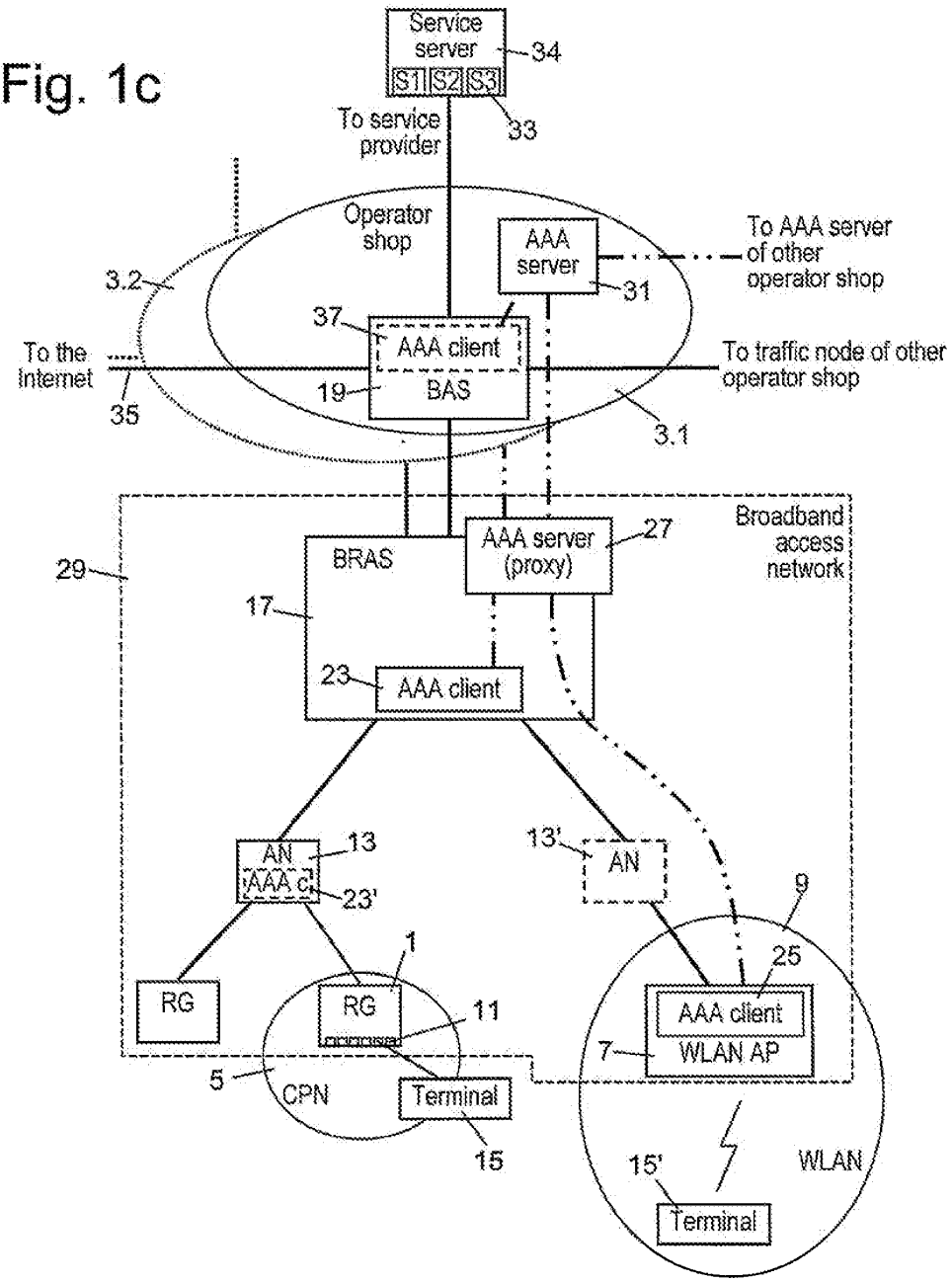
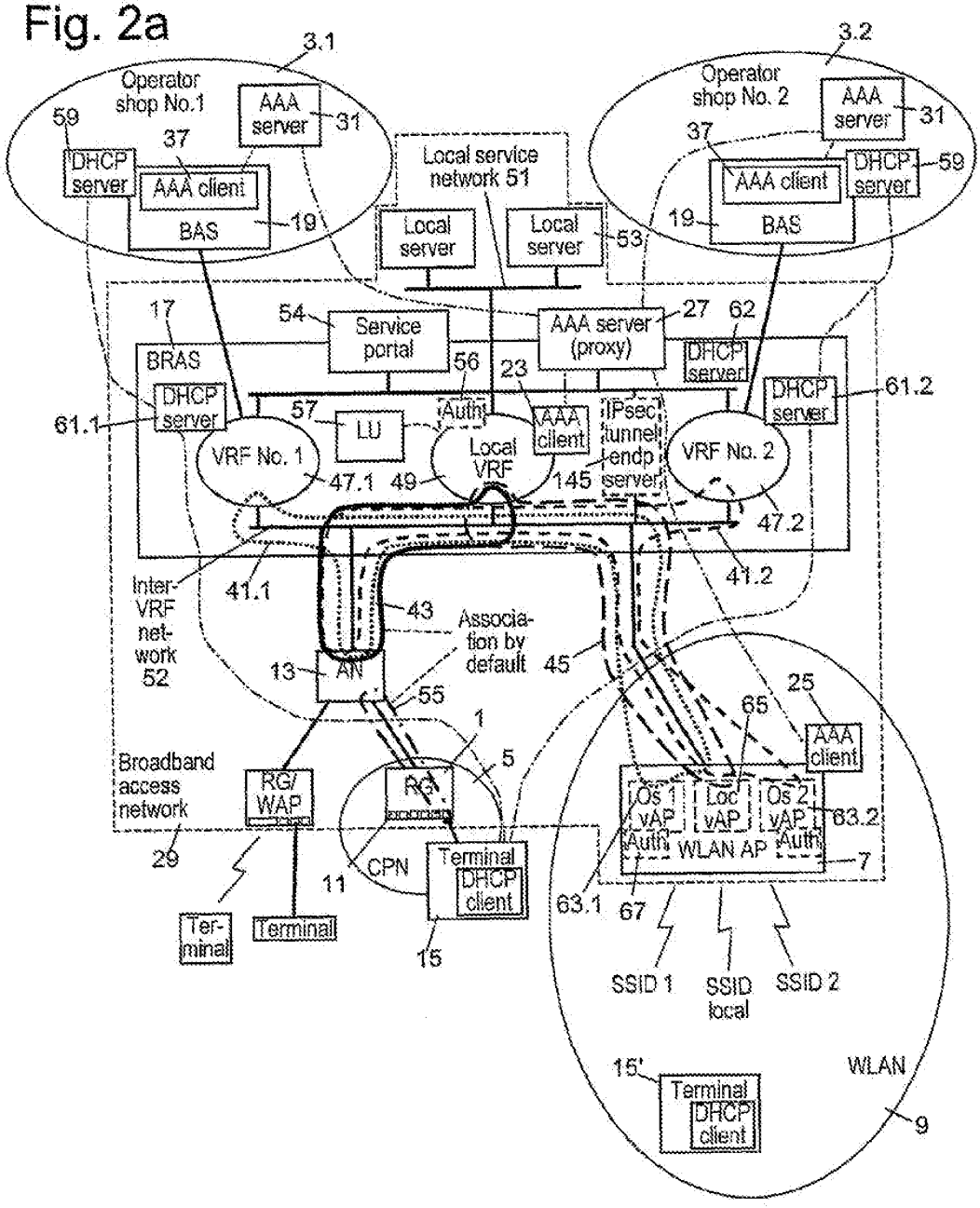

Service server
34
S1 S2 S3
33
To service provider
Operator shop
AAA server
31
To AAA server of other operator shop
3.2
37
AAA client
To the Internet
19
BAS
To traffic node of other operator shop
35
3.1
Broadband access network
29
BRAS
AAA server (proxy)
27
17
23
AAA client
AN
AAA c.
13
23'
13'
AN
9
25
1
RG
RG
11
AAA client
7
WLAN AP
5
CPN
Terminal
15
15'
WLAN
Terminal

Fig. 2a



VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2b

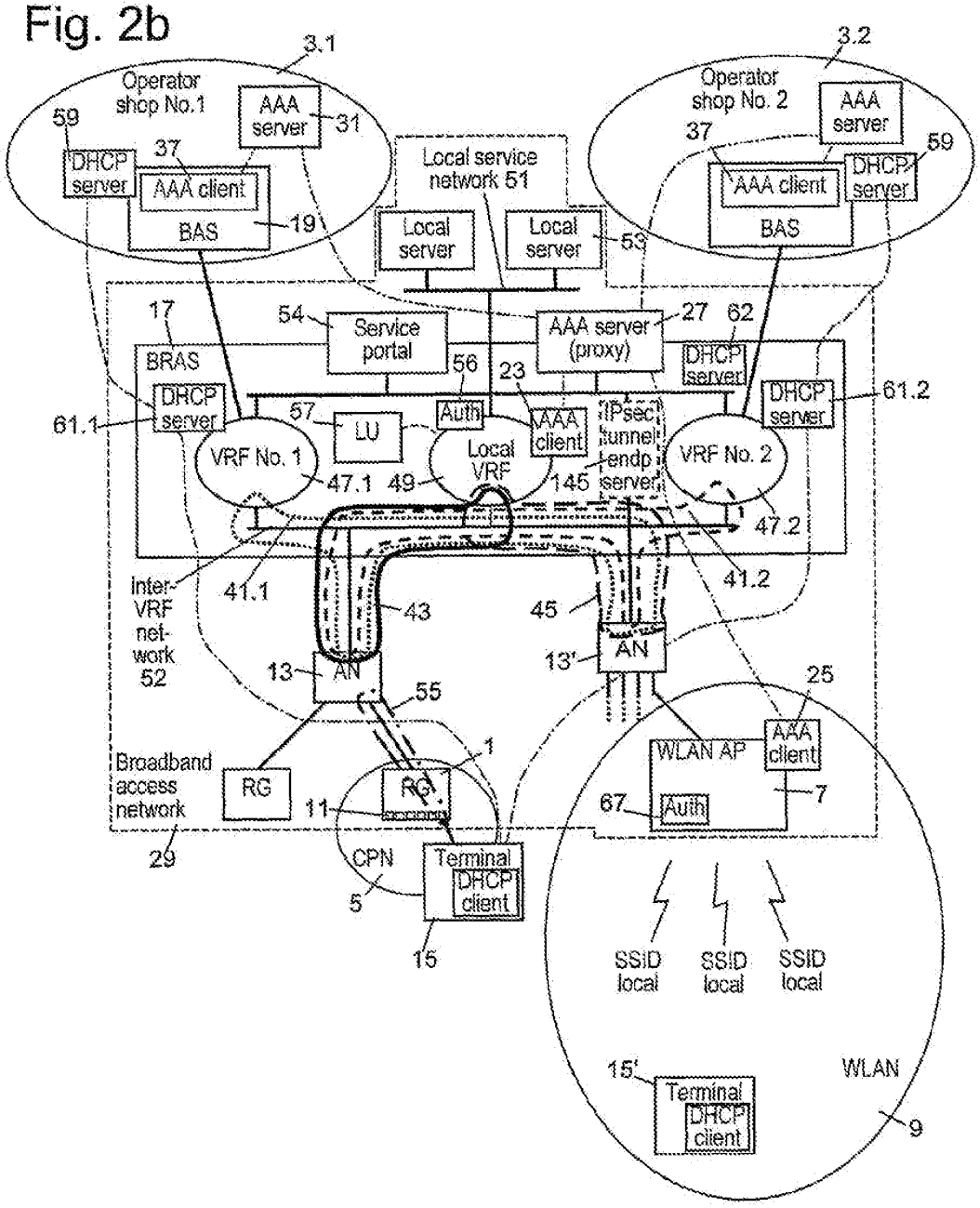

3.1
Operator shop No.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
3.2
Operator shop No. 2
AAA server
37
59
AAA client
DHCP server
BAS
Local service network 51
Local server
Local server
53
17
BRAS
DHCP server
61.1
54
Service portal
56
AAA server (proxy)
27
62
DHCP server
23
DHCP server
61.2
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
47.1
49
Local VRF
145
VRF No. 2
47.2
41.1
41.2
Inter-VRF net-work 52
43
45
13
AN
13'
AN
55
25
1
Broadband access network
29
RG
11
RG
WLAN AP
AAA client
7
67
Auth
CPN
5
Terminal
DHCP client
15
SSID local
SSID local
SSID local
15'
Terminal
DHCP client
WLAN
9
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2c

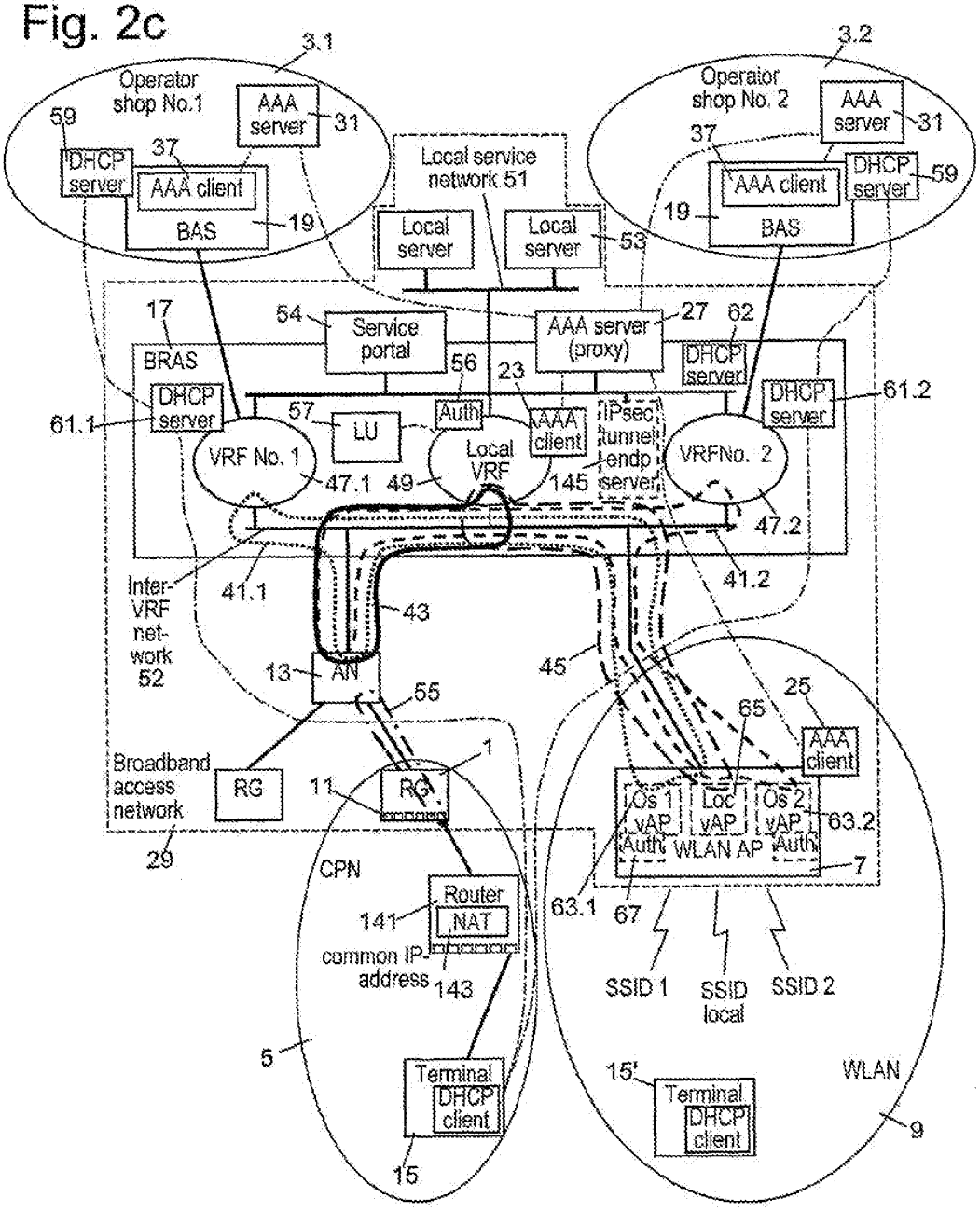
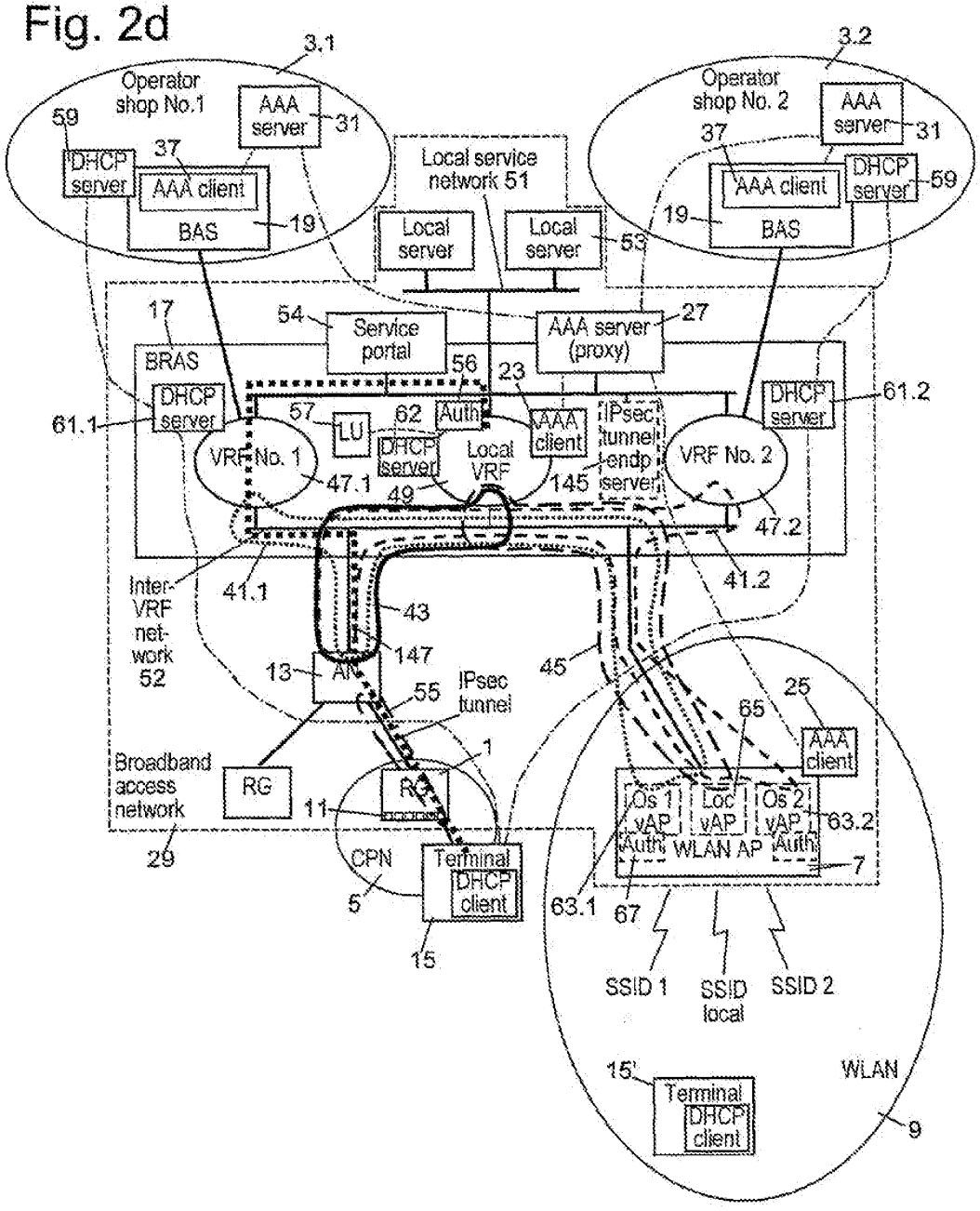
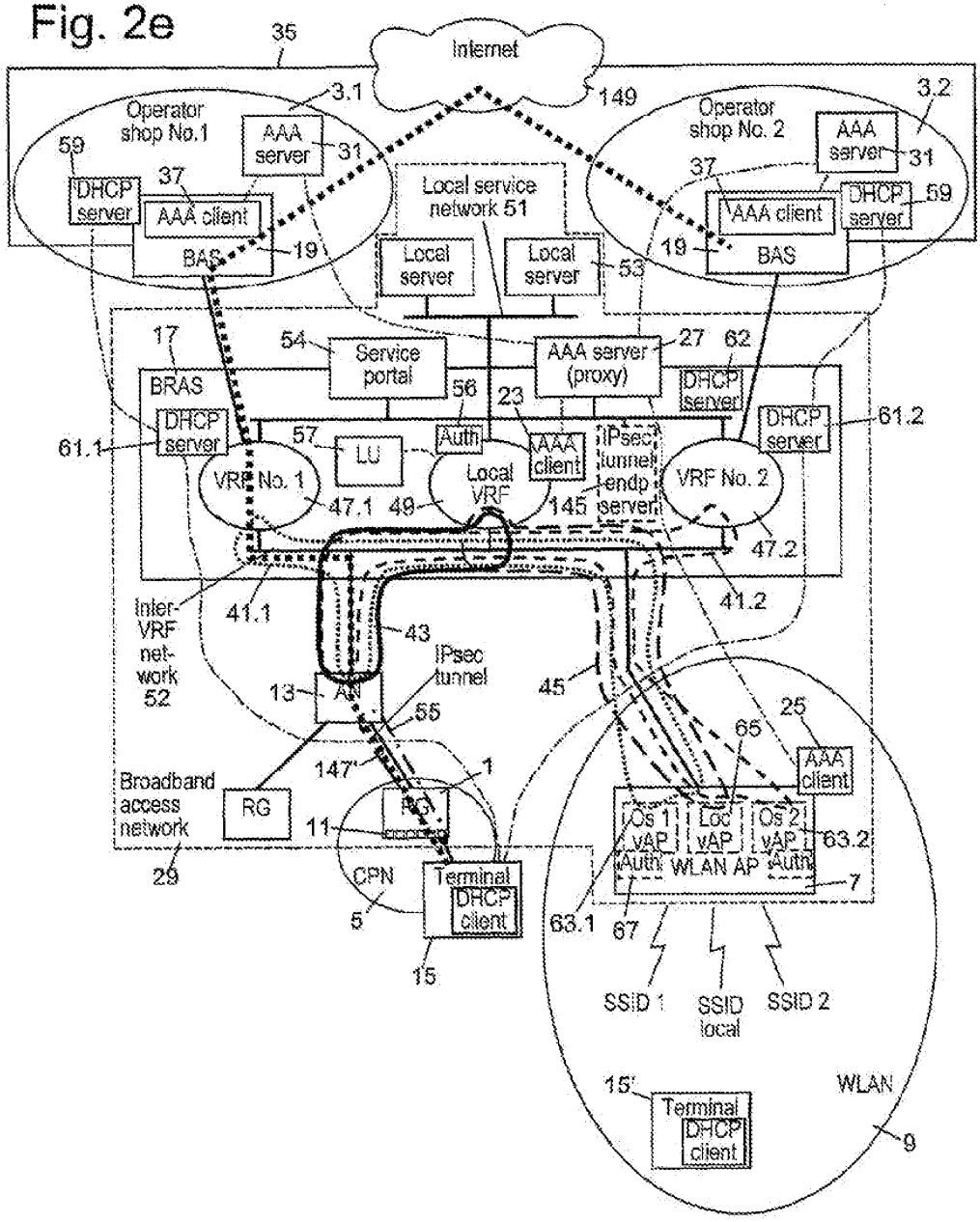

3.1
Operator shop No.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
3.2
Operator shop No. 2
AAA server
31
37
AAA client
DHCP server
59
19
BAS
Local service network 51
Local server
Local server
53
17
BRAS
54
Service portal
56
AAA server (proxy)
27
62
DHCP server
23
DHCP server
61.2
61.1
DHCP server
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
47.1
49
Local VRF
145
VRFNo. 2
47.2
41.1
41.2
Inter-VRF net-work 52
43
13
AN
55
45
25
65
AAA client
Broadband access network
29
RG
11
RG
1
CPN
Router
NAT
141
common IP address
143
5
Terminal
DHCP client
15
OS 1 vAP
Loc vAP
OS 2 vAP
63.2
Auth
WLAN AP
Auth
7
63.1
67
SSID 1
SSID local
SSID 2
15'
Terminal
DHCP client
WLAN
9
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2d



VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2e



VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2f

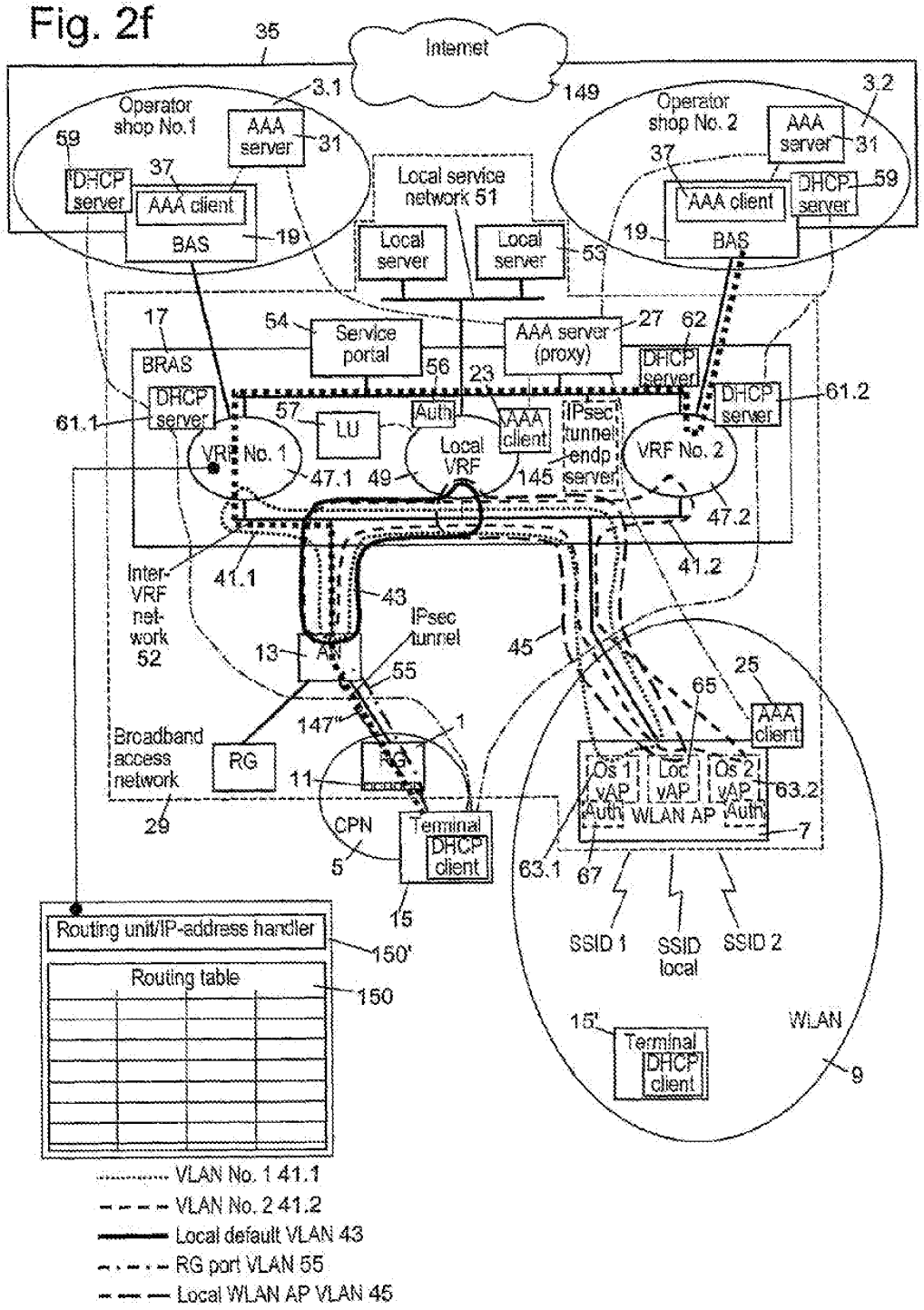
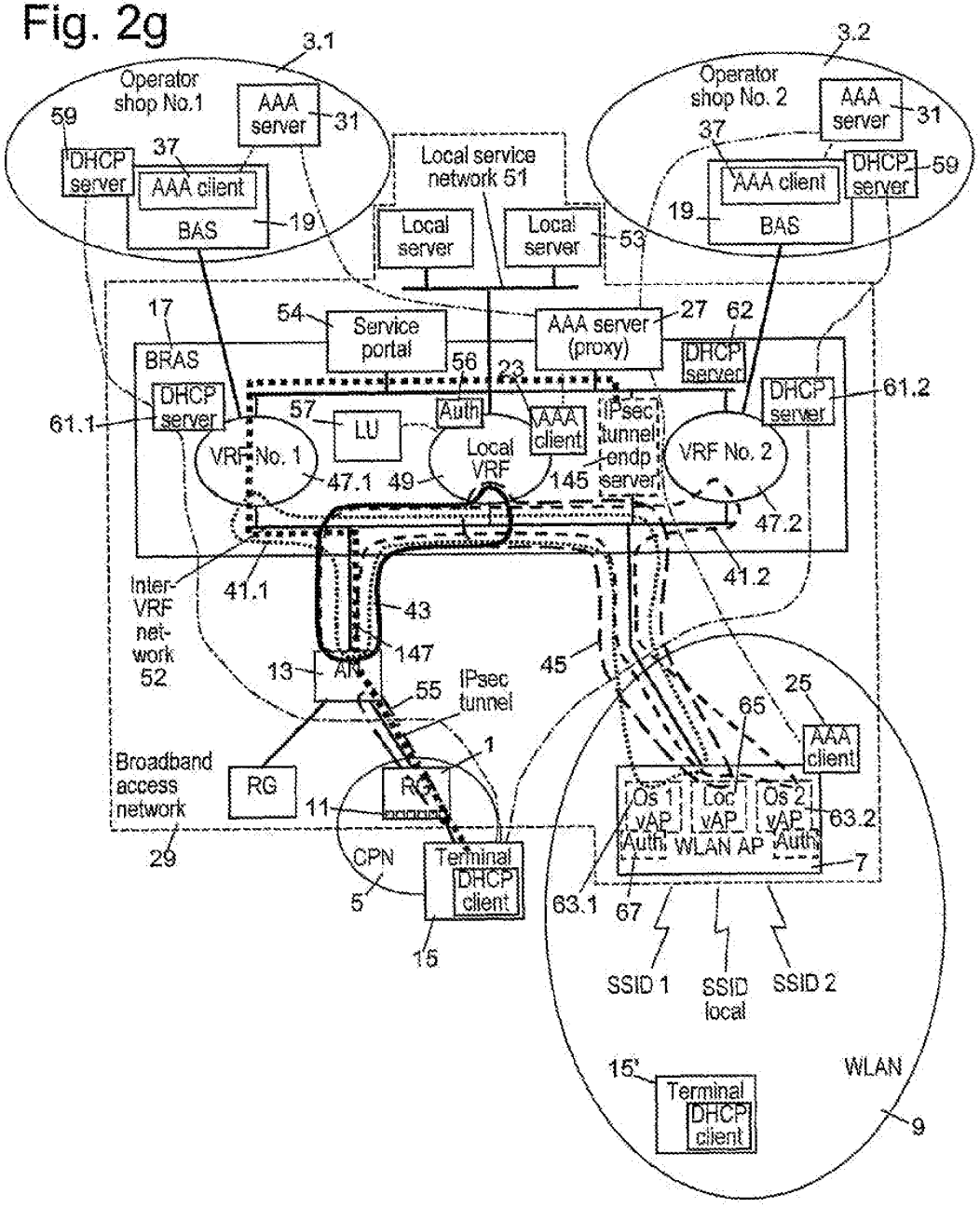

35
Internet
149
3.1
Operator shop No.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
Local service network 51
Local server
Local server
53
3.2
Operator shop No. 2
AAA server
31
37
AAA client
DHCP server
59
19
BAS
17
BRAS
54
Service portal
56
AAA server (proxy)
27
62
23
DHCP server
DHCP server
61.2
61.1
57
LU
Auth
AAA client
IPsec tunnel endp server
145
VRF No. 1
47.1
49
Local VRF
VRF No. 2
47.2
41.1
41.2
Inter-VRF net-work 52
43
IPsec tunnel
13
AS
55
45
65
25
AAA client
147'
1
Broadband access network
RG
11
RG
29
CPN
Terminal DHCP client
5
15
63.1
67
63.2
7
Os 1 vAP Auth
Loc vAP
Os 2 vAP Auth
WLAN AP
Routing unit/IP-address handler
150'
Routing table
150
SSID 1
SSID local
SSID 2
15'
Terminal DHCP client
WLAN
9
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2g



VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2h

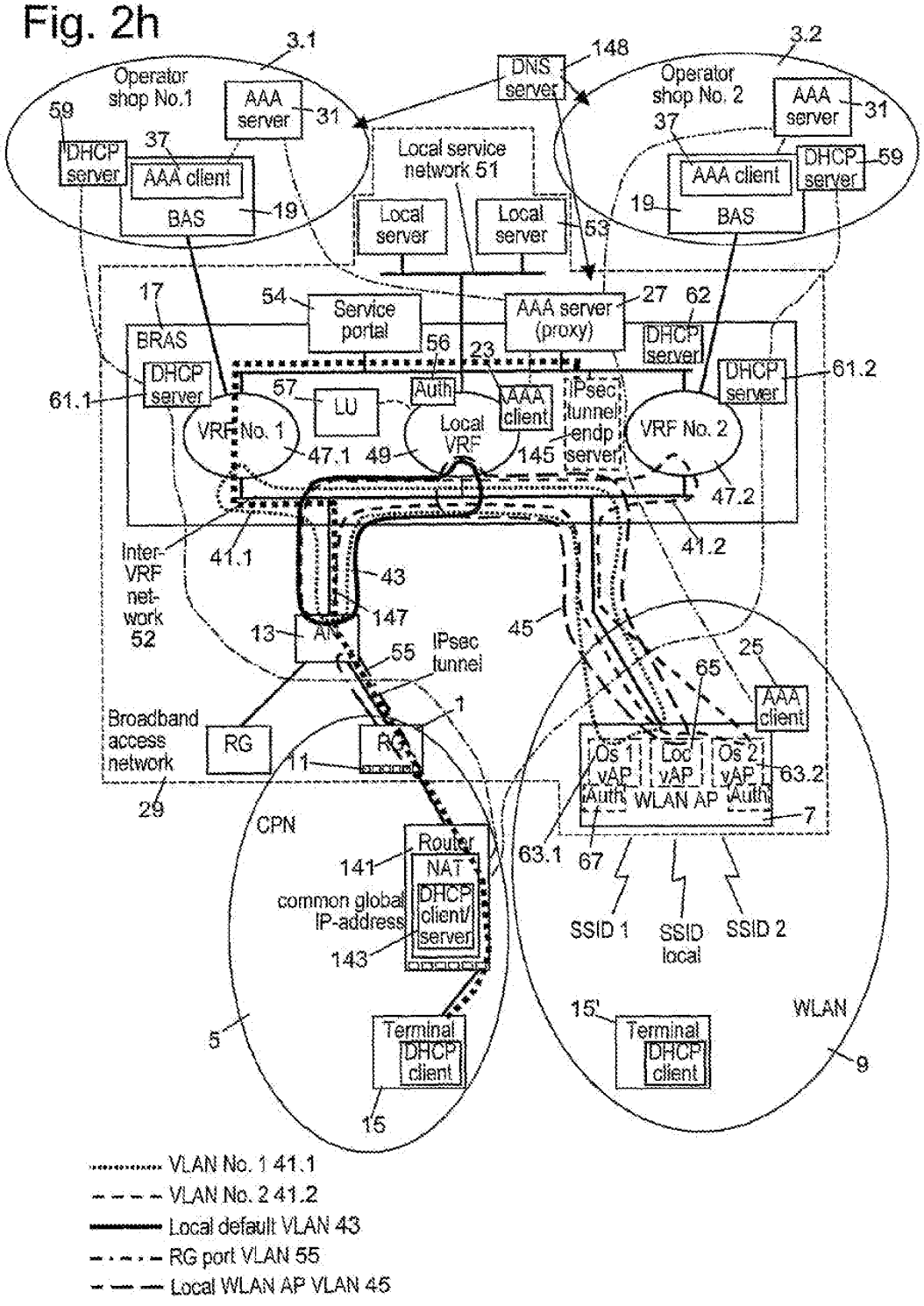

3.1
Operator shop No.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
DNS server
148
Local service network 51
Local server
Local server
53
3.2
Operator shop No. 2
AAA server
31
37
AAA client
DHCP server
59
19
BAS
17
BRAS
54
Service portal
56
23
AAA server (proxy)
27
62
DHCP server
DHCP server
61.2
61.1
DHCP server
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
47.1
49
Local VRF
145
VRF No. 2
47.2
41.1
41.2
Inter-VRF net-work 52
43
147
13
AN
55
IPsec tunnel
45
25
65
AAA client
1
Broadband access network
RG
RG
11
29
CPN
Router
NAT
DHCP client/ server
141
common global IP-address
143
OS 1 vAP
Loc vAP
OS 2 vAP
63.2
Auth
WLAN AP
Auth
7
63.1
67
SSID 1
SSID local
SSID 2
15'
WLAN
Terminal
DHCP client
5
9
Terminal
DHCP client
15
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2i

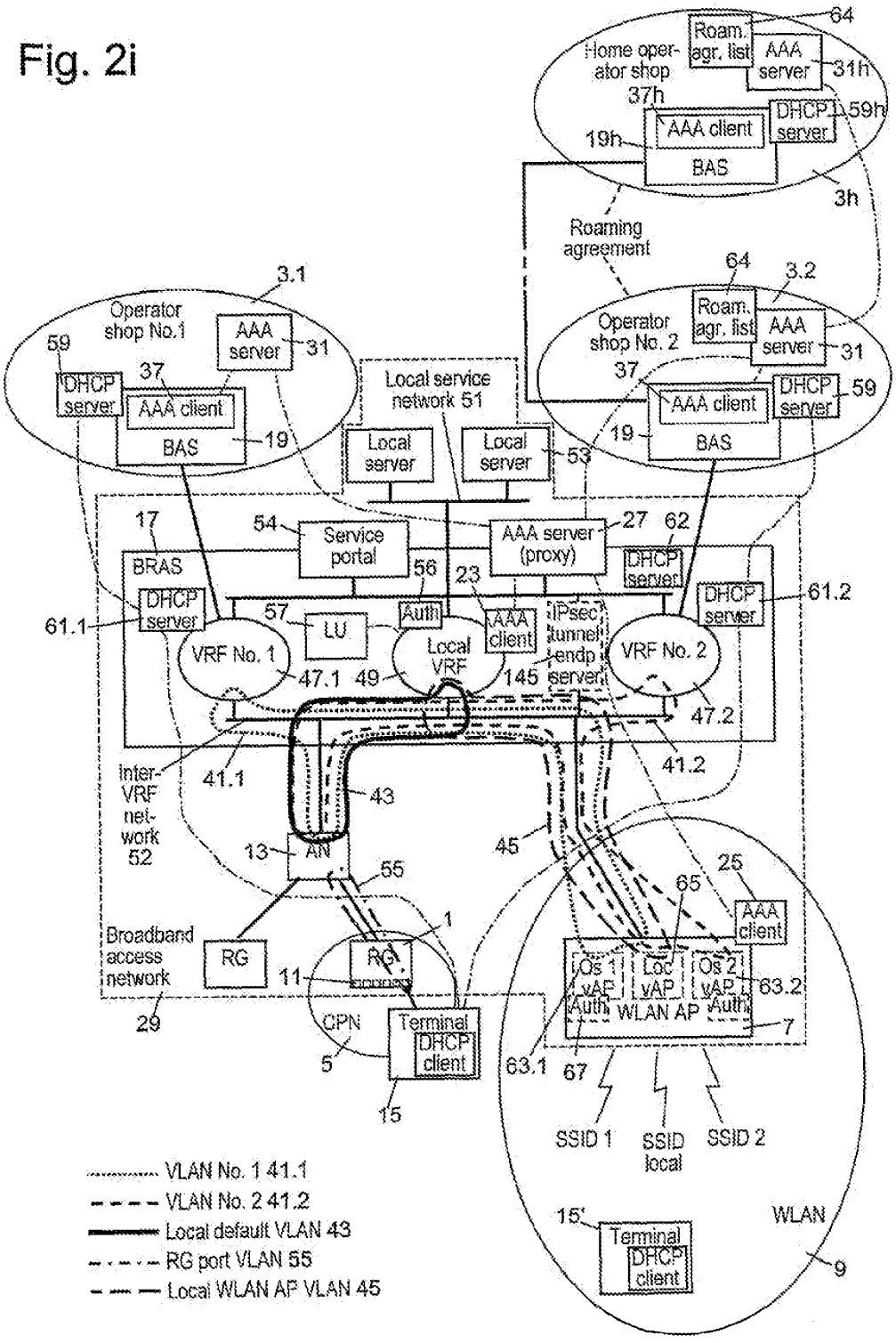

Home operator shop
37h
Roam. agr. list
AAA server
31h
64
59h
DHCP server
AAA client
19h
BAS
3h
Roaming agreement
3.1
Operator shop No.1
AAA server
31
59
37
DHCP server
AAA client
BAS
19
Local service network 51
Local server
Local server
53
64
3.2
Operator shop No. 2
Roam. agr. list
AAA server
31
37
AAA client
DHCP server
59
19
BAS
17
BRAS
54
Service portal
AAA server (proxy)
27
62
56
23
DHCP server
DHCP server
61.2
61.1
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
Local VRF
VRF No. 2
47.1
49
145
47.2
41.1
41.2
43
Inter-VRF network 52
13
AN
55
45
25
65
AAA client
Broadband access network
RG
RG
1
11
29
CPN
Terminal DHCP client
5
15
Os 1 vAP
Loc vAP
Os 2 vAP
63.2
Auth
WLAN AP
Auth
7
63.1
67
SSID 1
SSID local
SSID 2
15'
Terminal DHCP client
WLAN
9
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 2j

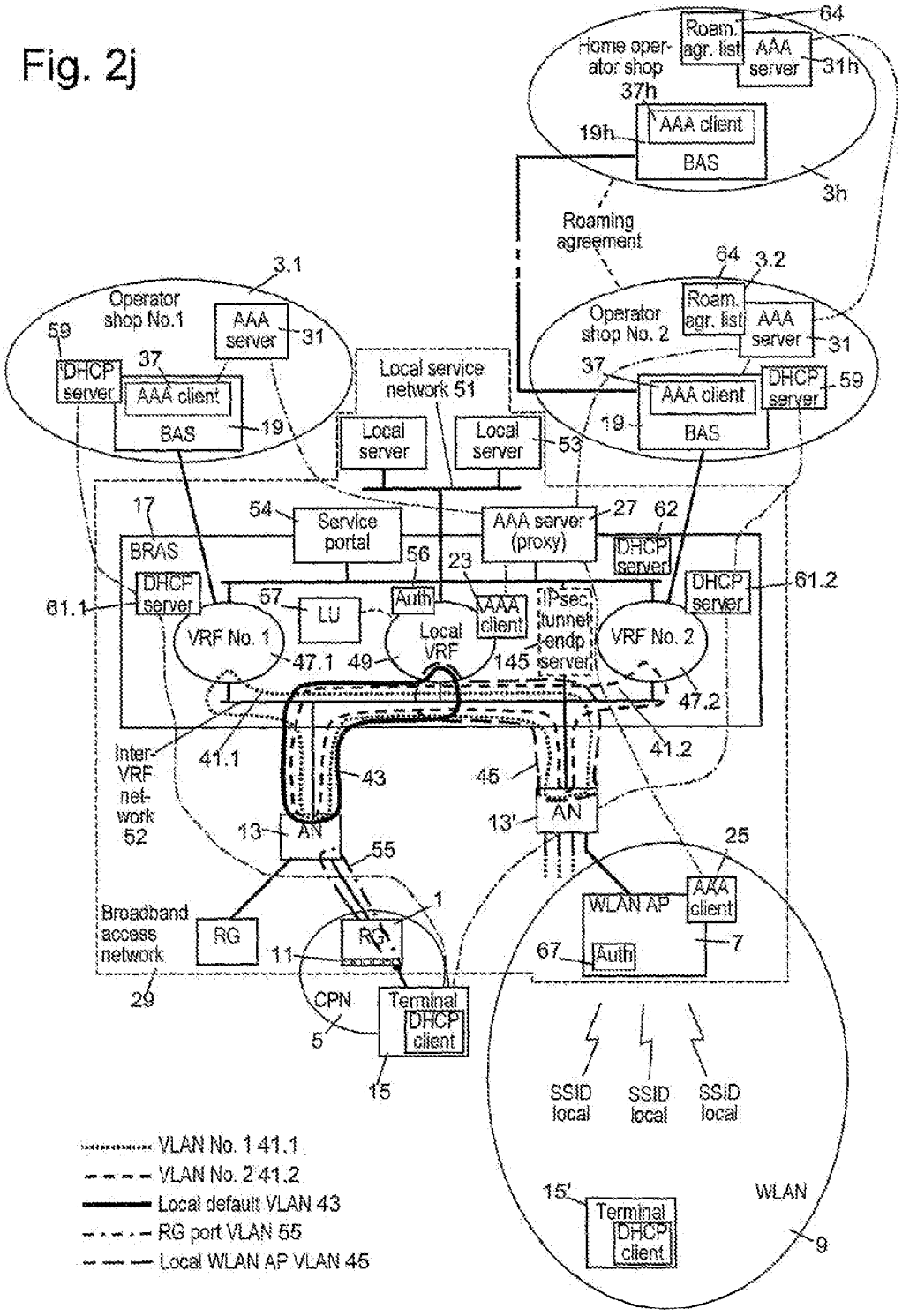

Home operator shop 37h
Roam. agr. list
AAA server
31h
64
AAA client
19h
BAS
3h
Roaming agreement
Operator shop No.1
3.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
Local service network 51
Local server
Local server
53
Operator shop No. 2
64
3.2
Roam. agr. list
AAA server
31
37
AAA client
BAS
19
DHCP server
59
17
BRAS
54
Service portal
56
AAA server (proxy)
27
62
DHCP server
23
DHCP server
61.2
61.1
DHCP server
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
47.1
49
Local VRF
145
VRF No. 2
47.2
41.1
41.2
Inter-VRF network 52
43
45
13
AN
55
13'
AN
25
Broadband access network
RG
1
RG
11
WLAN AP
AAA client
67
Auth
7
29
CPN
5
Terminal
DHCP client
15
SSID local
SSID local
SSID local
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45
15'
Terminal
DHCP client
WLAN
9

Fig. 2k

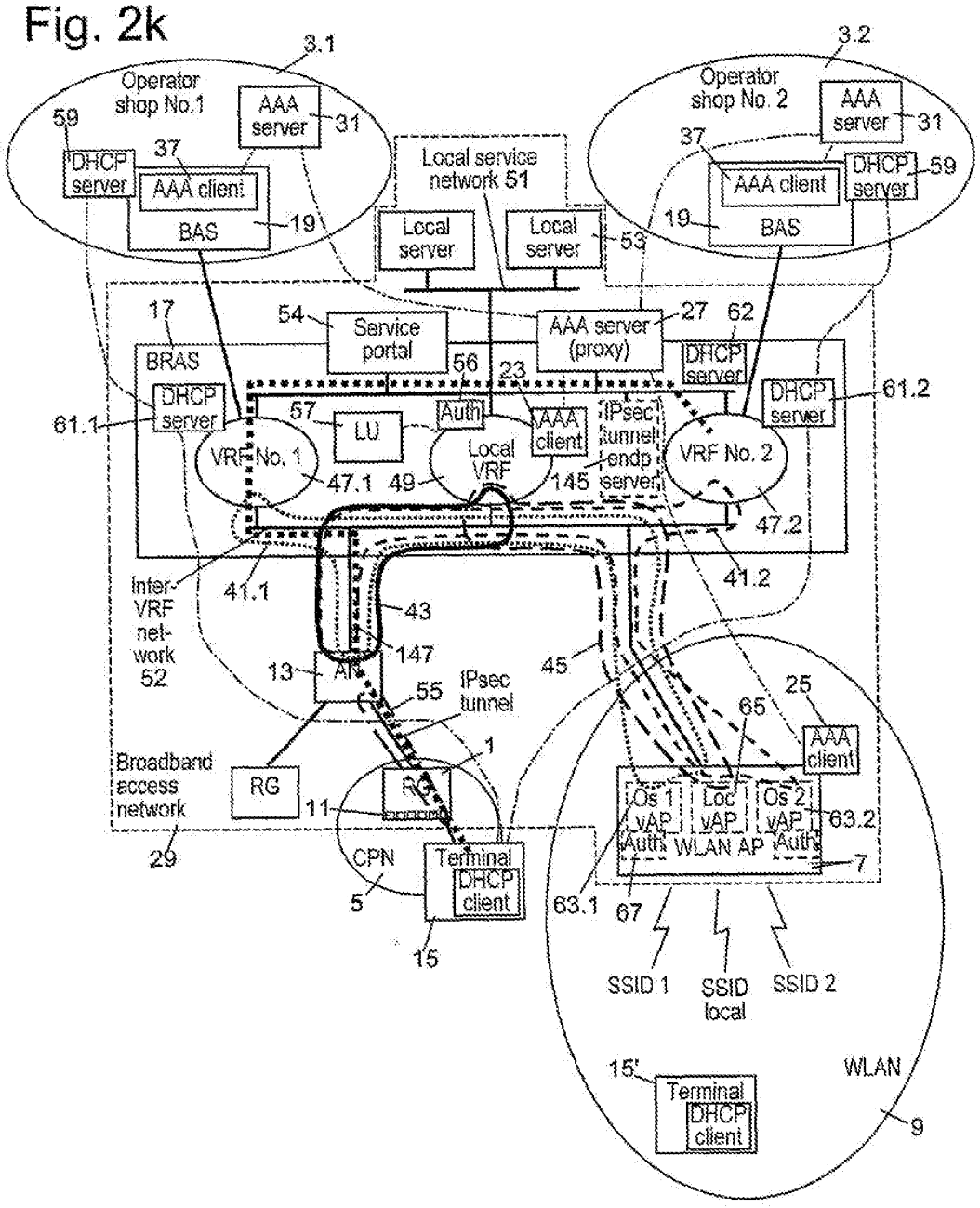

3.1
Operator shop No.1
AAA server
31
59
DHCP server
37
AAA client
BAS
19
3.2
Operator shop No. 2
Local service network 51
Local server
Local server
53
17
BRAS
54
Service portal
56
23
AAA server (proxy)
27
62
DHCP server
61.1
61.2
57
LU
Auth
AAA client
IPsec tunnel endp server
VRF No. 1
Local VRF
VRF No. 2
47.1
49
145
47.2
41.1
41.2
Inter-VRF net-work 52
43
147
13
AP
55
IPsec tunnel
45
25
65
1
Broadband access network
RG
11
29
CPN
Terminal
DHCP client
5
15
63.1
67
63.2
7
SSID 1
SSID local
SSID 2
15'
WLAN
9
VLAN No. 1 41.1
VLAN No. 2 41.2
Local default VLAN 43
RG port VLAN 55
Local WLAN AP VLAN 45

Fig. 3a

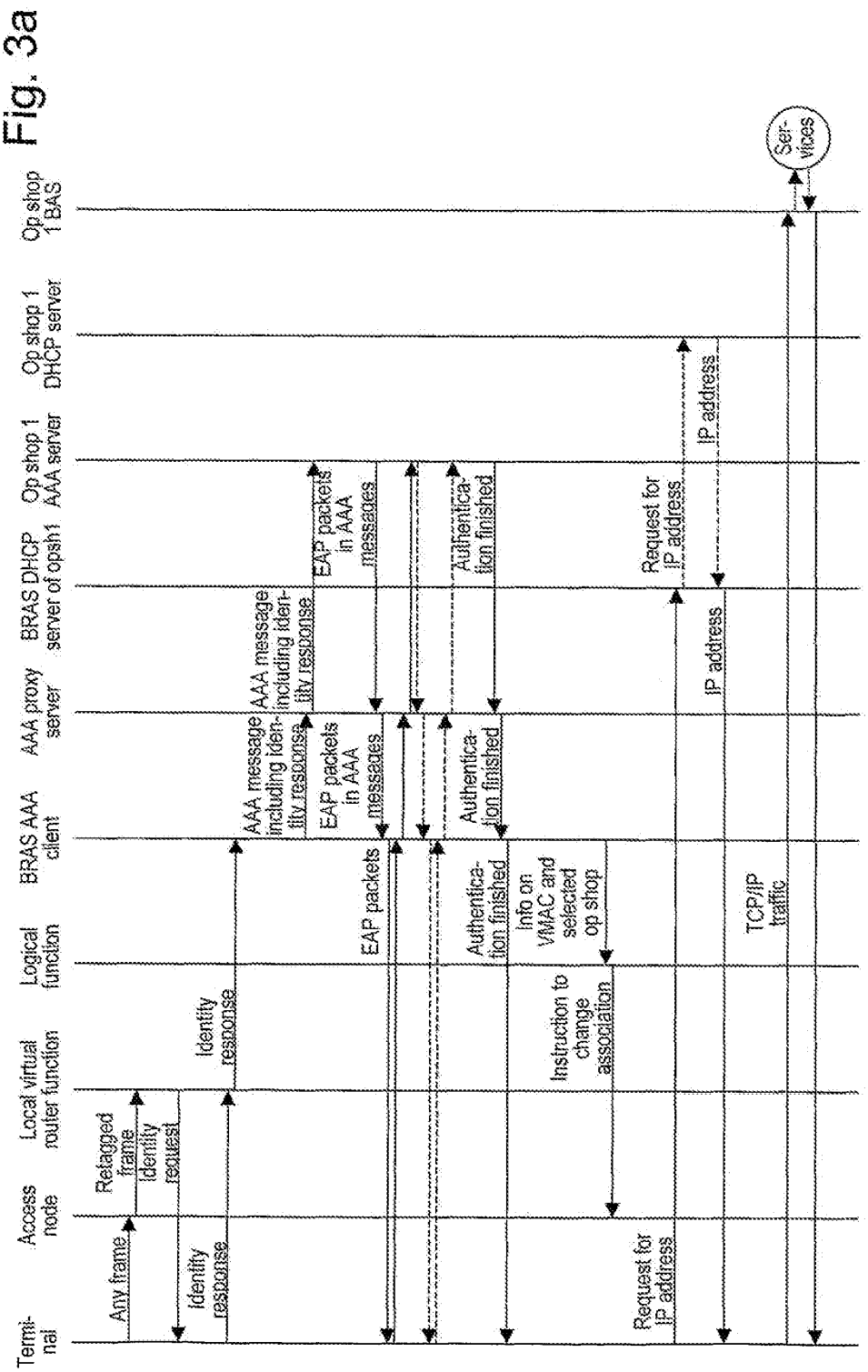

Termi-nal
Access node
Local virtual router function
Logical function
BRAS AAA client
AAA proxy server
BRAS DHCP server of opsh1
Op shop 1 AAA server
Op shop 1 DHCP server
Op shop 1 BAS
Any frame
Retagged frame identity request
Identity response
Identity response
AAA message including identity response
EAP packets in AAA messages
EAP packets
AAA message including identity response
EAP packets in AAA messages
Authentication finished
Authentication finished
Info on VMAC and selected op shop
Instruction to change association
Request for IP address
Request for IP address
IP address
IP address
TCP/IP traffic
Services

Fig. 3b

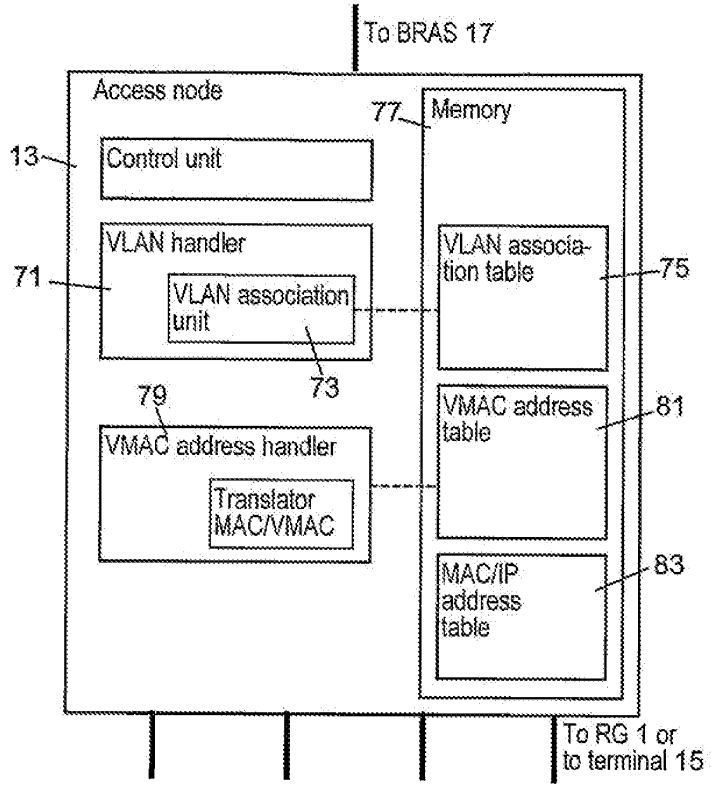

To BRAS 17
Access node
77
Memory
13
Control unit
VLAN handler
71
VLAN association unit
73
VLAN association table
75
79
VMAC address handler
Translator MAC/VMAC
VMAC address table
81
MAC/IP address table
83
To RG 1 or to terminal 15

Fig. 6b

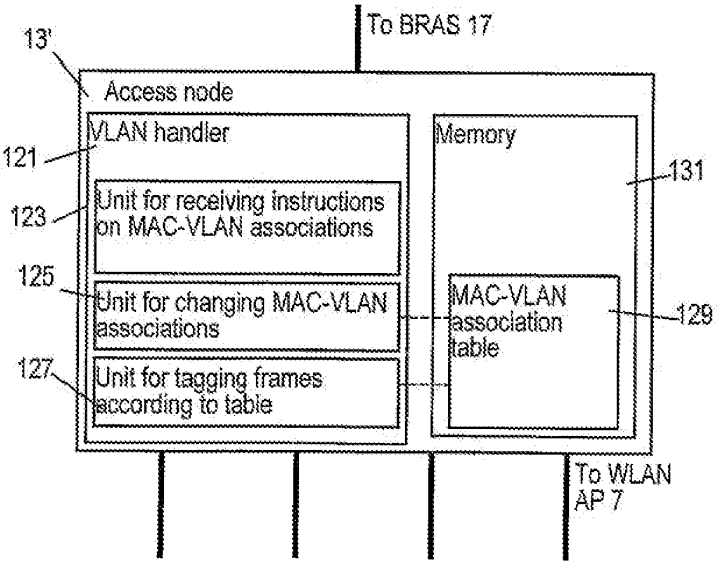

13'
To BRAS 17
Access node
VLAN handler
121
Memory
131
123
Unit for receiving instructions on MAC-VLAN associations
125
Unit for changing MAC-VLAN associations
MAC-VLAN association table
129
127
Unit for tagging frames according to table
To WLAN AP 7

Fig. 4a

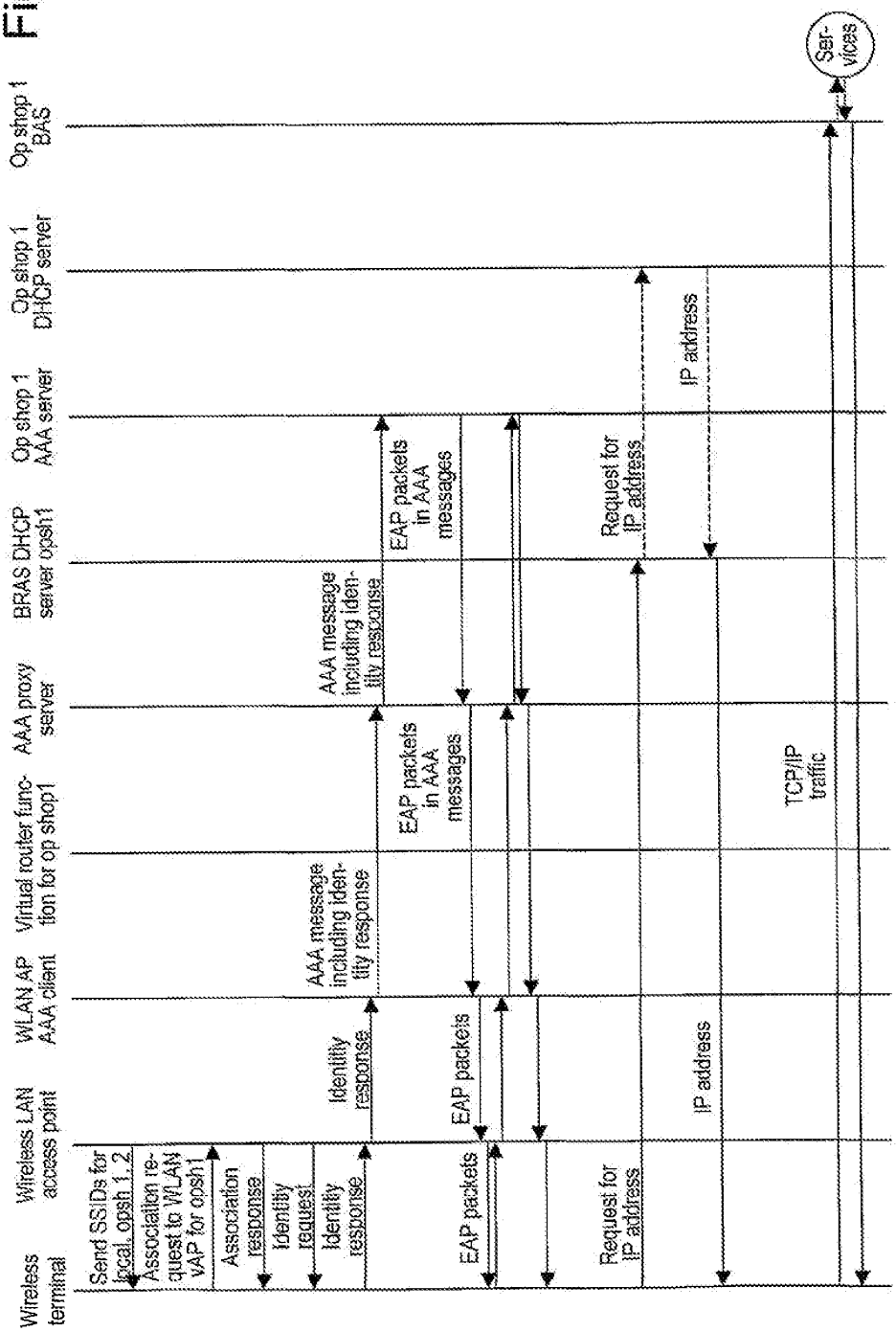

Wireless terminal
Wireless LAN access point
WLAN AP AAA client
Virtual router function for op shop1
AAA proxy server
BRAS DHCP server opsh1
Op shop 1 AAA server
Op shop 1 DHCP server
Op shop 1 BAS
Send SSIDs for local opsh 1,2
Association request to WLAN vAP for opsh1
Association response
Identity request
Identity response
Identitiy response
AAA message including identity response
EAP packets in AAA messages
AAA message including identity response
EAP packets
EAP packets
EAP packets in AAA messages
Request for IP address
IP address
Request for IP address
IP address
TCP/IP traffic
Services

Fig. 4b

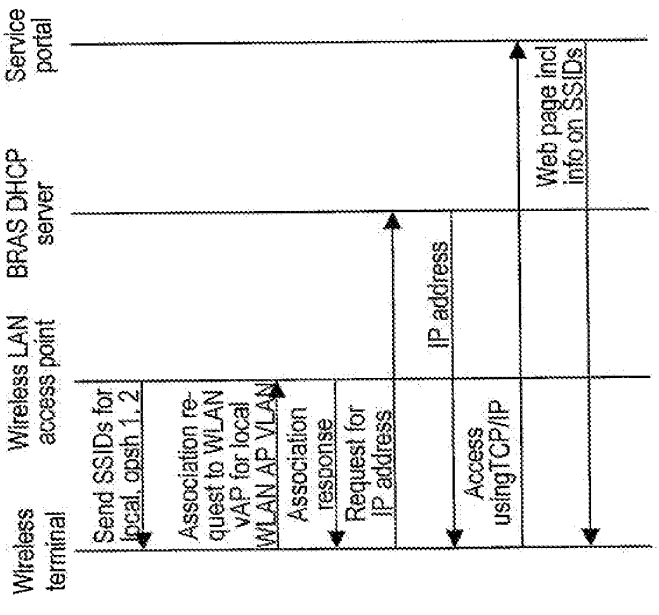

Wireless terminal
Wireless LAN access point
BRAS DHCP server
Service portal
Send SSIDs for local ssh 1, 2
Association request to WLAN vAP for local WLAN AP VLAN
Association response
Request for IP address
IP address
Access using TCP/IP
Web page incl info on SSIDs

Fig. 4c

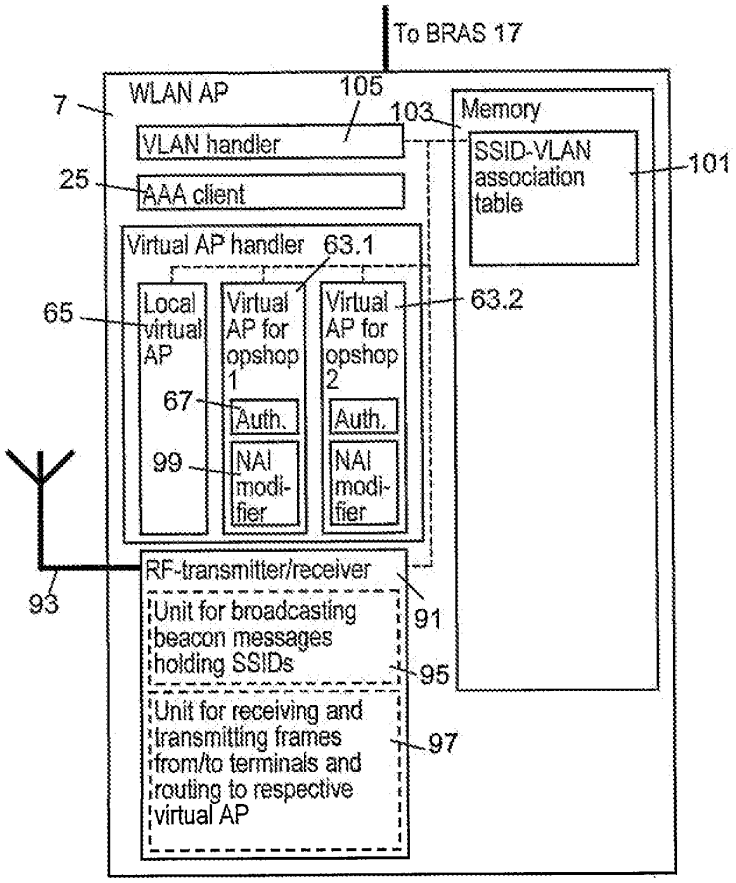


Fig. 4d

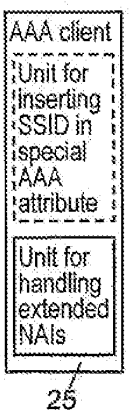


Fig. 4e

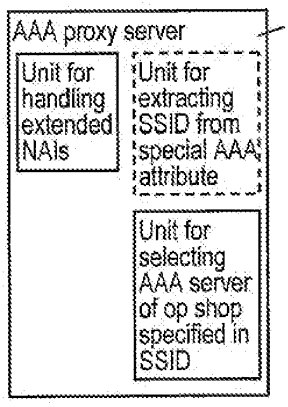


Fig. 4f

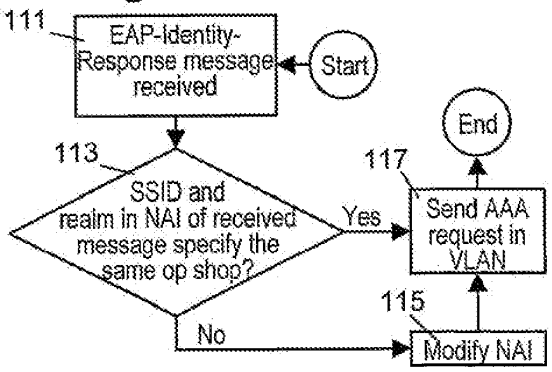


Fig. 5

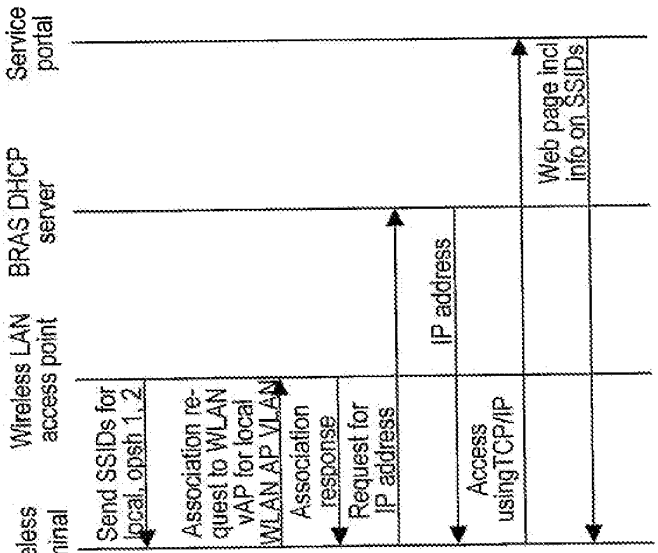

Wireless terminal
Wireless LAN access point
BRAS DHCP server
Service portal
Send SSIDs for local, opsh 1, 2
Association request to WLAN vAP for local WLAN AP VLAN
Association response
Request for IP address
IP address
Access usingTCP/IP
Web page incl info on SSIDs

Fig. 6a

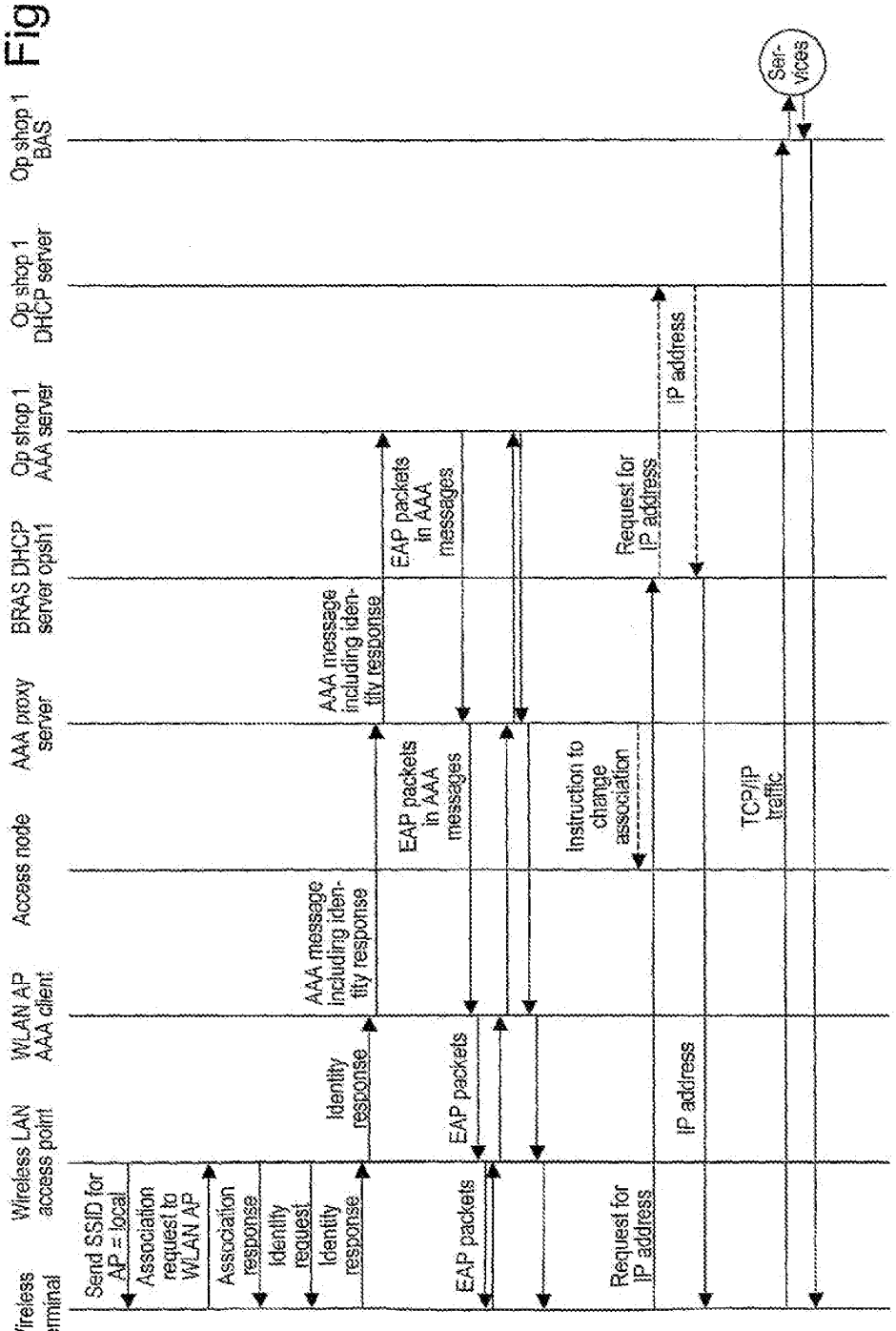

Wireless terminal
Wireless LAN access point
WLAN AP AAA client
Access node
AAA proxy server
BRAS DHCP server opsh1
Op shop 1 AAA server
Op shop 1 DHCP server
Op shop 1 BAS
Send SSID for AP = local
Association request to WLAN AP
Association response
Identity request
Identity response
AAA message including identity response
EAP packets in AAA messages
EAP packets
Identity response
AAA message including identity response
EAP packets in AAA messages
EAP packets
Instruction to change association
Request for IP address
Request for IP address
IP address
IP address
TCP/IP traffic
Services

Fig. 7a

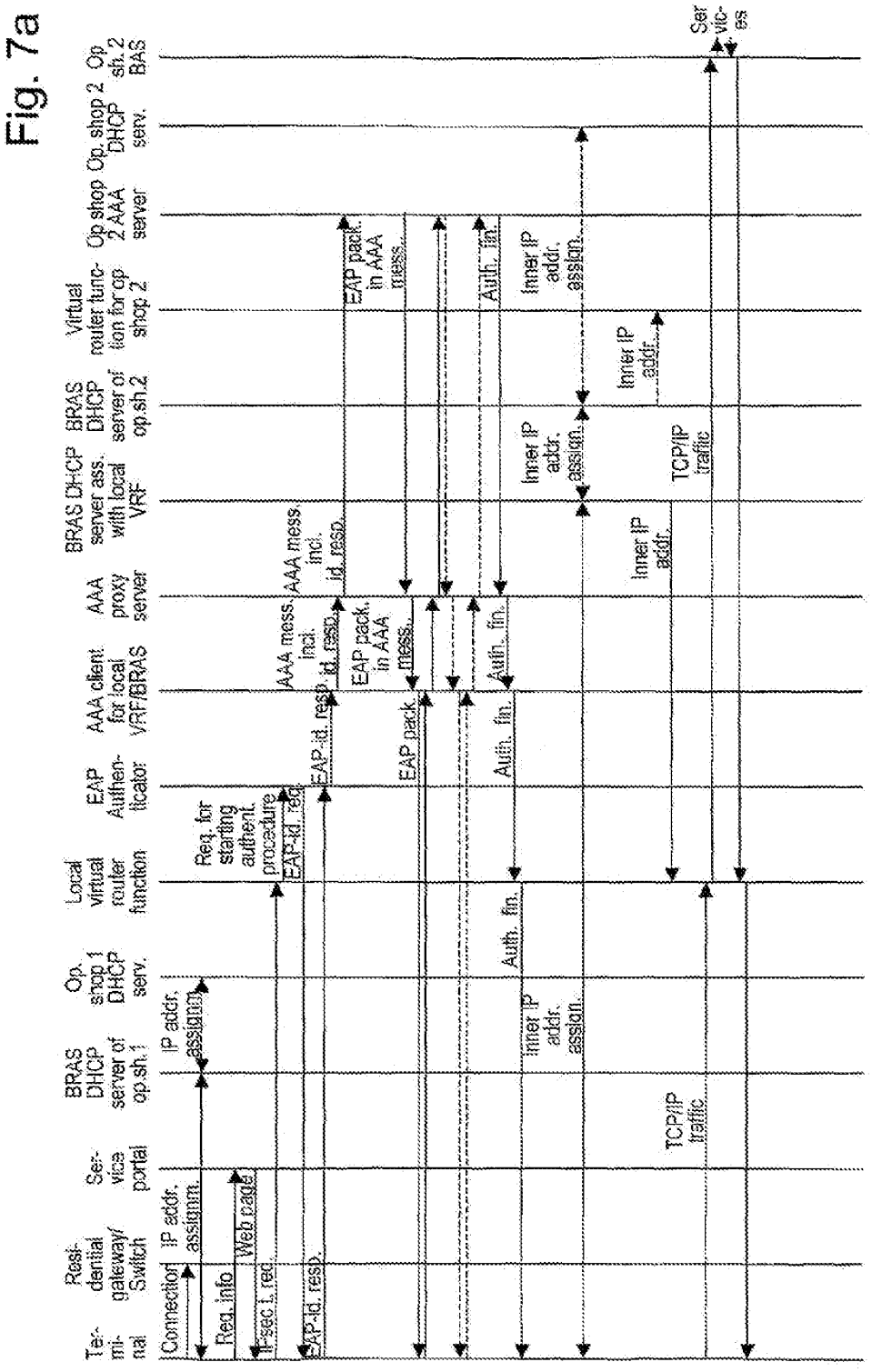
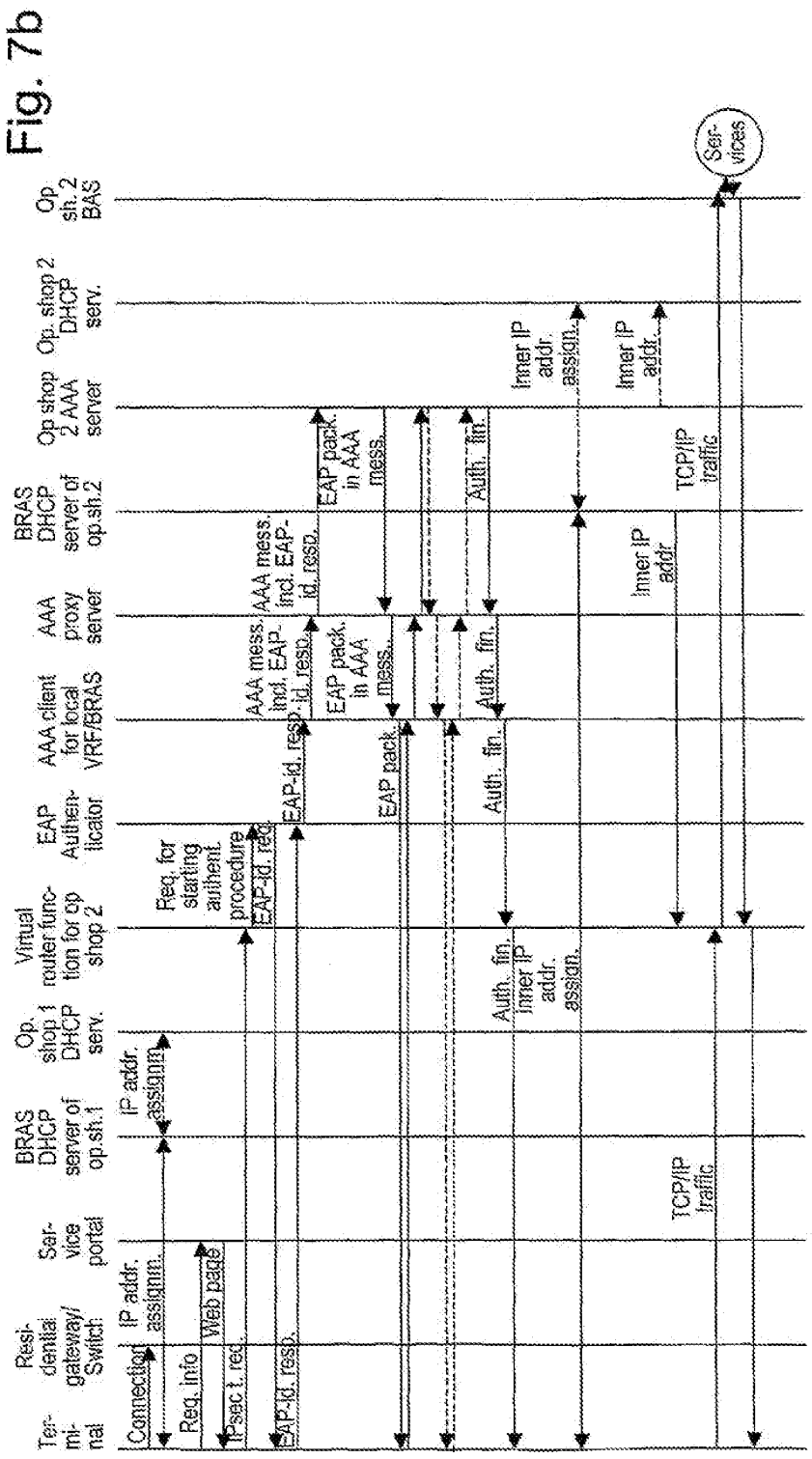

Ter-mi-nal
Resi-dential gateway/ Switch
Ser-vice portal
BRAS DHCP server of op.sh.1
Op. shop 1 DHCP serv.
Local virtual router function
EAP Authen-ticator
AAA client for local VRF/BRAS
AAA proxy server
BRAS DHCP server ass. with local VRF
BRAS DHCP server of op.sh.2
Virtual router func-tion for op shop 2
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Op sh. 2 BAS
Ser vic-es
Connection
IP addr. assignm.
Req. info
Web page
IP-sec t. req.
EAP-id. req.
EAP-id. resp.
IP addr. assign.
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
AAA mess. incl. id. resp.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
EAP pack.
EAP pack. in AAA mess.
Auth. fin.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr. assign.
Inner IP addr.
Inner IP addr.
Inner IP addr. assign.
TCP/IP traffic
TCP/IP traffic

Fig. 7b


Ter-mi-nal
Resi-dential gateway/ Switch
Ser-vice portal
BRAS DHCP server of op.sh.1
Op. shop 1 DHCP serv.
Virtual router func-tion for op shop 2
EAP Authen-ticator
AAA client for local VRF/BRAS
AAA proxy server
BRAS DHCP server of op.sh.2
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Op. sh. 2 BAS
Ser-vices
Connection
IP addr. assignm.
Req. info
Web page
IPsec t. rec.
EAP-id. req.
EAP-id. resp.
IP addr. assignm.
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
AAA mess. incl. EAP-id. resp.
AAA mess. incl. EAP-id. resp.
EAP pack. in AAA mess.
EAP pack.
EAP pack. in AAA mess.
Auth. fin.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr. assign.
Inner IP addr.
Inner IP addr
TCP/IP traffic
TCP/IP traffic

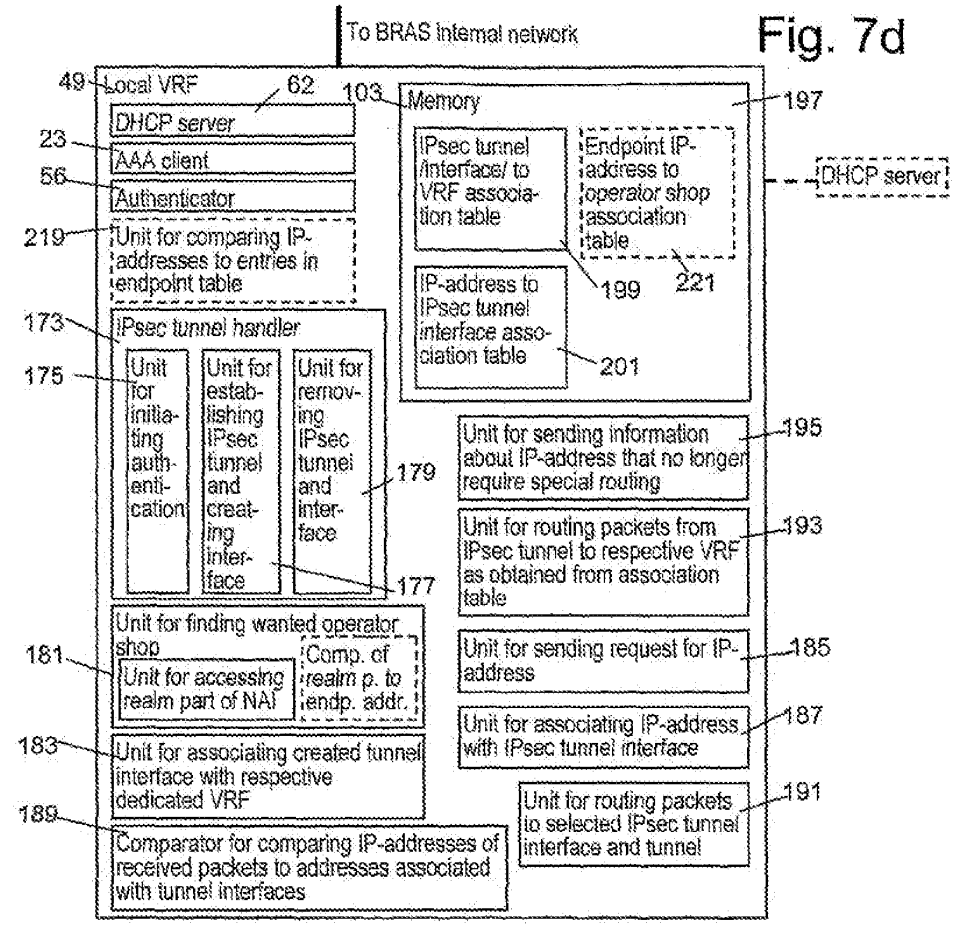


Fig. 7d

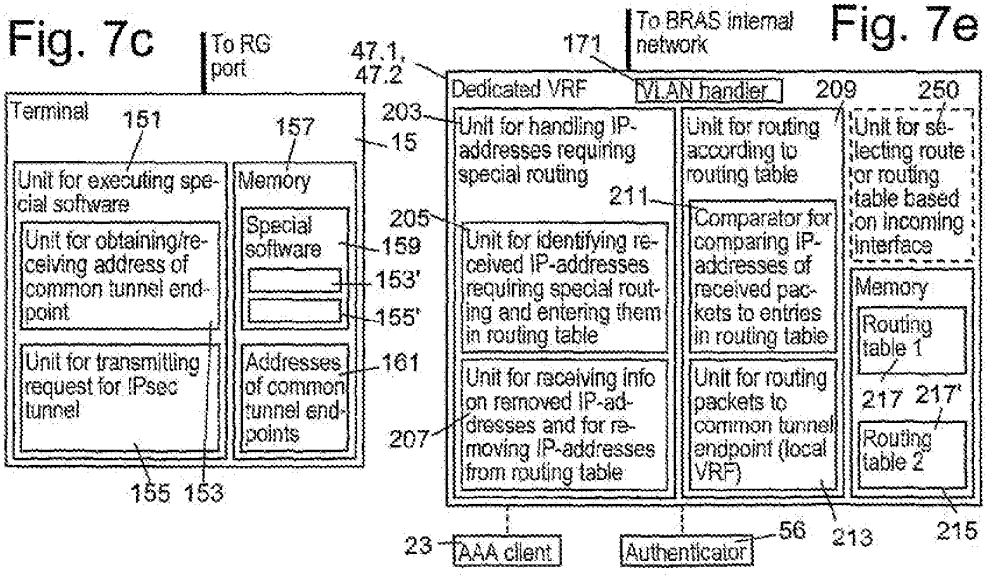


Fig. 7c

Fig. 7e

Fig. 7f

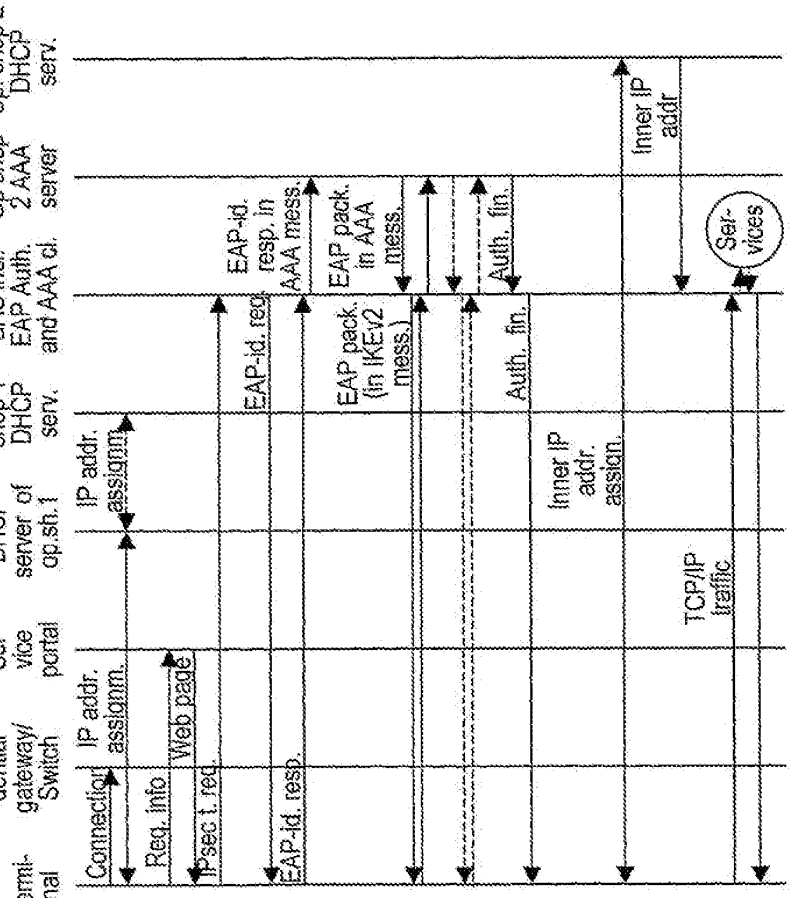

Termi-nal
Resi-dential gateway/ Switch
Ser-vice portal
BRAS DHCP server of op.sh.1
Op. shop 1 DHCP serv.
Op sh. 2 BAS incl. EAP Auth. and AAA cl.
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Connection
IP addr. assignm.
Req. info
Web page
IPsec t. req.
EAP-id. req.
EAP-id. resp.
EAP-id. resp. in AAA mess.
EAP pack. (in IKEv2 mess.)
EAP pack. in AAA mess.
Auth. fin.
Inner IP addr. assign.
Inner IP addr
TCP/IP traffic
Ser-vices

Fig. 7g

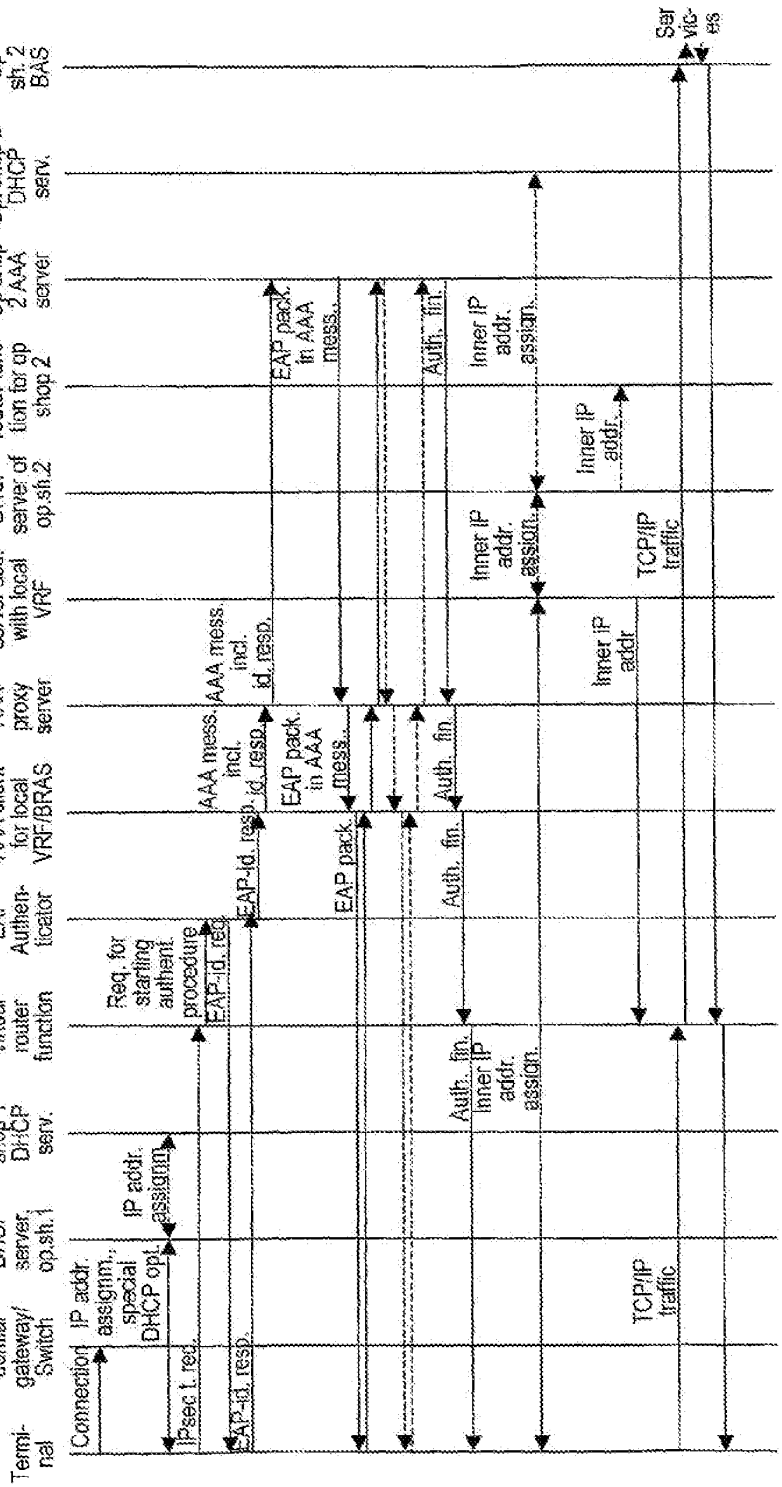

Termi-nal
Resi-dential gateway/ Switch
BRAS DHCP server, op.sh.1
Op. shop 1 DHCP serv.
Local virtual router function
EAP Authen-ticator
AAA client for local VRF/BRAS
AAA proxy server
BRAS DHCP server ass. with local VRF
BRAS DHCP server of op.sh.2
Virtual router func-tion for op shop 2
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Op. sh. 2 BAS
Ser vic-es
Connection
IP addr. assignm., special DHCP opt.
IPsec t. req.
EAP-id. req.
EAP-id. resp.
IP addr. assignm.
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
EAP pack.
Auth. fin.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr.
Inner IP addr.
Inner IP addr. assign.
TCP/IP traffic
TCP/IP traffic

Fig. 7h

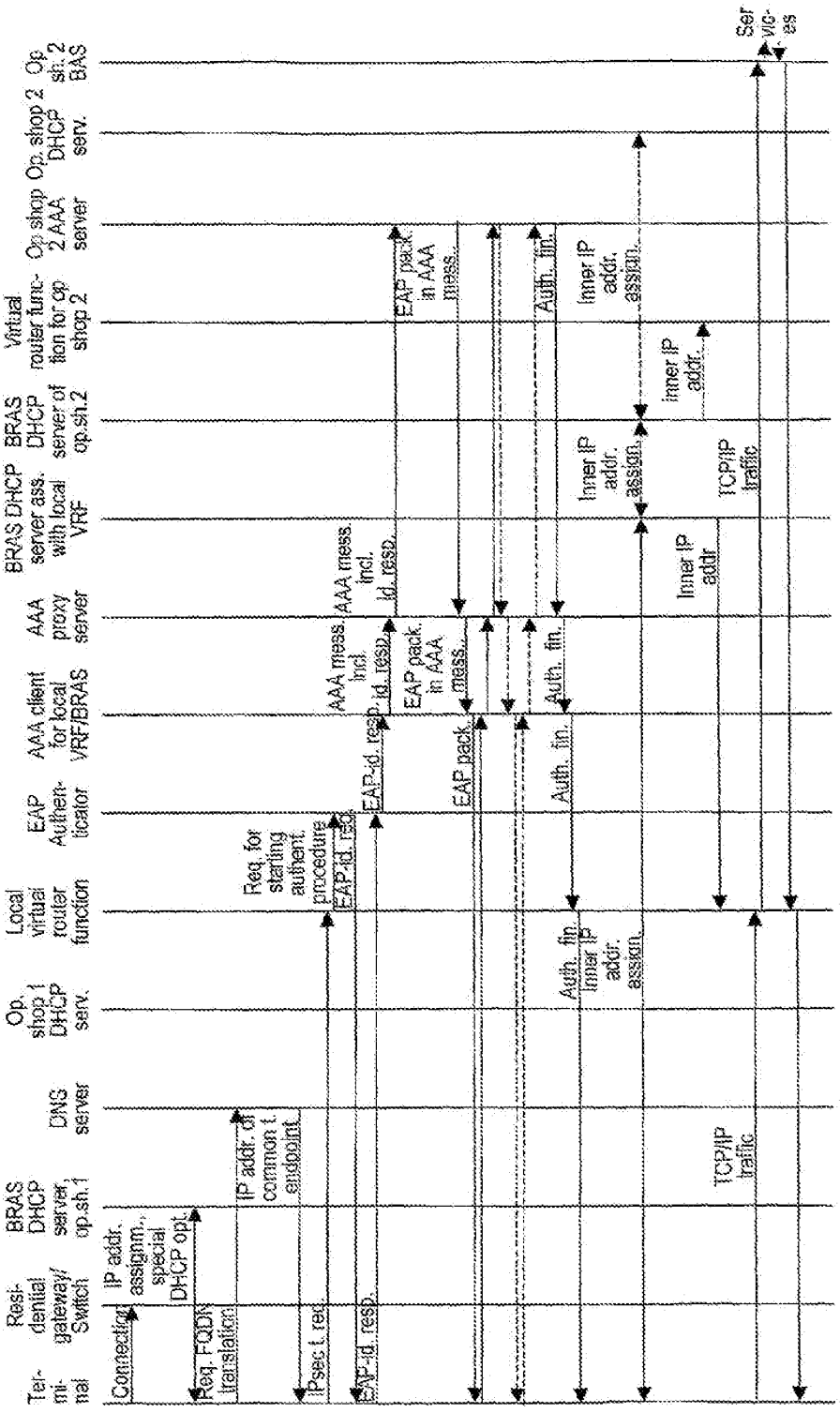

Ter-mi-nal
Resi-dential gateway/ Switch
BRAS DHCP server, op.sh.1
DNS server
Op. shop 1 DHCP serv.
Local virtual router function
EAP Authen-ticator
AAA client for local VRF/BRAS
AAA proxy server
BRAS DHCP server ass. with local VRF
BRAS DHCP server of op.sh.2
Virtual router func-tion for op shop 2
Op. shop 2 AAA server
Op. shop 2 DHCP serv.
Op. sh. 2 BAS
Ser vic-es
Connection
IP addr. assignm., special DHCP opt.
Req. FQDN translation
IP addr. of common t. endpoint
IPsec t. req.
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
EAP pack.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr.
Inner IP addr
TCP/IP traffic
TCP/IP traffic
Auth. fin.
Inner IP addr. assign.
Inner IP addr. assign.

Fig. 7i

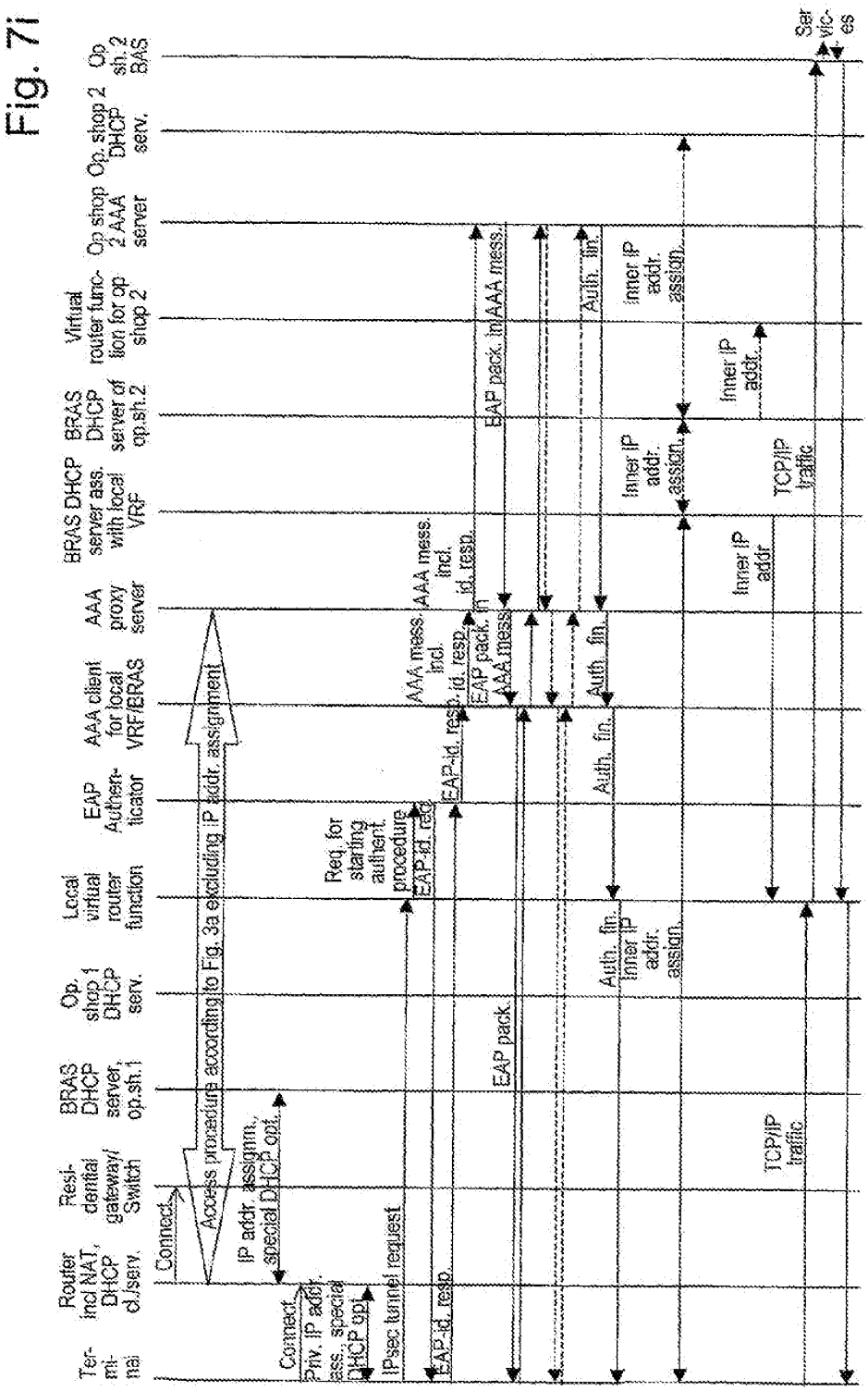

Ter-mi-nal
Router incl NAT, DHCP cl./serv.
Resi-dential gateway/ Switch
BRAS DHCP server, op.sh.1
Op. shop 1 DHCP serv.
Local virtual router function
EAP Authen-ticator
AAA client for local VRF/ERAS
AAA proxy server
BRAS DHCP server ass. with local VRF
BRAS DHCP server of op.sh.2
Virtual router func-tion for op shop 2
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Op. sh. 2 BAS
Ser vic-es
Connect
Access procedure according to Fig. 3a excluding IP addr. assignment
IP addr. assignm. special DHCP opt.
Connect
Priv. IP addr. ass., special DHCP opt.
IPsec tunnel request
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
EAP-id. resp. id. resp.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
EAP pack.
BAP pack. in AAA mess.
Auth. fin.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr. assign.
Inner IP addr. assign.
Inner IP addr.
Inner IP addr
TCP/IP traffic
TCP/IP traffic

Fig. 7j

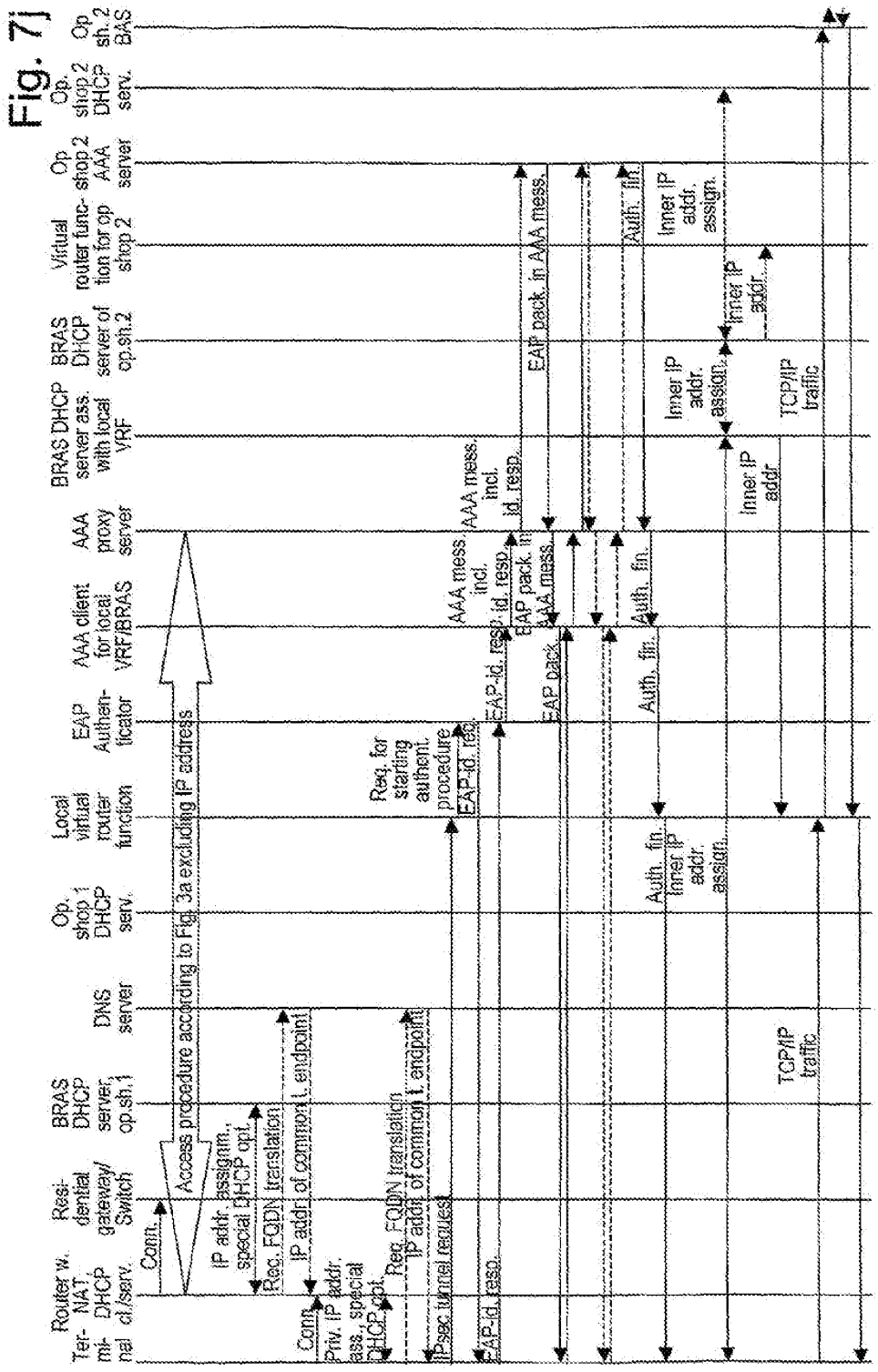

Router w. NAT, DHCP cl./serv.
Ter-mi-nal
Resi-dential gateway/ Switch
BRAS DHCP server, op.sh.1
DNS server
Op. shop 1 DHCP serv.
Local virtual router function
EAP Authen-ticator
AAA client for local VRF/BRAS
AAA proxy server
BRAS DHCP server ass. with local VRF
BRAS DHCP server of op.sh.2
Virtual router func-tion for op shop 2
Op shop 2 AAA server
Op. shop 2 DHCP serv.
Op. sh.2 BAS
Conn.
Access procedure according to Fig. 3a excluding IP address
IP addr. assignm., special DHCP opt.
Rec. FQDN translation
IP addr of common t. endpoint
Conn.
Priv. IP addr. ass., special DHCP opt.
Rec. FQDN translation
IP addr of common t. endpoint
IPsec tunnel request
Req. for starting authent. procedure
EAP-id. req.
EAP-id. resp.
AAA mess. incl. id. resp.
EAP pack. in AAA mess.
EAP pack.
AAA mess.
Auth. fin.
Auth. fin.
Inner IP addr. assign.
Inner IP addr
Inner IP addr. assign.
Inner IP addr.
Auth. fin.
Inner IP addr. assign.
TCP/IP traffic
TCP/IP traffic

Fig. 8a

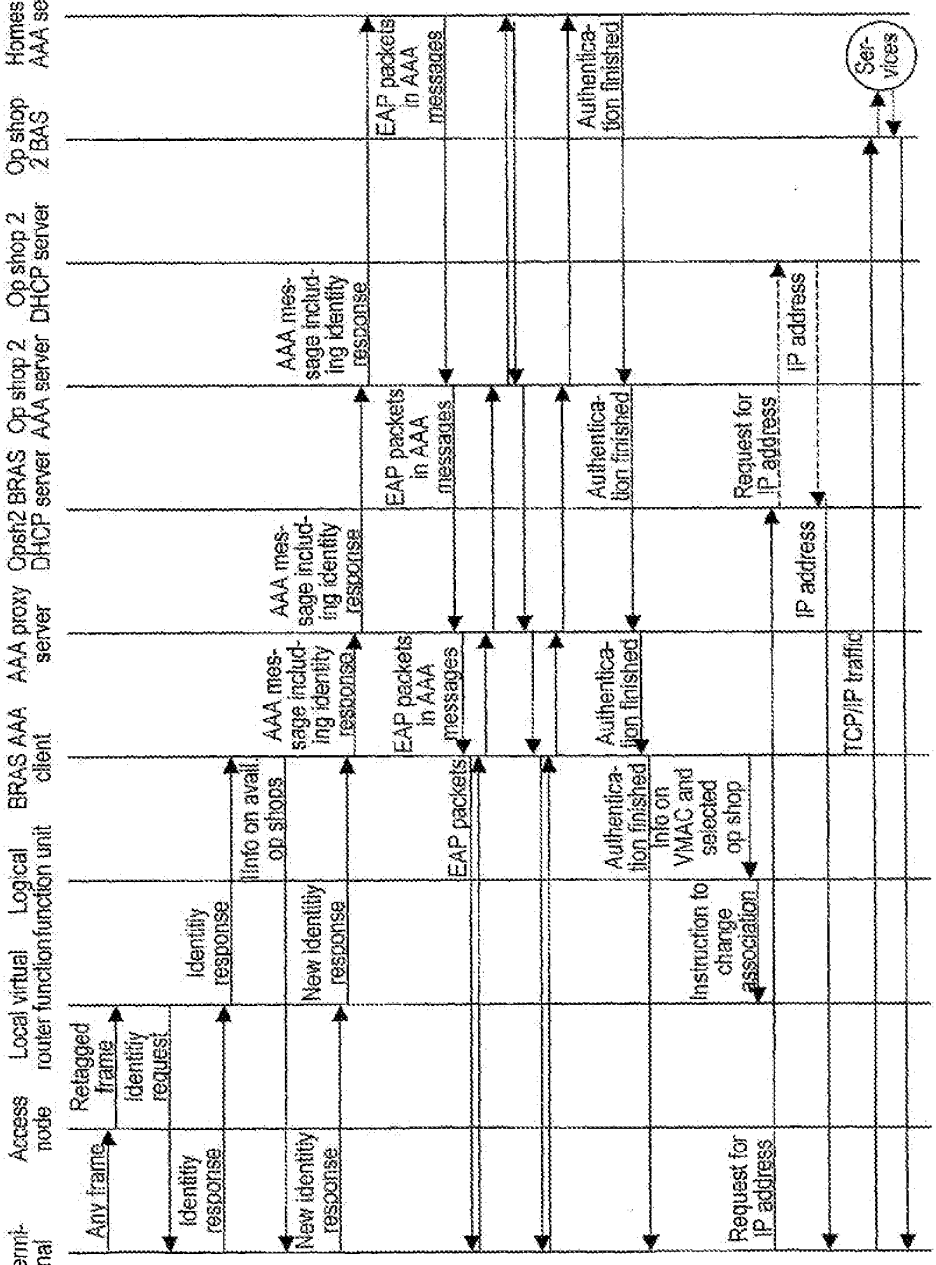

Termi-nal
Access node
Local virtual router function
Logical function unit
BRAS AAA client
AAA proxy server
Opsh2 DHCP server
BRAS AAA server
Op shop 2 AAA server
Op shop 2 DHCP server
Op shop 2 BAS
Homeshop AAA server
Any frame
Retagged frame
Identitiy request
Identitiy response
Identitiy response
Info on avail. op shops
New identitiy response
New identitiy response
AAA mes-sage includ-ing identity response
AAA mes-sage includ-ing identity response
AAA mes-sage includ-ing identity response
EAP packets in AAA messages
EAP packets
EAP packets in AAA messages
EAP packets in AAA messages
Authentica-tion finished
Authentica-tion finished
Authentica-tion finished
Info on VMAC and selected op shop
Instruction to change association
Request for IP address
Request for IP address
IP address
IP address
TCP/IP traffic
Ser-vices

Fig. 8b

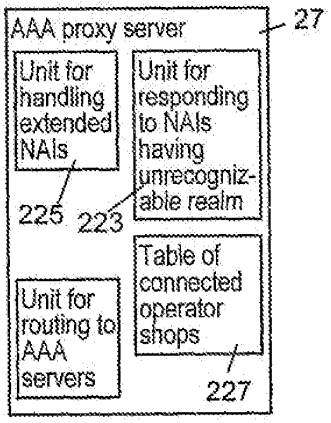


Fig. 8c

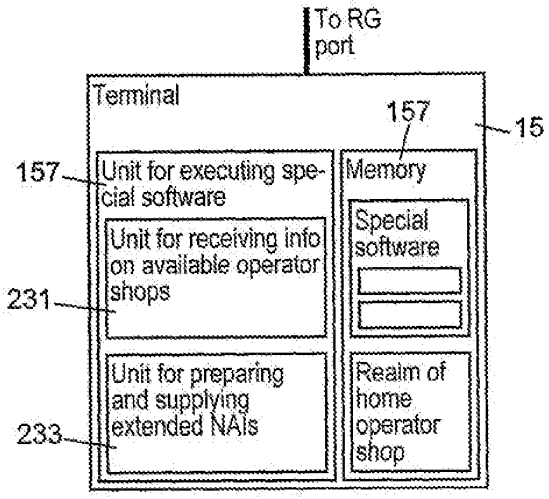


Fig. 8d

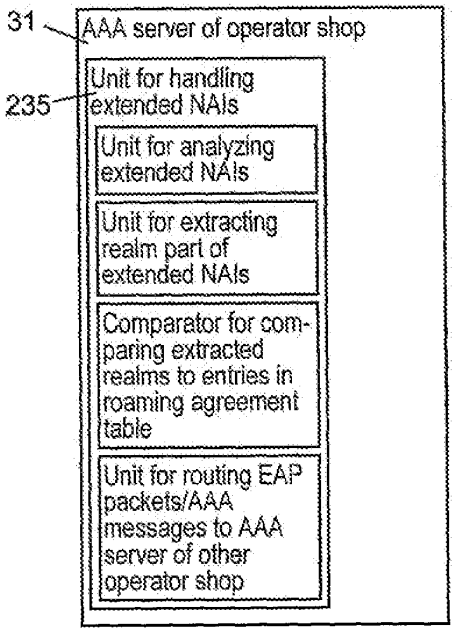


Fig. 9a

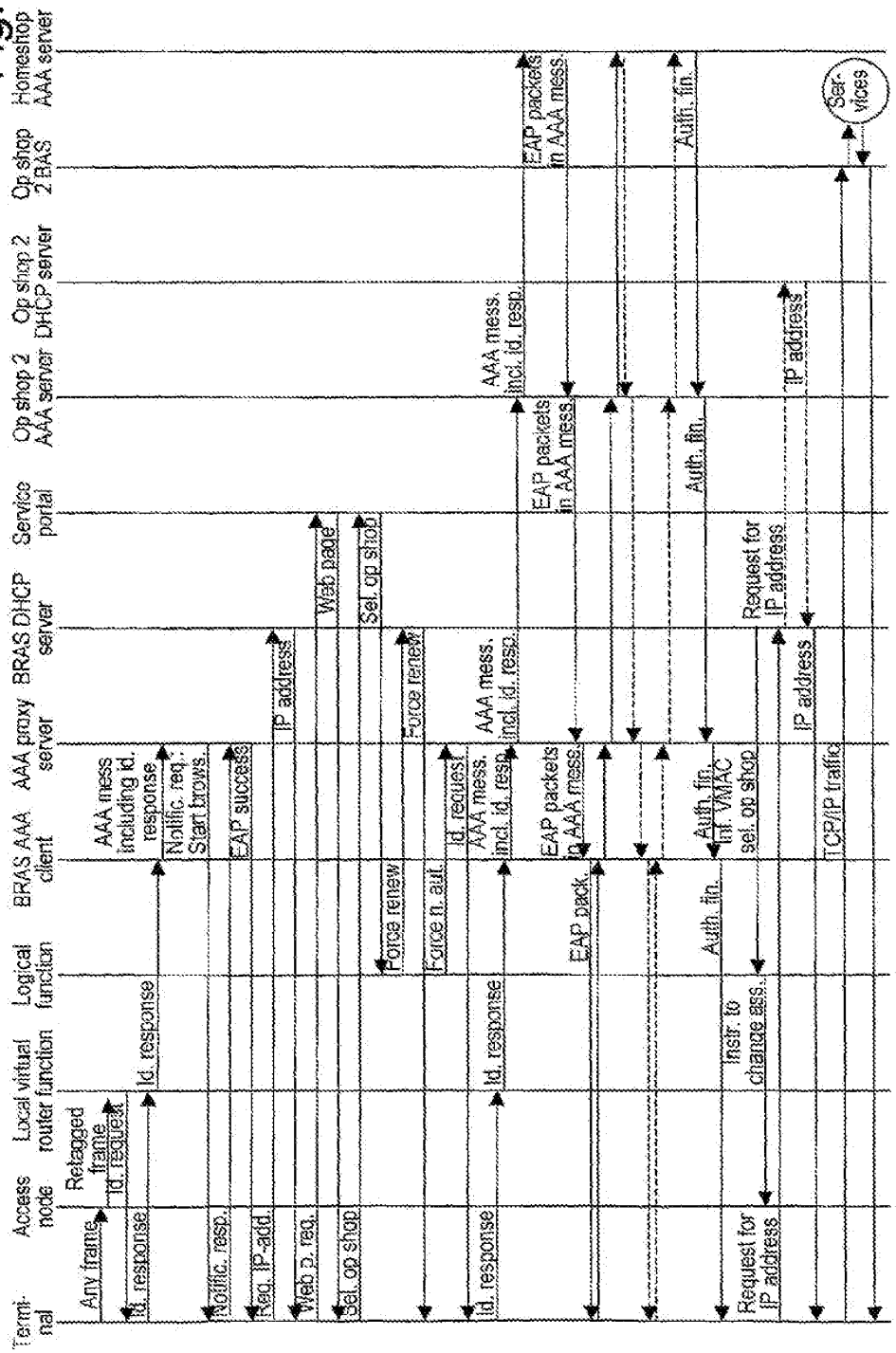

Termi-nal
Access node
Local virtual router function
Logical function
BRAS AAA client
AAA proxy server
BRAS DHCP server
Service portal
Op shop AAA server
Op shop 2 DHCP server
Op shop 2 BAS
Homeshop AAA server
Any frame
Retagged frame Id. request
Id. response
AAA mess including id. response
Notific. req. Start brows.
Notific. resp.
EAP success
Req. IP-add.
IP address
Web p. req.
Web page
Sel. op shop
Sel. op shop
Force renew
Force renew
Force n. aut.
Id. request
Id. response
AAA mess. incl. id. resp.
AAA mess. incl. id. resp.
Id. response
EAP packets in AAA mess.
EAP packets in AAA mess.
EAP pack.
EAP packets in AAA mess.
Auth. fin.
Auth. fin.
Auth. fin. Inf. VMAC sel. op shop
Auth. fin.
Insr. to change ass.
Request for IP address
Request for IP address
IP address
IP address
TCP/IP traffic
Ser-vices

Fig. 9b

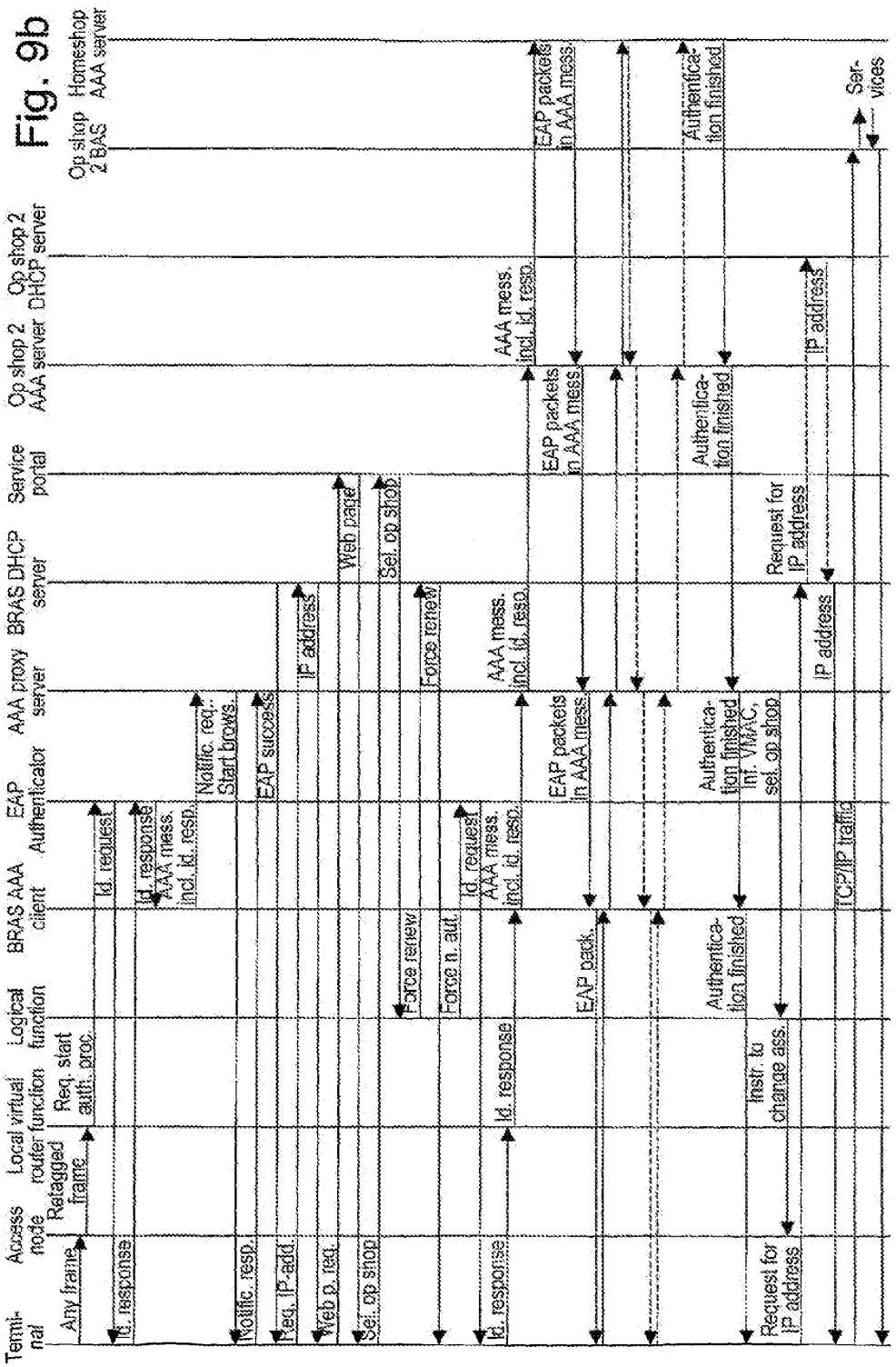

Termi-nal
Access node
Local virtual router function
Logical function
BRAS AAA client
EAP Authenticator
AAA proxy server
BRAS DHCP server
Service portal
Op shop 2 AAA server
Op shop 2 DHCP server
Op shop 2 BAS
Homeshop AAA server
Any frame
Retagged frame
Req. start auth. proc.
Id. request
Id. response
Id. response
AAA mess. incl. id. resp.
Notific. req.: Start brows.
Notific. resp.
EAP success
Req. IP-add.
IP address
Web p. req.
Web page
Sel. op shop
Sel. op shop
Force renew
Force renew
Force n. aut.
Id. request
Id. response
AAA mess. incl. id. resp.
AAA mess. incl. id. resp.
Id. response
EAP pack.
EAP packets in AAA mess.
EAP packets in AAA mess.
EAP packets in AAA mess.
Authentication finished
Authentication finished
Authentication finished Int. VMAC, sel. op shop
Instr. to change ass.
Request for IP address
Request for IP address
IP address
IP address
TCP/IP traffic
Ser-vices

Fig. 9c

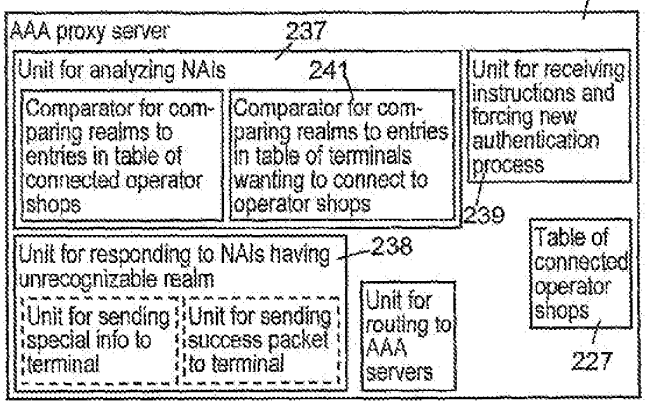


Fig. 9e

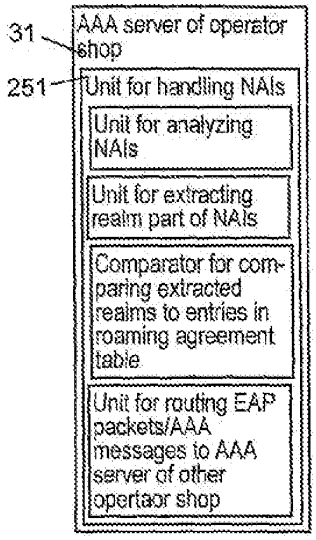


Fig. 9d

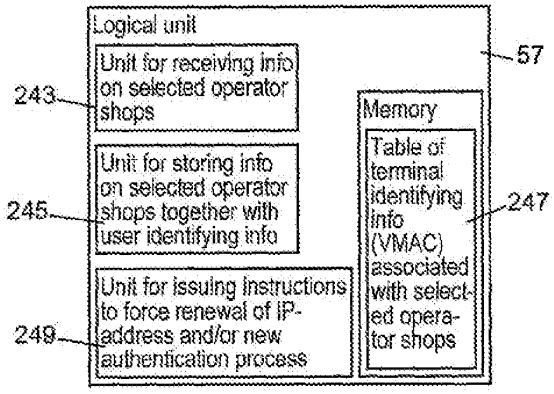


Fig. 9f

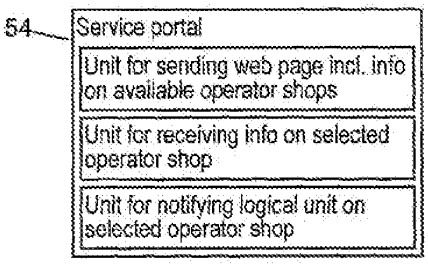
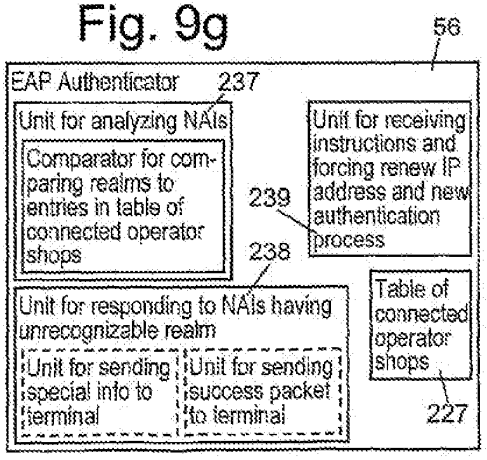


Fig. 9g



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2005060208 A **[0037]**
- US 2004066756 A **[0047]**
- US 2003117954 A **[0048]**
- US 2003037163 A **[0049]**
- WO 2006038843 A **[0202] [0230]**
- WO 2006038844 A **[0202] [0213] [0230] [0243]**

Non-patent literature cited in the description

- **B. ABOBA ; M. BEADLES.** The Network Access Identifier. RFC, January 1999, 2486 **[0060]**
- **B. ABOBA et al.** The Network Access Identifier. RFC, December 2005, 4282 **[0060]**
- **L. BLUNK ; J. VOLLBRECHT.** PPP Extensible Authentication Protocol (EAP). RFC, March 1998, 2284 **[0060]**
- **L. BLUNK et al.** Extensible Authentication Protocol (EAP). RFC, June 2004, 3748 **[0060]**
- MAC-Forced Forwarding: A Method for Traffic Separation on an Ethernet Access Network. **T. MELSEN ; S. BLAKE.** <draft-melsen-mac-forcedfwd-03.txt>, Personal Internet-Draft. IETF, August 2004 **[0061]**
- **MICHAEL BEGLEY.** The Public Ethernet - The next-generation broadband access network. *Ericsson Review*, 2004 **[0061]**
- *Medium Access Control (MAC) Security Enhancements*, 2004 **[0063]**
- **C. RIGNEY et al.** Remote Authentication Dial In User Service (RADIUS). RFC, June 2000, 2865 **[0069]**
- **B. ABOBA ; P. CALHOUN.** RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). RFC, September 2003, 3579 **[0069]**
- **P. CALHOUN ; J. LOUGHNEY ; E. GUTTMAN ; G. ZORN ; J. ARKKO.** Diameter Base Protocol. RFC, September 2003, 3588 **[0069]**
- Diameter Extensible Authentication Protocol (EAP) Application. Internet draft <draft-ietf-aaa-eap-03.txt>. IETF, October 2003 **[0069]**
- **D. MCPHERSON ; B. DYKES.** VLAN Aggregation for Efficient IP Address Allocation. RFC, February 2001, 3069 **[0077]**
- **L. MAMAKOS et al.** A Method for Transmitting PPP over Ethernet (PPPoE). RFC, February 1999, 2516 **[0081]**
- **D. HARRINGTON et al.** An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. RFC, December 2002, 3411 **[0083]**
- Internet draft, <draft-adrangi-eap-network-Discovery-and-Selection-01.txt>, Mediating Network Discovery and Selection **[0241]**

Samsung Ex. 1004, Page 382 of 563

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 29/10 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(11) 공개번호 10-2007-0061684
(43) 공개일자 2007년06월14일

(21) 출원번호 10-2005-0121329
(22) 출원일자 2005년12월10일
심사청구일자 2005년12월10일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지
에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
주식회사 케이티
경기 성남시 분당구 정자동 206
하나로텔레콤 주식회사
서울특별시 영등포구 여의도동 17-7

(72) 발명자 오정훈
대전광역시 유성구 신성동 럭키하나아파트 105동 702호
김현재
인천광역시 부평구 삼산동 삼산타운 주공아파트 709동 1201호
김영일
대전광역시 유성구 어은동 한빛아파트 135동 704호

(74) 대리인 유미특허법인

전체 청구항 수 : 총 30 항

(54) 무선 인터넷 시스템의 하위 매체 접근 계층 장치 및 그를이용한 데이터 처리 방법

(57) 요약

본 발명은 무선 인터넷 시스템의 하위 매체 접근 계층 장치 및 그를 이용한 데이터 처리 방법에 관한 것이다.

이를 위하여 본 발명은, 물리 계층과 데이터 신호 및 제어 신호를 송수신하는 물리 계층 인터페이스 블록, 상위 MAC 계층과 데이터 신호 및 제어 신호를 송수신하는 상위 MAC 인터페이스 블록, 상향 링크 데이터에 필요한 복호화 작업 및 CRC 확인 작업을 수행하는 상향 링크 블록, 하향 링크 데이터에 필요한 암호화 작업 및 CRC 생성 작업을 수행하는 하향 링크 블록, 및 물리 계층 인터페이스 블록, 상위 MAC 인터페이스 블록, 상향 링크 블록 및 하향 링크 블록 사이에 전달되는 제어 정보 및 데이터를 저장하는 메모리를 포함하여 무선 인터넷 시스템에서 데이터의 암복호화 및 CRC 연산을 수행하는 하위 MAC 장치를 제공한다.

본 발명에 의하면, 하위 MAC 계층에서 상위 MAC 계층으로 전달되는 대용량의 데이터에 대하여 시간 지연 없이 암호화, 복호화 작업 수행, CRC 생성 및 확인 작업을 수행할 수 있어 대용량 데이터의 실시간 통신이 가능하다.

대표도

도 3

특허청구의 범위

청구항 1.

무선 인터넷 시스템에서 데이터의 암복호화 및 CRC(Cyclic Redundancy Code) 연산을 수행하는 하위 MAC(Media Access Control) 장치에 있어서,

물리 계층과 데이터 신호 및 제어 신호를 송수신하는 물리 계층 인터페이스 블록;

상위 MAC 계층과 상기 데이터 신호 및 상기 제어 신호를 송수신하는 상위 MAC 인터페이스 블록;

상향 링크 데이터에 필요한 복호화 작업 및 CRC 확인 작업을 수행하는 상향 링크 블록;

하향 링크 데이터에 필요한 암호화 작업 및 CRC 생성 작업을 수행하는 하향 링크 블록; 및

상기 물리 계층 인터페이스 블록, 상기 상위 MAC 인터페이스 블록, 상기 상향 링크 블록 및 상기 하향 링크 블록 사이에 전달되는 제어 정보 및 데이터를 저장하는 메모리

를 포함하는 것을 특징으로 하는 하위 MAC 장치.

청구항 2.

제1항에 있어서, 상기 하향 링크 블록은,

입력되는 하향 링크 데이터의 PDU 페이로드(Payload)에 대한 블록 암호화 알고리즘을 실행하는 암호 블록;

상기 하향 링크 데이터에 포함되는 CRC를 생성하는 CRC 생성 블록;

상기 암호 블록과 상기 CRC 생성 블록 사이에 위치하여, 상기 하향 링크 데이터의 처리 순서를 관리하는 하향 링크 FIFO (First-In First-Out); 및

상기 암호 블록과 상기 CRC 생성 블록의 동작 제어, 초기화 작업을 수행하며, 발생되는 오류 정보를 상기 상위 MAC 계층으로 보고하는 하향 링크 제어 블록

을 포함하는 것을 특징으로 하는 하위 MAC 장치.

청구항 3.

제2항에 있어서, 상기 하향 링크 FIFO는,

상기 암호 블록에서 암호화 작업이 진행되는 중에, 상기 암호 블록으로부터 암호화가 종료된 데이터를 입력받아, 별도의 저장 과정 없이 순차적으로 상기 CRC 생성 블록으로 진행시키는 것을 특징으로 하는 하위 MAC 장치.

청구항 4.

제1항에 있어서, 상기 상향 링크 블록은,

입력되는 상향 링크 데이터의 PDU 페이로드에 대한 블록 복호화 알고리즘을 실행하는 복호 블록;

상기 상향 링크 데이터에 포함되는 PDU 단위의 CRC를 확인하는 CRC 확인 블록;

상기 복호 블록과 상기 CRC 확인 블록 사이에 위치하여, 상기 상향 링크 데이터의 처리 순서를 관리하는 상향 링크 FIFO; 및

상기 복호 블록과 상기 CRC 확인 블록의 동작 제어, 초기화 작업을 수행하며, 발생되는 오류 정보를 상기 상위 MAC 계층으로 보고하는 상향 링크 제어 블록

을 포함하는 것을 특징으로 하는 하위 MAC 장치.

청구항 5.

제4항에 있어서, 상기 상향 링크 FIFO는,

상기 복호 블록에서 복호화 작업이 진행되는 중에, 상기 복호 블록으로부터 복호화가 완료된 데이터를 입력받아, 별도의 저장 과정 없이 순차적으로 상기 CRC 확인 블록으로 진행시키는 것을 특징으로 하는 하위 MAC 장치.

청구항 6.

제1항에 있어서, 상기 상위 MAC 인터페이스 블록은,

상기 상향 링크 블록과 상향 링크 제어 신호를 송수신하기 위한 상향 링크 제어 신호선을 통해 연결되어 있으며, 상기 하향 링크 블록과 하향 링크 제어 신호를 송수신하기 위한 하향 링크 제어 신호선을 통해 연결되어 있는 것을 특징으로 하는 하위 MAC 장치.

청구항 7.

제1항에 있어서, 상기 메모리는,

상기 물리 계층 인터페이스 블록과 상기 상향 링크 블록 사이에 전달되는 데이터를 저장하는 상향 링크 물리 계층 메모리;

상기 물리 계층 인터페이스 블록과 상기 하향 링크 블록 사이에 전달되는 데이터를 저장하는 하향 링크 물리 계층 메모리;

상기 상위 MAC 인터페이스 블록과 상기 상향 링크 블록 사이에 전달되는 데이터를 저장하는 상향 링크 메모리; 및

상기 상위 MAC 인터페이스 블록과 상기 하향 링크 블록 사이에 전달되는 데이터를 저장하는 하향 링크 메모리

를 포함하는 것을 특징으로 하는 하위 MAC 장치.

청구항 8.

Samsung Ex. 1004, Page 385 of 563

제7항에 있어서,

상기 상향 링크 물리 계층 메모리는 상기 제어 정보를 저장하기 위한 상향 링크 물리 계층 제어 정보 메모리와, 상기 데이터를 저장하기 위한 상향 링크 물리 계층 데이터 메모리를 포함하고,

상기 하향 링크 물리 계층 메모리는 상기 제어 정보를 저장하기 위한 하향 링크 물리 계층 제어 정보 메모리와, 상기 데이터를 저장하기 위한 하향 링크 물리 계층 데이터 메모리를 포함하며,

상기 상향 링크 메모리는 상기 제어 정보를 저장하기 위한 상향 링크 제어 정보 메모리와, 상기 데이터를 저장하기 위한 상향 링크 데이터 메모리를 포함하고,

상기 하향 링크 메모리는 상기 제어 정보를 저장하기 위한 하향 링크 제어 정보 메모리와, 상기 데이터를 저장하기 위한 하향 링크 데이터 메모리를 포함하는 것을 특징으로 하는 하위 MAC 장치.

청구항 9.

무선 인터넷 시스템에서 데이터 암복호화 및 CRC(Cyclic Redundancy Code) 연산을 수행하는 하위 MAC(Media Access Control) 장치에 포함된 하향 링크 블록에서의 하향 링크 데이터 처리 방법에 있어서,

(a) 입력되는 하향 링크 데이터의 버스트 정보를 확인하는 단계;

(b) 암호화 및 CRC 생성을 위하여 필요한 제어 메시지 및 동작 시작 신호를 생성하여, 암호화 작업을 수행하는 암호 블록 및 CRC 생성 작업을 수행하는 CRC 생성 블록으로 전달하는 단계;

(c) 상기 암호 블록을 통하여 상기 하향 링크 데이터의 버스트에 대한 암호화 작업을 수행하고, 상기 암호화 작업이 완료된 데이터를 상기 CRC 생성 블록으로 전달하는 단계;

(d) 상기 CRC 생성 블록을 통해 상기 CRC 생성 작업을 수행하고, 생성된 상기 CRC를 상기 하향 링크 데이터의 마지막 부분에 첨가하는 단계; 및

(e) 상기 버스트의 개수를 하나 줄인 후, 상기 버스트의 개수가 0이 아니면 상기 단계 (b) 이후의 과정을 반복하고, 상기 버스트의 개수가 0이면 상기 하향 링크 데이터 처리 작업을 종료하는 단계

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 10.

제9항에 있어서, 상기 (a)는,

상위 MAC 계층으로부터 하향 링크 제어 신호선을 통해 상기 버스트 정보가 포함된 하향 링크 제어 정보와, 상기 하향 링크 데이터를 읽기 위한 신호(Ctrl Req, Data Req)를 수신하는 단계;

상기 Ctrl Req와 Data Req에 따라, 상기 하향 링크 제어 정보와 상기 하향 링크 데이터에 포함되어 있는 상기 버스트 정보를 확인하는 단계; 및

상기 버스트 정보를 통해 한 프레임에 속해 있는 버스트 개수를 확인하고, 상기 버스트 개수가 0이면 프레임 완료 신호를 출력하여 상기 하향 링크 데이터 처리 작업을 종료하고, 상기 버스트 개수가 0이 아니면 상기 단계 (b)로 진행하는 단계

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

Samsung Ex. 1004, Page 386 of 563

청구항 11.

제9항에 있어서, 상기 단계 (b)는,

버스트 시작 어드레스, 버스트 크기, 버스트 내부의 PDU 개수, PUD 암호화를 위한 초기 값, PDU 암호화를 위한 키 값을 포함하는 제어 메시지를 생성하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 12.

제9항에 있어서, 상기 단계 (c)는,

(c1) 상기 제어 신호를 통해 수신된 버스트 내부의 PDU 개수를 확인하는 단계;

(c2) 상기 PDU의 헤더 내에 포함되어 있는 암호화 정보를 이용하여, 상기 PDU의 페이로드 부분에 대한 암호화 작업을 수행하는 단계;

(c3) 상기 암호화된 PDU를 하향 링크 FIFO로 출력하는 단계; 및

(c4) 상기 PDU의 개수를 하나 감소시키고, 상기 단계 (c1) 이하의 과정을 반복하는 단계

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 13.

제12항에 있어서, 상기 단계 (c1)에 앞서서,

상기 하향 링크 데이터의 버스트를 읽기 위하여 메모리의 포인터 위치를 설정하는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 14.

제12항에 있어서, 상기 단계 (c3)와 상기 단계 (c4) 사이에,

상기 PDU 헤더에서 추출한 PDU 길이 정보를 이용하여, 상기 PDU의 크기를 누적하는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 15.

제14항에 있어서, 상기 (c1)은,

상기 PDU의 개수가 0이면, 상기 PDU 크기의 누적분과 상기 버스트 크기를 비교하는 단계; 및

상기 PDU 크기가 상기 버스트 크기보다 크면 비정상적으로 동작한 것으로 판단하여 암호 블록 오류 신호를 출력하고, 상기 버스트 크기가 상기 PDU 크기의 누적분보다 크면 상기 암호화 작업을 정상 종료시키는 단계

Samsung Ex. 1004, Page 387 of 563

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 16.

제1항에 있어서, 상기 단계 (d)는,

(d1) 상기 제어 신호를 통해 수신된 버스트 내부의 PDU 개수를 확인하는 단계;

(d2) 상기 PDU의 헤더 내에 포함되어 있는 CRC 생성 여부 정보를 확인하여, 상기 PDU의 페이로드까지의 CRC를 생성하는 단계;

(d3) 상기 PDU의 마지막 부분에 상기 CRC를 첨가하는 단계; 및

(d4) 상기 PDU의 개수를 하나 감소시키고, 상기 단계 (d1) 이하의 과정을 반복하는 단계

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 17.

제16항에 있어서, 상기 단계 (d1)과 상기 단계 (d2) 사이에,

상기 암호화가 종료된 데이터가 저장되는 하향 링크 FIFO로부터 상기 암호화된 PDU를 읽어오는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 18.

제16항에 있어서, 상기 단계 (d1) 이전에,

상기 CRC 생성 작업이 완료된 PDU를 저장하기 위한 메모리의 포인터 위치를 설정하는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 19.

제18항에 있어서, 상기 단계 (d3) 이후에,

상기 PDU 헤더에서 추출된 PDU 길이 정보를 이용하여, 상기 메모리의 포인터 위치를 상기 PDU 크기만큼 증가시키는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 20.

제16항에 있어서, 상기 단계 (d3) 이후에,

상기 PDU 헤더에서 추출한 PDU 길이 정보를 이용하여, 상기 PDU의 크기를 누적하는 단계

를 추가로 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 21.

제20항에 있어서, 상기 (d1)은,

상기 PDU의 개수가 0이면, 상기 PDU 크기의 누적분과 상기 버스트 크기를 비교하는 단계; 및

상기 PDU 크기의 누적분이 상기 버스트 크기보다 크면 비정상적으로 동작한 것으로 판단하여 CRC 생성 블록 오류 신호를 출력하고, 상기 PDU 크기의 누적분이 상기 버스트 크기보다 작으면 완료 신호를 생성하고 상기 CRC 작업을 종료하는 단계

를 포함하는 것을 특징으로 하는 하향 링크 데이터 처리 방법.

청구항 22.

무선 인터넷 시스템에서 데이터 암복호화 및 CRC(Cyclic Redundancy Code) 연산을 수행하는 하위 MAC(Media Access Control) 장치에 포함된 상향 링크 블록에서의 상향 링크 데이터 처리 방법에 있어서,

(a) 입력되는 상향 링크 데이터의 버스트 정보를 확인하는 단계;

(b) 복호화 및 CRC 확인을 위하여 필요한 제어 메시지 및 동작 시작 신호를 생성하여, 복호화 작업을 수행하는 복호 블록 및 상기 CRC 확인 작업을 수행하는 CRC 확인 블록으로 전달하는 단계;

(c) 상기 복호 블록을 통하여 상기 상향 링크 데이터의 버스트에 대한 복호화 작업을 수행하고, 상기 복호화 작업이 완료된 데이터를 상기 CRC 확인 블록으로 전달하는 단계;

(d) 상기 CRC 확인 블록을 통해 상기 CRC 확인 작업을 수행하는 단계; 및

(e) 상기 버스트의 개수를 하나 줄인 후, 상기 버스트의 개수가 0이 아니면 상기 단계 (b) 이후의 과정을 반복하고, 상기 버스트의 개수가 0이면 상기 상향 링크 데이터 처리 작업을 종료하는 단계

를 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 23.

제22항에 있어서, 상기 (a)는,

상위 MAC 계층으로부터 상향 링크 제어 신호선을 통해 상기 버스트 정보가 포함된 상향 링크 제어 정보와, 상기 상향 링크 데이터를 읽기 위한 신호(Ctrl Req, Data Req)를 수신하는 단계;

상기 Ctrl Req와 Data Req에 따라, 상기 상향 링크 제어 정보와 상기 상향 링크 데이터에 포함되어 있는 상기 버스트 정보를 확인하는 단계; 및

상기 버스트 정보를 통해 한 프레임에 속해 있는 버스트 개수를 확인하고, 상기 버스트 개수가 0이면 프레임 완료 신호를 출력하여 상기 상향 링크 데이터 처리 작업을 종료하고, 상기 버스트 개수가 0이 아니면 상기 단계 (b)로 진행하는 단계

를 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 24.

제22항에 있어서, 상기 단계 (b)는,

버스트 시작 어드레스, 버스트 크기, PUD 암호화를 위한 초기 값, PDU 암호화를 위한 키 값을 포함하는 제어 메시지를 생성하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 25.

제22항에 있어서, 상기 단계 (c)는,

(c1) 상기 제어 신호를 통해 수신된 버스트 크기와 상기 버스트 내부의 PDU 크기의 누적분을 비교하는 단계;

(c2) 상기 PDU의 헤더 내에 포함되어 있는 복호화 정보를 이용하여, 상기 PDU의 페이로드 부분에 대한 복호화 작업을 수행하는 단계;

(c3) 상기 복호화된 PDU를 상향 링크 FIFO로 출력하는 단계; 및

(c4) 상기 PDU 크기를 누적하고, 상기 단계 (c1) 이하의 과정을 반복하는 단계

를 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 26.

제25항에 있어서, 상기 (c1)은,

상기 버스트 크기가 상기 PDU 크기의 누적분보다 크면 상기 복호화 작업을 정상 종료시키고, 상기 버스트 크기가 상기 PDU 크기의 누적분보다 작으면 상기 단계 (c2)로 진행하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 27.

제22항에 있어서, 상기 단계 (d)는,

(d1) 상기 버스트 크기와 상기 버스트 내부의 PDU 크기의 누적분을 비교하는 단계;

(d2) 상기 PDU의 헤더부터 페이로드까지의 CRC를 확인하여, 에러 발생 여부를 확인하는 단계;

(d3) 상기 에러가 발생한 경우에는 CRC 오류 신호를 생성하여 출력하고, 상기 에러가 발생하지 않은 경우에는 상기 CRC 확인된 PDU를 출력시키고, PDU의 크기를 누적하여 상기 단계 (d1) 이하의 과정을 반복하는 단계;

를 추가로 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 28.

제27항에 있어서, 상기 단계 (d1)과 상기 단계 (d2) 사이에,

상기 복호화가 종료된 데이터가 저장되는 상향 링크 FIFO로부터 상기 복호화된 PDU를 읽어오는 단계

를 추가로 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 29.

제27항에 있어서, 상기 단계 (d1) 이전에,

상기 CRC 확인 작업이 완료된 PDU를 저장하기 위한 메모리의 포인터 위치를 설정하는 단계

를 추가로 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

청구항 30.

제29항에 있어서, 상기 단계 (d3) 이후에,

상기 PDU 헤더에서 추출된 PDU 길이 정보를 이용하여, 상기 메모리의 포인터 위치를 상기 PDU 크기만큼 증가시키는 단계

를 추가로 포함하는 것을 특징으로 하는 상향 링크 데이터 처리 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선 인터넷 시스템의 하위 매체 접근 계층 장치 및 그를 이용한 데이터 처리 방법에 관한 것이다. 더욱 상세하게는, IEEE 802.16 기반의 무선 인터넷 시스템에서, 고속 데이터 송수신을 위한 상위 제어 계층과 물리 계층을 이어주는 하위 매체 접근 제어(MAC: Media Access Control) 계층의 데이터 처리 장치 및 데이터 처리 방법에 관한 것이다.

전자, 통신 기술이 비약적으로 발전함에 따라 무선 통신망(Wireless Network)을 이용한 다양한 무선 통신 서비스가 제공되고 있다. 가장 기본적인 무선 통신 서비스는 이동통신 단말기 사용자들에게 무선으로 음성 통화를 제공하는 무선 음성 통화 서비스로서 이는 시간과 장소에 구애받지 않고 서비스를 제공할 수 있다는 특징이 있다. 또한, 문자 메시지 서비스를 제공하여 음성 통화 서비스를 보완해주는 한편, 최근에는 이동통신 단말기의 사용자에게 무선 통신망을 통해 인터넷 통신 서비스를 제공하는 무선 인터넷 서비스가 대두되었다.

이처럼 이동통신 기술의 발달로 인해 부호 분할 다중 접속(CDMA: Code Division Multiple Access) 이동통신 시스템에서 제공하는 서비스는 음성 서비스뿐만이 아니라, 써킷(Circuit) 데이터, 패킷(Packet) 데이터 등과 같은 데이터를 전송하는 멀티미디어 통신 서비스로 발전해 가고 있다.

또한, 최근에는 정보통신의 발달로 ITU-R에서 표준으로 제정하고 있는 제 3 세대 이동통신 시스템인 IMT-2000 (International Mobile Telecommunication 2000)(예컨대, CDMA2000 1X, 3X, EV-DO, WCDMA(WideBand CDMA) 등)이 상용화되고 있다. IMT-2000은 CDMA 2000 1X, 3X, EV-DO, WCDMA(WideBand CDMA) 등으로 기존의 IS-95A, IS-95B 망에서 진화한 IS-95C 망을 이용하여 IS-95A, IS-95B 망에서 지원 가능한 데이터 전송 속도인 14.4 Kbps나 56 Kbps보다 훨씬 빠른 최고 144 Kbps의 전송 속도로 무선 인터넷을 제공할 수 있는 서비스이다. 특히 IMT-2000 서비스를 이용하면 기존의 음성 및 WAP 서비스 품질의 향상은 물론 각종 멀티미디어 서비스(AOD, VOD 등)를 더욱 빠른 속도로 제공할 수 있다.

그러나, 기존의 이동통신 시스템은 기지국 구축 비용이 높기 때문에 무선 인터넷의 이용 요금이 높고, 이동통신 단말기의 화면 크기가 작기 때문에 이용할 수 있는 콘텐츠에 제약이 있는 등 초고속 무선 인터넷을 제공하기에는 한계가 있다. 또한, 무선 랜(Wireless Local Area Network) 기술은 전파 간섭 및 좁은 사용 영역(Coverage) 등의 문제로 공중 서비스의 제공에 한계가 있다. 따라서, 휴대성과 이동성이 보장하며 저렴한 요금으로 초고속 무선 인터넷 서비스를 이용할 수 있는 초고속 무선 인터넷(WiBro: Wireless Broadband 또는 HPi: High-Speed Portable internet) 시스템 등이 대두되었다. 이와 같은 무선 인터넷 시스템 및 연결 방법은 IEEE 802.16(광대역 무선 통신 표준)에 적용되어 있다. 또한, IEEE 802.16에는 무선 인터넷 시스템에서 데이터를 송수신하기 위한 계층 구조에 대해 정의되어 있다.

도 1은 무선 인터넷 시스템에서 통신을 수행하기 위한 기지국과 단말기의 계층 구조를 간략하게 나타낸 블록도이다.

무선 인터넷 시스템에서 데이터를 송수신하기 위한 기지국 및 단말기는 물리 계층(110), 하위 매체 접근 제어(MAC, 이하 'MAC'이라 칭함) 계층(120), 상위 MAC 계층(130) 및 및 서비스 수렴부 계층(140)을 포함한다.

물리 계층(110)은 무선 인터넷 시스템에서 기지국과 단말기 사이에 전송되는 데이터에 대한 전기적, 기계적인 인터페이스를 변형시키는 부분이다. 여기서, 광대역 무선 접속 통신망의 무선 인터넷 시스템에서 데이터 전송을 위한 물리 계층(110)의 전송 속도는 50 Mbps 이상으로 설정된다.

서비스 수렴부 계층(140)은 외부 망으로부터 수렴 부계층 서비스 액세스 포인트(CS SAP: Convergence Sublayer Service Access Point)를 통하여 수신된 데이터와, 수신된 MAC 서비스 데이터(SDU: Service Data Unit, 이하, 'SDU'라 칭함)를 변환 및 매핑해주는 역할을 수행한다. 외부로부터 수신된 SDU들을 적절한 MAC 서비스 절차 및 연결 식별자(CID: Connection IDentifer)들과의 매핑을 수행한다. 또한, 탑재물 헤더 억압(Payload Header Suppression)을 수행하는 부분이다.

상위 MAC 계층(130)은 MAC SDU를 이용하여 시스템 접속, 대역폭 할당, 연결 설정 및 연결 관리 등을 수행하며, 물리 계층(110)의 데이터 전송을 위한 데이터 프레임화 작업을 수행하고, 프레임 크기에 맞도록 데이터를 스케줄링하는 역할을 수행한다.

하위 MAC 계층(120)은 데이터 보호를 위한 암복호화 및 CRC(Cyclic Redundancy Code) 연산 등을 제공하며, 물리 계층의 제어 및 통계 자료 수집 등의 역할을 수행하여, 물리 계층(110)과 상위 MAC 계층(130)이 밀접한 관계를 갖도록 하는 부분이다.

도 2는 무선 인터넷 시스템에서 사용되는 데이터 프레임의 구조를 상세하게 나타낸 구조도이다.

상위 MAC 계층(130)의 프레임 형성은 2A와 같이 하향 링크 프레임과 상향 링크 프레임으로 나뉘어 있으며, 하나의 단말기에 하나의 버스트(Burst)가 할당된다. 2B를 통해 확인할 수 있듯이, 각 버스트 안에는 여러 개의 PDU가 존재하며, PDU는 2C와 같이 PDU 헤더(Header), 실제 데이터 영역인 페이로드(Payload) 및 데이터 수신 측의 PDU 헤더와 페이로드의 오류 확인을 위하여 첨가시키는 CRC 영역으로 구성된다. 그리고, 보안을 위하여 데이터 영역인 페이로드 영역을 암호화한다.

하위 MAC 계층(120)에서 암호화와 CRC를 생성하기 위해서는, 먼저 메모리에서 해당 PDU의 데이터 영역을 읽어 암호화한 뒤 메모리에 저장한다. 그리고, CRC 연산을 수행하기 위하여 다시 PDU의 데이터가 저장된 메모리를 읽어 CRC 연산을 수행한다. 이에 따라, 하위 MAC 계층(120)이 메모리를 두 번 읽어야하므로 하위 MAC 계층(120)의 연산 속도가 떨어지게 되고, 이에 따라 데이터의 병목 현상이 발생하여 전체 시스템의 속도가 느려지는 단점이 있다.

즉, 무선 인터넷 시스템에서의 물리 계층(110)의 데이터 전송 속도는 50 Mbps 이상이지만, 하위 MAC 계층(120)에서 데이터 병목 현상을 발생시켜 데이터 처리 속도를 떨어뜨리게 된다.

이와 같은 데이터 처리 속도의 향상을 위하여, 국내 특허 출원 2002-0080316 '무선랜 시스템 장치와 매체접근제어를 통한 데이터 송수신 및 그 운용 방법'(2002.12.16), 국내 특허 출원 1999-0059967 '무선 이동 단말 장치의 매체접근제어 처리 장치'(1999.12.21) 및 국내 특허 출원 2003-0000601 '무선 랜에서 매체 접근 제어 방법 및 장치'(2003.1.6)를 통해서, QoS 보장을 위한 무선랜 시스템 장치, 물리 계층에서 만들어진 프레임(MSDU)을 비동기식 버스 제어 방식으로 처리하는

Samsung Ex. 1004, Page 392 of 563

MAC 처리 장치 및 여러 개의 큐를 두어 헤더 비교 없이 데이터를 구분할 수 있는 MAC 처리 장치를 제공하고 있으나, 하위 MAC 계층(120)에서 발생하는 시간 지연을 없애는 장치는 제공되고 있지 못하여, 데이터 처리 속도의 향상에 한계를 가지게 된다.

이에 따라, 무선 인터넷에서 고속의 다양한 데이터를 처리하기 위해서 하위 MAC 계층(120)에서 발생하는 시간 지연을 없애는 고속 연산 장치가 요구되고 있다.

발명이 이루고자 하는 기술적 과제

이와 같은 문제점을 해결하기 위하여, 본 발명은 메모리에서 PDU 데이터를 한 번만 읽어와서 암복호화 기능과 CRC 연산을 동시에 수행함으로써, 시간 지연 없이 데이터를 처리할 수 있는 하위 MAC 장치와 하위 MAC 장치를 이용한 데이터 처리 방법을 제공한다.

발명의 구성

이러한 기술적 과제를 달성하기 위하여 본 발명은 하위 MAC 장치로서, 무선 인터넷 시스템에서 데이터의 암복호화 및 CRC 연산을 수행하는 하위 MAC 장치에 있어서, 물리 계층과 데이터 신호 및 제어 신호를 송수신하는 물리 계층 인터페이스 블록; 상위 MAC 계층과 데이터 신호 및 제어 신호를 송수신하는 상위 MAC 인터페이스 블록; 상향 링크 데이터에 필요한 복호화 작업 및 CRC 확인 작업을 수행하는 상향 링크 블록; 하향 링크 데이터에 필요한 암호화 작업 및 CRC 생성 작업을 수행하는 하향 링크 블록; 및 물리 계층 인터페이스 블록, 상위 MAC 인터페이스 블록, 상향 링크 블록 및 하향 링크 블록 사이에 전달되는 제어 정보 및 데이터를 저장하는 메모리를 포함한다.

또한, 제2의 기술적 과제를 달성하기 위하여 본 발명은 하향 링크 데이터 처리 방법으로서, 무선 인터넷 시스템에서 데이터 암복호화 및 CRC 연산을 수행하는 하위 MAC 장치에 포함된 하향 링크 블록에서의 하향 링크 데이터 처리 방법에 있어서, (a) 입력되는 하향 링크 데이터의 버스트 정보를 확인하는 단계; (b) 암호화 및 CRC 생성을 위하여 필요한 제어 메시지 및 동작 시작 신호를 생성하여, 암호화 작업을 수행하는 암호 블록 및 CRC 생성 작업을 수행하는 CRC 생성 블록으로 전달하는 단계; (c) 암호 블록을 통하여 하향 링크 데이터의 버스트에 대한 암호화 작업을 수행하고, 암호화 작업이 완료된 데이터를 CRC 생성 블록으로 전달하는 단계; (d) CRC 생성 블록을 통해 CRC 생성 작업을 수행하고, 생성된 CRC를 하향 링크 데이터의 마지막 부분에 첨가하는 단계; 및 (e) 버스트의 개수를 하나 줄인 후, 버스트의 개수가 0이 아니면 단계 (b) 이후의 과정을 반복하고, 버스트의 개수가 0이면 하향 링크 데이터 처리 작업을 종료하는 단계를 포함한다.

또한, 제3의 기술적 과제를 달성하기 위하여 본 발명은 상향 링크 데이터 처리 방법으로서, 무선 인터넷 시스템에서 데이터 암복호화 및 CRC 연산을 수행하는 하위 MAC 장치에 포함된 상향 링크 블록에서의 상향 링크 데이터 처리 방법에 있어서, (a) 입력되는 상향 링크 데이터의 버스트 정보를 확인하는 단계; (b) 복호화 및 CRC 확인을 위하여 필요한 제어 메시지 및 동작 시작 신호를 생성하여, 복호화 작업을 수행하는 복호 블록 및 CRC 확인 작업을 수행하는 CRC 확인 블록으로 전달하는 단계; (c) 복호 블록을 통하여 상향 링크 데이터의 버스트에 대한 복호화 작업을 수행하고, 복호화 작업이 완료된 데이터를 CRC 확인 블록으로 전달하는 단계; (d) CRC 확인 블록을 통해 CRC 확인 작업을 수행하는 단계; 및 (e) 버스트의 개수를 하나 줄인 후, 버스트의 개수가 0이 아니면 단계 (b) 이후의 과정을 반복하고, 버스트의 개수가 0이면 상향 링크 데이터 처리 작업을 종료하는 단계를 포함한다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

또한, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

또한, 본 명세서에서 기재한 모듈(module)이란 용어는 특정한 기능이나 동작을 처리하는 하나의 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현할 수 있다.

도 3은 본 발명에 따른 하위 MAC 장치의 구조를 간략하게 나타낸 블록 구성도이다.

Samsung Ex. 1004, Page 393 of 563

본 발명에 따른 하위 MAC 장치는 상위 MAC 계층(130)에서 물리 계층(110)으로 전달하거나, 물리 계층(110)에서 상위 MAC 계층(130)으로 대용량 데이터가 고속으로 전달하기 위한 하위 MAC 장치로써, 물리 계층 인터페이스 블록(310), 상향 링크 블록(330), 상위 MAC 인터페이스 블록(350), 하향 링크 블록(370) 및 메모리(320, 340, 360, 380)를 포함한다.

물리 계층 인터페이스 블록(310)은 물리 계층(110)에 데이터를 쓰거나 물리 계층(110)으로부터 전달되는 데이터를 읽고, 물리 계층(110)에 필요한 제어 신호를 전달하는 기능을 수행한다.

상향 링크 블록(330)은 물리 계층 인터페이스 블록(310)을 통해 전달된 상향 링크 데이터에 필요한 복호화 작업과 CRC 확인 작업을 수행하는 부분이다. 상향 링크 블록(330)의 구조에 대해서는 도 8을 통해 상세하게 설명하기로 한다.

상위 MAC 인터페이스 블록(350)은 상위 MAC 계층(130)과 인터페이스를 하면서, 상위 MAC 계층(130)에서 전달받은 제어 정보와 데이터를 분리하여 메모리(340, 360)에 쓰거나, 메모리(340)에 저장된 데이터를 읽고, 하위 MAC 계층(120)에서 생성된 제어 신호를 상위 MAC 계층(130)으로 전달하는 기능을 수행한다.

그리고, 상위 MAC 인터페이스 블록(350)은 상향 링크 블록(330)과 상향 링크 제어 신호를 송수신하기 위한 상향 링크 제어 신호선을 통하여 연결되어 있으며, 하향 링크 블록(370)과 하향 링크 제어 신호를 송수신하기 위한 하향 링크 제어 신호선을 통하여 연결되어 있다.

하향 링크 블록(370)은 상위 MAC 인터페이스 블록(350)을 통해 전달받은 하향 링크 데이터에 필요한 암호화 작업 및 CRC 생성 작업을 수행하는 부분이다. 상향 링크 블록(370)의 구조에 대해서는 도 4를 통해 상세하게 설명하기로 한다.

메모리(320, 340, 360, 380)는 각 블록 사이에 전달되는 데이터를 저장하는 부분이다.

물리 계층 인터페이스 블록(310)과 상향 링크 블록(330) 사이에는 전달되는 제어 정보 및 데이터 저장을 위한 상향 링크 물리 계층 메모리(320)가 존재하며, 상향 링크 물리 계층 메모리(320)는 상향 링크 블록(330)으로부터 물리 계층 인터페이스 블록(310)으로 전달되는 제어 정보를 저장하는 상향 링크 물리 계층 제어 정보 메모리(322)와, 물리 계층 인터페이스 블록(310)으로부터 상향 링크 블록(330)으로 전달되는 데이터를 저장하는 상향 링크 물리 계층 데이터 메모리(324)가 포함된다.

상향 링크 블록(330)과 상위 MAC 인터페이스 블록(350) 사이에는 전달되는 제어 정보 및 데이터 저장을 위하여 상향 링크 메모리(340)가 존재하며, 상향 링크 메모리(340)는 상위 MAC 인터페이스 블록(350)으로부터 상향 링크 블록(330)으로 전달되는 제어 정보를 저장하는 상향 링크 제어 정보 메모리(342)와, 상향 링크 블록(330)으로부터 상위 MAC 인터페이스 블록(350)으로 전달되는 데이터를 저장하는 상향 링크 데이터 메모리(344)가 포함된다.

하향 링크 블록(370)과 상위 MAC 인터페이스 블록(350) 사이에는 전달되는 제어 정보 및 데이터 저장을 위하여 하향 링크 메모리(360)가 존재하며, 하향 링크 메모리(360)는 상위 MAC 인터페이스 블록(350)으로부터 하향 링크 블록(370)으로 전달되는 제어 정보를 저장하는 하향 링크 제어 정보 메모리(362)와, 데이터를 저장하는 하향 링크 데이터 메모리(364)가 포함된다.

하향 링크 블록(370)과 물리 계층 인터페이스 블록(310) 사이에는 전달되는 제어 정보 및 데이터 저장을 위하여 하향 링크 물리 계층 메모리(380)가 존재하며, 하향 링크 메모리(380)는 하향 링크 블록(370)으로부터 물리 계층 인터페이스 블록(310)으로 전달되는 제어 정보를 저장하는 하향 링크 물리 계층 제어 정보 메모리(382)와, 데이터를 저장하는 하향 링크 물리 계층 데이터 메모리(384)가 포함된다.

도 4는 본 발명의 실시예에 따른 하위 MAC 블록 내의 하향 링크 블록의 구조를 나타낸 블록 구성도이다.

하향 링크 블록(370)은 하향 링크 제어 블록(410), 암호 블록(420), 하향 링크 FIFO(First-In First-Out)(430), CRC 생성 블록(440)을 포함한다.

하향 링크 제어 블록(410)은 암호 블록(420), CRC 생성 블록(440)을 제어하며 각 블록에 대한 오류 정보를 상위 MAC 계층(130)으로 보고하고, 암호 블록(420), CRC 생성 블록(440)을 초기화하는 기능을 포함한다.

암호 블록(420)은 입력되는 데이터의 PDU 페이로드에 대하여 블록 암호화 알고리즘을 수행하는 부분이고, 하향 링크 FIFO(430)는 입력되는 하향 링크 데이터의 처리 순서, 호출 순서 등을 관리하는 부분이며, CRC 생성 블록(440)은 입력되는 데이터에 대해 PDU 단위의 CRC를 생성하는 부분이다.

이와 같이 하향 링크 블록(370)은 암호 블록(420), CRC 생성 블록(440) 사이에 하향 링크 FIFO(430)를 사용함으로써, 하향 링크 FIFO(430)의 플래그 신호를 이용하여 데이터 흐름의 지연 없이, 암호 블록(420)에서 CRC 생성 블록(440)으로 데이터를 전송할 수 있다. 즉, 종래의 방법에 따라 하향 링크 데이터 모두에 대해 암호화를 실행한 후, 메모리에 저장하고, 다시 CRC 형성을 위하여 메모리에서 데이터를 읽게 되면, 두 번에 걸친 메모리 접근으로 인하여 시간 지연 및 프레임 데이터를 저장할 메모리가 여러 개 필요하게 되어 시스템이 커지며, 비용도 많이 소모된다.

따라서, 본 발명의 실시예에 따라, 암호 블록(420)과 CRC 생성 블록(440) 사이에 하향 링크 FIFO(430)를 구성하게 되면, 하나의 PDU에 대하여 암호화가 진행되는 중에 데이터가 순차적으로 하향 링크 FIFO(430)에 입력 가능하며, 하향 링크 FIFO(430)의 플래그 신호를 감지하고 있는 CRC 생성 블록(440)은 데이터 입력과 동시에 하향 링크 FIFO(430)에서 헤더를 포함한 데이터를 입력받아 CRC 연산을 수행하게 되므로, 블록 암호화와 CRC 생성을 지연 없이 진행시킬 수 있으며, 데이터 입출력이 바로 실행되므로, 데이터 보관에 필요한 큰 사이즈의 하향 링크 FIFO(430)가 필요 없게 된다.

하향 링크 블록(370)에서 버스트에 대한 제어 정보는 상위 MAC계층(130)에서 전달받아 버스트 개수와 PDU 개수를 알 수 있으므로, PDU 개수로 버스트 연산 완료 시점을 알 수 있고, PDU 길이 누적분과, 버스트 크기를 비교함으로써, 버스트 연산에 따른 블록 에러를 확인할 수 있다. 그리고, 확인된 에러 정보를 이용하여 하향 링크 제어 블록(420)은 다른 블록을 초기화시킬 수 있다.

여기서, 본 발명의 실시예에 따른 하향 링크 제어 블록(410), 암호 블록(420), CRC 생성 블록(440)의 기능에 대해서는 도 5 내지 도 7을 통해 상세하게 설명하기로 한다.

도 5는 본 발명의 실시예에 따른 하향링크 제어 블록의 기능을 설명하기 위한 순서도이다.

하향 링크 제어 블록(410)은 하향 링크 제어 신호선을 통하여 각 버스트에 대한 정보를 저장하고 있는 하향 링크 제어 정보와, 데이터를 읽으라는 신호(Ctrl Req, Data Req)를 수신한다(S510).

이와 같이 Ctrl Req, Data Req가 수신되면, 하향 링크 제어 블록(410)은 하향 링크 제어 정보 및 데이터를 읽기 위하여, 각 버스트에 대한 정보를 저장하고 있는 하향 링크 제어 정보 메모리(362)에서 한 프레임에 속해 있는 버스트 개수를 입력받는다(S520).

하향 링크 제어 블록(410)은 입력된 버스트의 개수를 확인한다(S530). 이 때, 버스트 개수가 '0'인 경우에는, 연산에 필요한 버스트가 없는 것이므로, 프레임 완료 신호를 출력하고, 데이터 처리 작업을 종료한다(S532).

S530 단계에서, 버스트 개수가 '0'이 아님이 확인된 경우에는, 하향 링크 제어 정보 메모리(362)에서 하나의 버스트 정보를 읽어 물리 계층(110)에 필요한 제어 메시지를 생성한 후, 하향 링크 물리 계층 제어 정보 메모리(382)로 출력한다(S540).

그리고, 하향 링크 제어 정보 메모리(362)에서는 하나의 버스트 정보를 해석하는 동시에(S550), 암호 블록(420)과 CRC 생성 블록(440)에 필요한 제어 메시지와, 동작 시작을 알리는 시작(Start) 신호를 생성하여 암호 블록(420) 및 CRC 생성 블록(440)으로 출력한다. 이 때, 암호 블록(420)과 CRC 생성 블록(440)으로 전달하는 제어 메시지로서, 버스트 시작 어드레스, 버스트 크기, 버스트 내부의 PDU 개수, PDU 암호화를 위한 초기 값, PDU 암호화를 위한 키 값 등을 출력하게 된다(S560).

이와 같이, 하향 링크 제어 블록(410)은 암호 블록(420) 및 CRC 생성 블록(440)으로 제어 메시지 및 시작 신호가 전달한 후, CRC 생성 블록(440)으로부터의 버스트 연산 완료 신호 수신을 기다린다. CRC 생성 블록(440)에서 버스트의 CRC 생성이 완료되어 버스트 연산 완료 신호가 전달되면(S570), 버스트 개수를 하나 줄인 후, S530 단계 이후의 과정을 반복한다(S580). 이와 같은 작업은 버스트 개수가 '0'이 되어 S532 단계로 진행될 때까지 반복된다.

도 6은 본 발명의 실시예에 따른 암호 블록의 기능을 설명하기 위한 순서도이다.

암호 블록(420)은 하향 링크 제어 블록(410)으로부터 S560 단계를 통해, 버스트 시작 어드레스, 버스트 크기, 버스트 내부의 PDU 개수, PDU 암호화를 위한 초기 값 및 PDU 암호화를 위한 키 값이 포함된 제어 메시지 및 시작 메시지를 수신하면, 암호화를 위한 동작을 시작한다(S610).

암호 블록(420)은 수신된 버스트 시작 어드레스를 통해 하향 링크 데이터 메모리(364)로부터 버스트를 읽기 위한 메모리 포인터 위치를 설정하고, PDU 누적 레지스터를 초기화시킨다(S620).

그리고, 수신된 제어 메시지 내에 포함되어 있는 버스트 내부의 PDU 개수를 확인한다(S630). 이 때, PDU 개수가 '0'이 아니면, 하향 링크 데이터 메모리(364)에서 버스트의 PDU를 해석하여 암호화 여부를 판단한다. 여기서, PDU 헤더 내에는 암호화 여부에 대한 정보를 포함하고 있는 필드가 존재한다. 그리고, PDU의 헤더 정보에 따라 하향 링크 제어 블록(410)에서 입력받은 암호화 정보를 이용하여, PDU 내의 페이로드 부분에 대하여 암호화 작업을 수행한다(S640).

그리고, PDU 내의 페이로드 부분에 대한 암호화 작업이 완료되면, 암호화된 페이로드를 하향 링크 FIFO(430)로 출력한다(S650).

그리고, PDU 헤더에서 추출한 PDU 길이 정보를 이용하여 다음 PDU를 읽기 위한 메모리 포인터의 위치를 재설정하고, 각 PDU의 크기를 누적한다(S660). 그리고, PDU의 개수를 하나 감소시켜 다시 S630 단계 이후의 과정을 반복하여 실행한다(S670).

여기서, S630 단계에서 PDU 개수를 확인한 결과 '0'이면, PDU 크기의 누적분과 버스트 크기를 비교한다(S632). 이 때, 버스트 크기가 PDU 크기의 누적분보다 큰 경우에는 암호 블록(420)이 버스트에 대하여 정상 동작을 실행한 것이므로, 정상적으로 종료시킨다. 그러나, PDU 크기의 누적분이 버스트 크기보다 큰 경우에는, 암호 블록(420)이 버스트에 대하여 비정상적으로 동작한 것이므로, 하향 링크 제어 블록(410)으로 암호 블록 오류 신호를 생성하여 출력한다(S634).

도 7은 본 발명의 실시예에 따른 CRC 생성 블록의 기능을 설명하기 위한 순서도이다.

CRC 생성 블록(440)은 하향 링크 제어 블록(410)으로부터 S560 단계를 통해, 버스트 크기와 버스트 내부의 PDU 개수에 관한 정보를 포함하는 제어 메시지 및 시작 메시지를 수신하면, CRC 생성 작업을 시작한다. 이 때, 하향 링크 FIFO(430)의 Empty 신호도 수신한다(S710).

CRC 생성 블록(440)은 CRC 생성 작업이 완료된 PDU를 하향 링크 물리 계층 데이터 메모리(384)에 저장시킬 메모리 포인터를 설정하고, PDU 누적 레지스터를 초기화시킨다(S720).

그리고, 수신된 제어 메시지 내에 포함되어 있는 버스트 내부의 PDU 개수를 확인한다(S730). 이 때, PDU 개수가 '0'이 아니면, 하향 링크 FIFO(430)에서 PDU를 읽어 온다. 이 때, PDU 헤더 내에는 CRC 생성 여부에 대한 정보를 포함하고 있는 필드가 존재한다. PDU 헤더 내의 CRC 생성 여부 정보에 따라, PDU 헤더에서부터 페이로드까지 CRC 생성 작업을 수행한다(S740).

그리고, PDU의 마지막 부분에 생성된 CRC를 첨가하고, 하향 링크 물리 계층 데이터 메모리(384)로 출력시킨다(S750).

그리고, PDU 헤더에서 추출한 PDU 길이 정보를 이용하여 다음 PDU를 쓰기 위한 메모리 포인터를 PDU 크기만큼 증가시키고, 각 PDU의 크기를 누적한다(S760).

그리고, PDU의 개수를 하나 감소시켜 다시 S730 단계 이후의 과정을 반복하여 실행한다(S770).

여기서, S730 단계에서 PDU 개수를 확인한 결과 '0'이면, PDU 크기의 누적분과 버스트 크기를 비교한다(S732). 이 때, 버스트 크기가 PDU 크기의 누적분보다 큰 경우에는 CRC 생성 블록(440)이 버스트에 대하여 정상 동작을 실행한 것이므로, 하향 링크 제어 블록(410)으로 완료 신호를 출력하고, 정상적으로 종료시킨다(S734). 그러나, PDU 크기의 누적분이 버스트 크기보다 큰 경우에는, CRC 생성 블록(440)이 버스트에 대하여 비정상적으로 동작한 것이므로, 하향 링크 제어 블록(410)으로 CRC 생성 블록 오류 신호를 생성하여 출력한다(S736).

도 8은 본 발명의 실시예에 따른 하위 MAC 블록 내의 상향 링크 블록의 구조를 나타낸 블록 구성도이다.

Samsung Ex. 1004, Page 396 of 563

상향 링크 블록(330)은 상향 링크 제어 블록(810), 복호 블록(820), 상향 링크 FIFO(First-In First-Out)(830), CRC 확인 블록(840)을 포함한다.

상향 링크 제어 블록(810)은 복호 블록(820), CRC 확인 블록(840)을 제어하며 각 블록에 대한 오류 정보를 상위 MAC 계층(130)으로 보고하고, 복호 블록(820), CRC 확인 블록(840)을 초기화하는 기능을 포함한다.

복호 블록(820)은 입력되는 데이터의 PDU 페이로드에 대하여 블록 복호화 알고리즘을 수행하는 부분이고, 상향 링크 FIFO(830)는 입력되는 상향 링크 데이터의 처리 순서, 호출 순서 등을 관리하는 부분이며, CRC 확인 블록(840)은 입력되는 데이터에 대해 PDU 단위의 CRC를 확인하는 부분이다.

상향 링크 블록(330)에서도 복호 블록(820)과 CRC 확인 블록(840) 사이에 상향 링크 FIFO(830)를 사용하며, 상량 링크 FIFO(830)를 사용하는 이유는 앞서 언급된 하향 링크 FIFO(430)의 사용 이유와 동일하다.

상향 링크 블록(330)에서 버스트에 대한 제어 정보는 상위 MAC계층(130)에서 전달받아 버스트 개수는 알 수 있지만, 버스트 내의 PDU는 단말기에서 생성되므로, 하향 링크 블록(370)에서처럼 PDU의 개수를 알 수는 없다. 따라서, 버스트에 대한 크기 정보와 연산에 따른 PDU 길이 누적을 비교함으로써, 버스트의 완료 시점을 알 수 있다.

여기서, 본 발명에 따른 상향 링크 제어 블록(810), 복호 블록(820), CRC 확인 블록(840)의 기능에 대해서는 도 9 내지 도 11을 통해 상세하게 설명하기로 한다.

도 9는 본 발명의 실시예에 따른 상향 링크 제어 블록의 기능을 설명하기 위한 순서도이다.

상향 링크 제어 블록(810)은 상향 링크 제어 신호선을 통하여 각 버스트에 대한 정보를 저장하고 있는 상향 링크 제어 정보와, 데이터를 읽으라는 신호(Ctrl Req, Data Req)를 수신한다(S910)

이와 같이 Ctrl Req, Data Req가 수신되면, 상향 링크 제어 블록(810)은 상향 링크 제어 정보 및 데이터를 읽기 위하여, 각 버스트에 대한 정보를 저장하고 있는 상향 링크 제어 정보 메모리(342)에서 한 프레임에 속해 있는 버스트 개수를 입력받는다(S920).

상향 링크 제어 블록(810)은 입력된 버스트의 개수를 확인한다(S930). 이 때, 버스트 개수가 '0'인 경우에는, 연산에 필요한 버스트가 없는 것이므로, 프레임 완료 신호를 출력하고, 데이터 처리 작업을 종료한다(S932).

S930 단계에서, 버스트 개수가 '0'이 아님이 확인된 경우에는, 상향 링크 제어 정보 메모리(362)에서 하나의 버스트 정보를 읽어 물리 계층(110)에 필요한 제어 메시지를 생성한 후, 상향 링크 물리 계층 제어 정보 메모리(322)로 출력한다(S940).

그리고, 상향 링크 제어 정보 메모리(342)에서 하나의 버스트 정보를 해석하는 동시에(S950), 복호 블록(820)과 CRC 확인 블록(840)에 필요한 제어 메시지와, 동작 시작을 알리는 시작(Start) 신호를 생성하여 복호 블록(820) 및 CRC 확인 블록(840)으로 출력한다. 이 때, 복호 블록(820)과 CRC 확인 블록(840)으로 전달하는 제어 메시지로서, 버스트 시작 어드레스, 버스트 크기, PDU 복호화를 위한 초기 값, PDU 복호화를 위한 키 값 등을 출력하게 된다(S960).

이와 같이, 상향 링크 제어 블록(810)은 복호 블록(820) 및 CRC 확인 블록(840)으로 제어 메시지 및 시작 신호가 전달한 후, CRC 확인 블록(840)으로부터의 버스트 연산 완료 신호 수신을 기다린다. CRC 확인 블록(840)에서 버스트의 CRC 확인이 완료되어 버스트 연산 완료 신호가 전달되면(S970), 버스트 개수를 하나 줄인 후, S930 단계 이후의 과정을 반복한다(S980). 이와 같은 작업은 버스트 개수가 '0'이 되어 S932 단계로 진행될 때까지 반복된다.

도 10은 본 발명의 실시예에 따른 복호 블록의 기능을 설명하기 위한 순서도이다.

복호 블록(820)은 상향 링크 제어 블록(810)으로부터 S960 단계를 통해, 버스트 시작 어드레스, 버스트 크기, PDU 암호화를 위한 초기 값 및 PDU 암호화를 위한 키 값이 포함된 제어 메시지 및 시작 메시지를 수신하면, 복호화를 위한 동작을 시작한다(S1010).

Samsung Ex. 1004, Page 397 of 563

복호 블록(820)은 수신된 버스트 시작 어드레스를 통해 상향 링크 데이터 메모리(344)에 복호화 작업이 처리된 데이터를 저장할 메모리 포인터 위치를 설정하고, PDU 누적 레지스터를 초기화시킨다(S1020).

그리고, PDU 크기의 누적분과 버스트 크기를 비교한다. 이 때, 버스트 크기가 PDU 크기 누적분보다 큰 경우에는 버스트 연산을 종료시킨다(S1030).

그러나, PDU 크기의 누적분과 버스트 크기를 비교한 결과, PDU 크기 누적분이 버스트 크기보다 큰 경우에는, 버스트 내의 PDU를 확인하여 PDU 헤더 정보를 확인한다. 여기서, PDU 헤더 내에는 복호화에 필요한 복호화 정보를 포함하고 있는 필드가 존재한다. 그리고, 상향 링크 제어 블록(810)에서 전달받은 복호화 정보를 이용하여 PDU 내의 페이로드 부분에 대하여 복호화 작업을 수행한다(S1040).

그리고, PDU 내의 페이로드 부분에 대한 복호화 작업이 완료되면, 복호화된 페이로드를 상향 링크 FIFO(830)로 출력한다(S1050).

그리고, PDU 헤더에서 추출한 PDU 길이 정보를 이용하여 다음 PDU를 읽기 위한 메모리 포인터의 위치를 재설정하고, 각 PDU의 크기를 누적하는 단계를 거쳐 다시 S1030 단계 이후의 과정을 반복하여 실행한다(S1060).

여기서, 복호 블록(820)에서 연산된 데이터는 바로 상향 링크 FIFO(830)로 입력되며, 상향 링크 FIFO(830)에 입력되는 순간 상향 링크 FIFO(830)의 Empty 신호(EF: Empty Flag)를 이용하여, CRC 확인 블록(840)이 상향 링크 FIFO(830)에서 PDU를 입력받아 동작할 수 있다. 이에 따라 복호 블록(820)과 거의 동시에 PDU에 대한 CRC 연산을 수행할 수 있다.

도 11은 본 발명의 실시예에 따른 CRC 확인 블록의 기능을 설명하기 위한 순서도이다.

CRC 확인 블록(840)이 상향 링크 제어 블록(810)으로부터 S960 단계를 통하여 버스트 크기 정보가 포함된 제어 메시지, 시작 메시지 및 상향 링크 FIFO(830)의 Empty 신호를 수신하면, CRC 확인 작업을 시작한다(S1110).

CRC 확인 블록(840)은 CRC 확인 작업이 완료되면, 완료된 PDU를 상향 링크 데이터 메모리(344)에 저장시킬 메모리 포인터의 위치를 설정하고, PDU 누적 레지스터를 초기화시킨다(S1120).

그리고, PDU 크기의 누적분과 버스트 크기를 비교한다(S1130). 이 때, 버스트 크기가 PDU 크기 누적분보다 큰 경우에는 상향 링크 제어 블록(810)으로 CRC 확인 작업의 완료 신호를 출력하고, 정상적으로 종료시킨다(S1132).

그러나, PDU 크기의 누적분과 버스트 크기를 비교한 결과, PDU 크기 누적분이 버스트 크기보다 큰 경우에는, 상향 링크 FIFO(830)에서 PDU를 읽어 온다. 이 때, PDU 헤더 내에는 복호화에 필요한 복호화 정보를 포함하고 있는 필드가 존재한다. 그리고, PDU 헤더에서부터 페이로드까지 CRC 확인 작업을 수행한다(S1140).

그리고, CRC 확인 작업을 수행함과 동시에, CRC 에러가 발생하는지 여부를 확인한다(S1150). 이 때, CRC 에러가 발생하지 않는 경우에는 PDU를 상향 링크 데이터 메모리(344)로 출력하고(S1160), PDU 헤더에서 추출한 PDU 길이 정보를 이용하여 다음 PDU를 쓰기 위한 메모리 포인터를 PDU 크기만큼 증가시키고, 각 PDU의 크기를 누적한다. 그리고, S1130 단계 이후의 과정을 반복하여 실행한다(S1170).

여기서, S1150 단계에서 CRC 에러가 발생한 경우에는 상향 링크 제어 블록(810)으로 CRC 오류 신호를 생성하여 출력시킨다(S1162).

이와 같이 구성되는 상향 링크 블록(330) 및 하향 링크 블록(370)을 포함하는 하위 MAC 계층을 통하여 빠른 데이터 처리를 수행할 수 있다.

이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

Samsung Ex. 1004, Page 398 of 563

이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

전술한 구성에 의하여, 하위 MAC 계층에서 상위 MAC 계층으로 전달되는 대용량의 데이터에 대하여 시간 지연 없이 암호화와 데이터에 대한 CRC 생성 작업을 수행하여 물리 계층으로 전달함으로써, 대용량 데이터의 실시간 통신이 가능하다. 또한, 하위 MAC 계층은 물리 계층에서 전달되는 다양한 단말 데이터에 대하여 시간 지연 없이 복호화와 CRC 확인 작업을 수행하여 상위 MAC 계층으로 실시간 전달이 가능해진다. 이와 같이, 본 발명에 따라 시스템의 고속화와 대용량화가 가능해지는 효과를 기대할 수 있다.

도면의 간단한 설명

도 1은 무선 인터넷 시스템에서 통신을 수행하기 위한 기지국과 단말기의 계층 구조를 간략하게 나타낸 블록도,

도 2는 무선 인터넷 시스템에서 사용되는 데이터 프레임의 구조를 상세하게 나타낸 구조도,

도 3은 본 발명에 따른 하위 MAC 장치의 구조를 간략하게 나타낸 블록 구성도,

도 4는 본 발명의 실시예에 따른 하위 MAC 블록 내의 하향 링크 블록의 구조를 나타낸 블록 구성도,

도 5는 본 발명의 실시예에 따른 하향링크 제어 블록의 기능을 설명하기 위한 순서도,

도 6은 본 발명의 실시예에 따른 암호 블록의 기능을 설명하기 위한 순서도,

도 7은 본 발명의 실시예에 따른 CRC 생성 블록의 기능을 설명하기 위한 순서도,

도 8은 본 발명의 실시예에 따른 하위 MAC 블록 내의 상향 링크 블록의 구조를 나타낸 블록 구성도,

도 9는 본 발명의 실시예에 따른 상향 링크 제어 블록의 기능을 설명하기 위한 순서도,

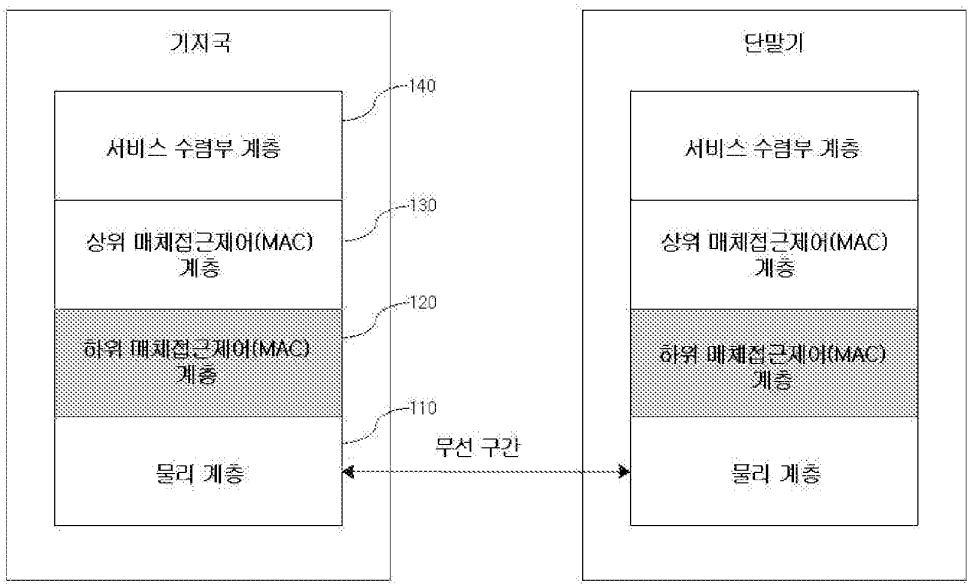
도 10은 본 발명의 실시예에 따른 복호 블록의 기능을 설명하기 위한 순서도,

도 11은 본 발명의 실시예에 따른 CRC 확인 블록의 기능을 설명하기 위한 순서도이다.

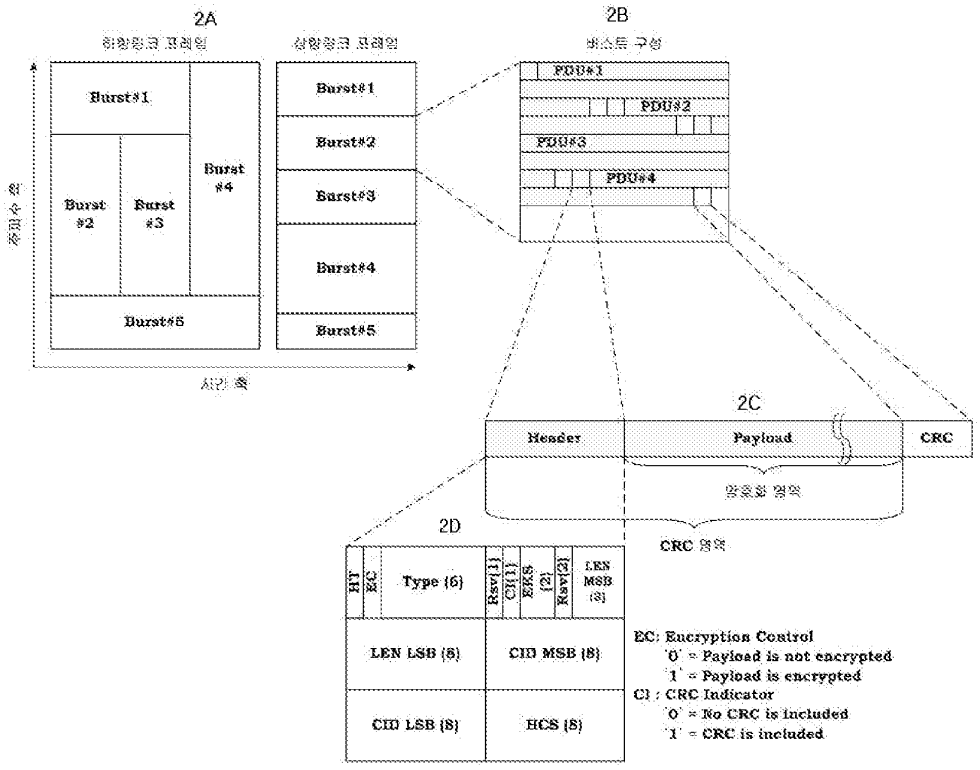
도면

Samsung Ex. 1004, Page 399 of 563

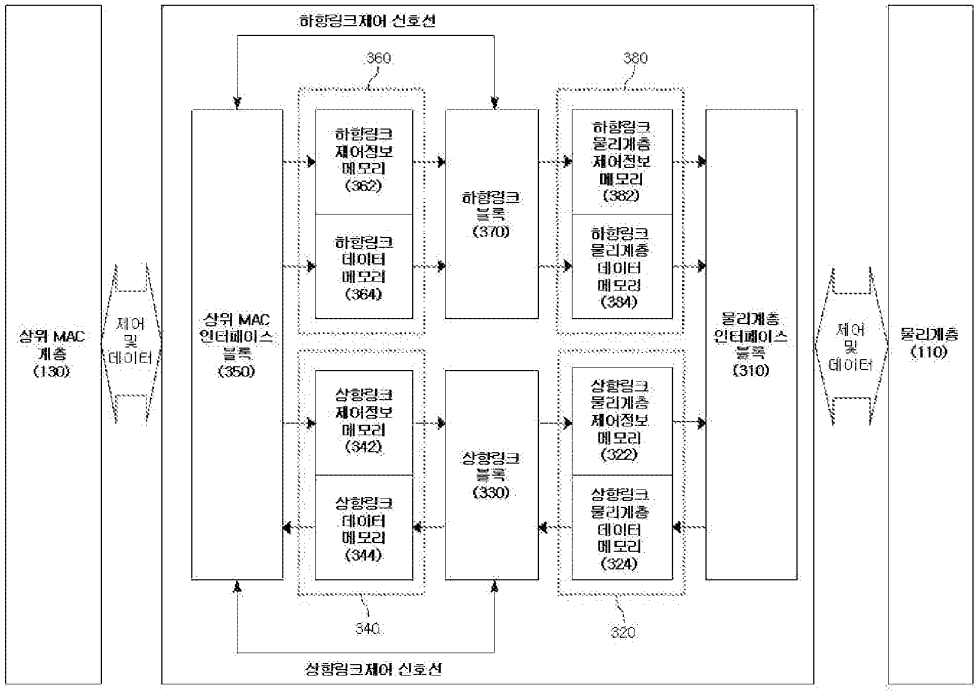
도면1


기지국
단말기
140
서비스 수렴부 계층
130
상위 매체접근제어(MAC) 계층
120
하위 매체접근제어(MAC) 계층
110
물리 계층
무선 구간
서비스 수렴부 계층
상위 매체접근제어(MAC) 계층
하위 매체접근제어(MAC) 계층
물리 계층

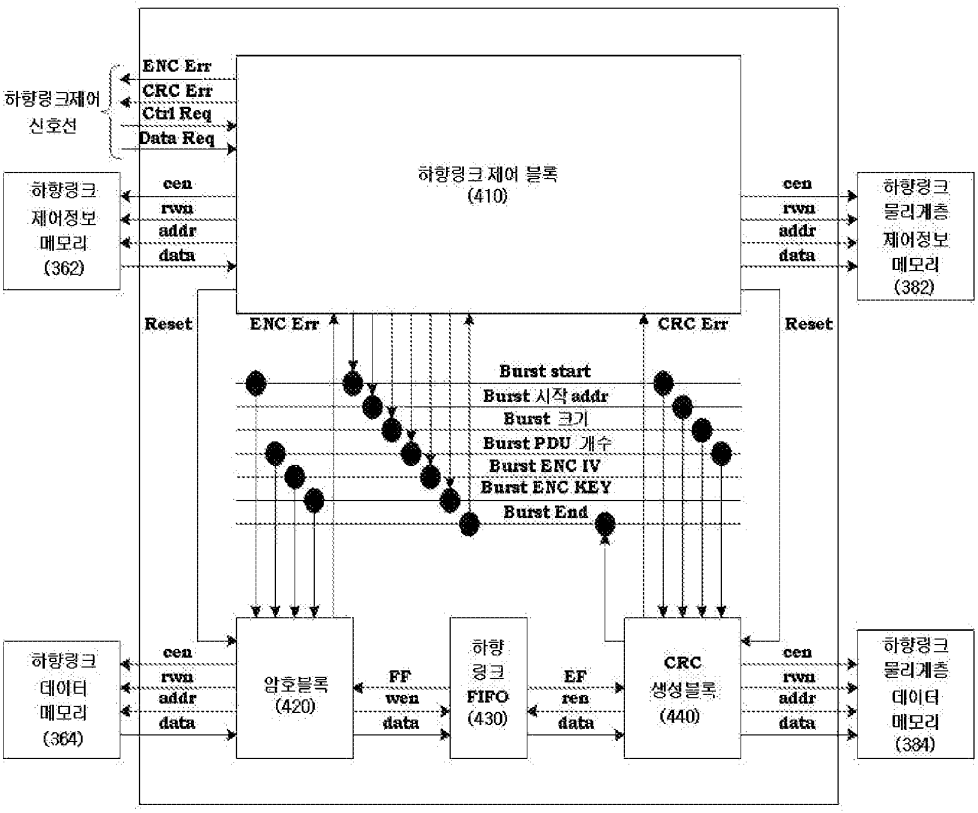
도면2


2A
하향링크 프레임
상향링크 프레임
Burst#1
Burst #2
Burst #3
Burst #4
Burst#5
주파수 축
시간 축
2B
버스트 구성
PDU#1
PDU#2
PDU#3
PDU#4
2C
Header
Payload
CRC
암호화 영역
CRC 영역
2D
HT
EC
Type (6)
Rsv(1)
CI(1)
EKS (2)
Rsv(2)
LEN MSB (3)
LEN LSB (8)
CID MSB (8)
CID LSB (8)
HCS (8)
EC: Encryption Control
'0' = Payload is not encrypted
'1' = Payload is encrypted
CI : CRC Indicator
'0' = No CRC is included
'1' = CRC is included

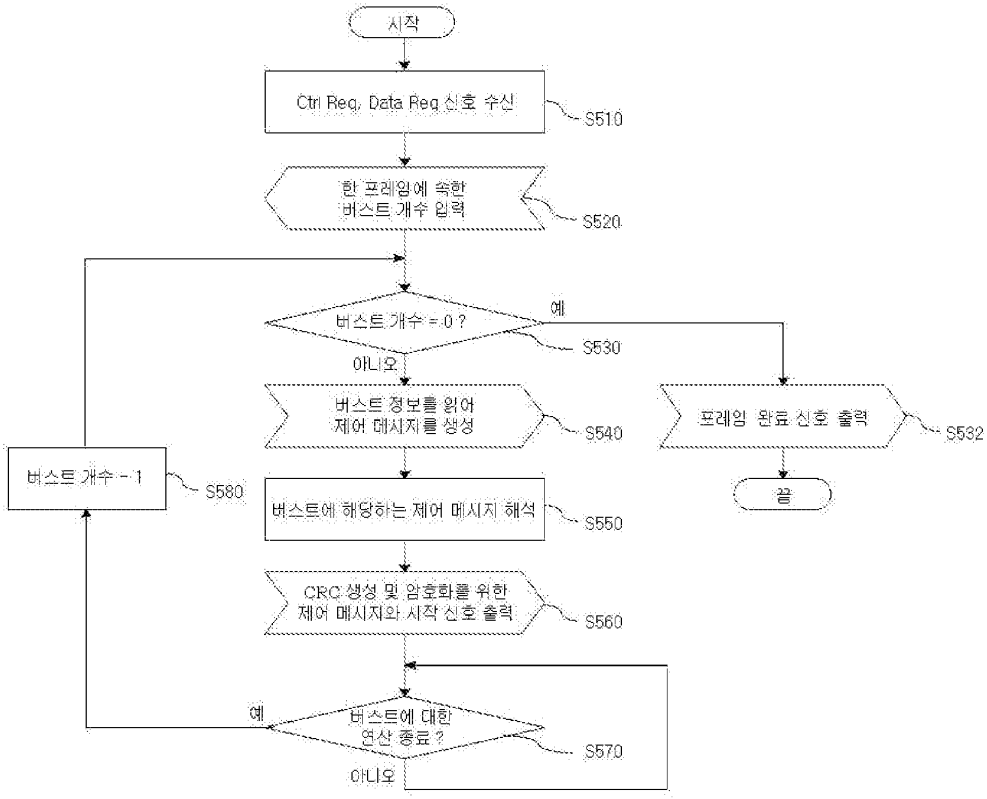
도면3


하향링크제어 신호선
360
380
상위 MAC 계층 (130)
제어 및 데이터
상위 MAC 인터페이스 블록 (350)
하향링크 제어정보 메모리 (362)
하향링크 데이터 메모리 (364)
하향링크 블록 (370)
하향링크 물리계층 제어정보 메모리 (382)
하향링크 물리계층 데이터 메모리 (384)
물리계층 인터페이스 블록 (310)
제어 및 데이터
물리계층 (110)
상향링크 제어정보 메모리 (342)
상향링크 데이터 메모리 (344)
상향링크 블록 (330)
상향링크 물리계층 제어정보 메모리 (322)
상향링크 물리계층 데이터 메모리 (324)
340
320
상향링크제어 신호선

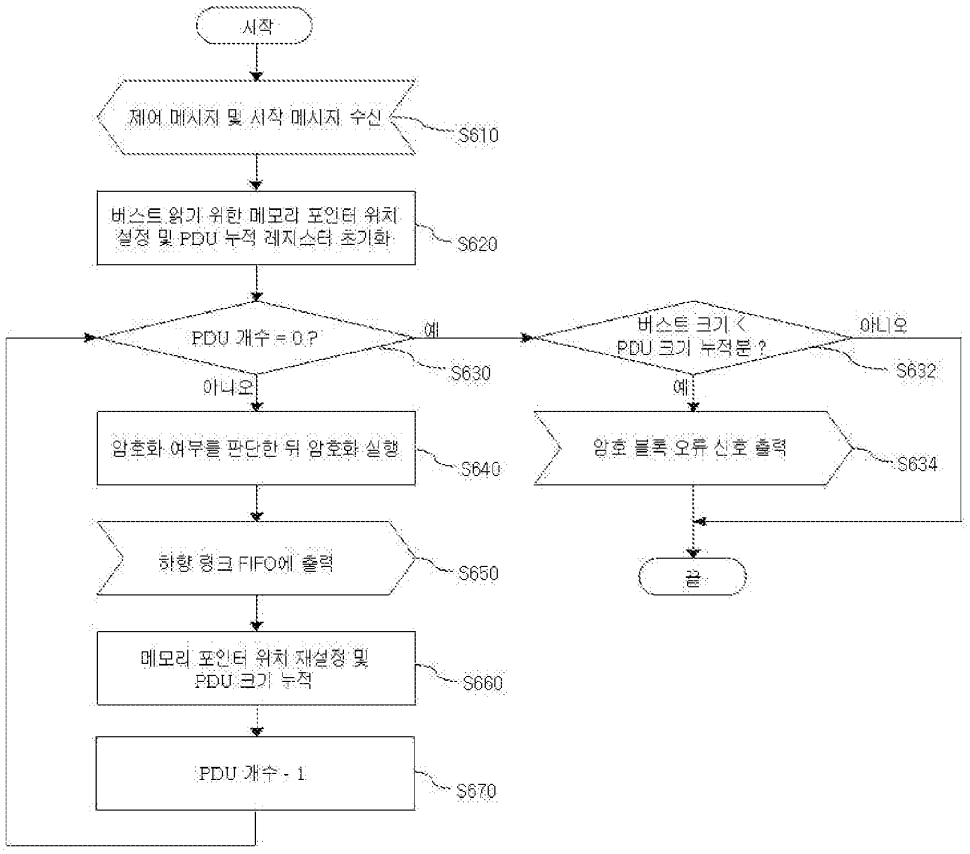
도면4


하향링크제어
신호선
ENC Err
CRC Err
Ctrl Req
Data Req
하향링크
제어정보
메모리
(362)
cen
rwn
addr
data
하향링크 제어 블록
(410)
cen
rwn
addr
data
하향링크
물리계층
제어정보
메모리
(382)
Reset
ENC Err
CRC Err
Reset
Burst start
Burst 시작 addr
Burst 크기
Burst PDU 개수
Burst ENC IV
Burst ENC KEY
Burst End
하향링크
데이터
메모리
(364)
cen
rwn
addr
data
암호블록
(420)
FF
wen
data
하향
링크
FIFO
(430)
EF
ren
data
CRC
생성블록
(440)
cen
rwn
addr
data
하향링크
물리계층
데이터
메모리
(384)

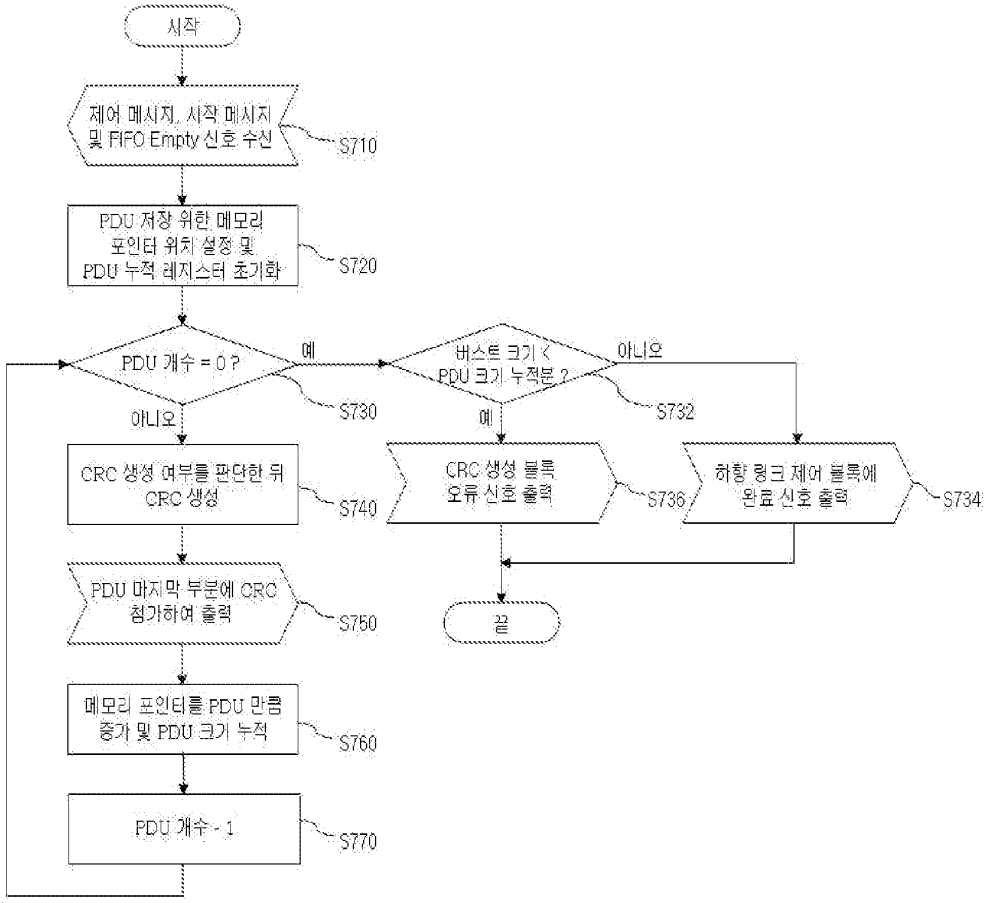
도면5


시작
Ctrl Req, Data Req 신호 수신
S510
한 프레임에 속한
버스트 개수 입력
S520
버스트 개수 = 0 ?
S530
예
아니오
버스트 정보를 읽어
제어 메시지를 생성
S540
포레임 완료 신호 출력
S532
끝
버스트 개수 - 1
S580
버스트에 해당하는 제어 메시지 해석
S550
CRC 생성 및 암호화를 위한
제어 메시지와 시작 신호 출력
S560
버스트에 대한
연산 종료 ?
S570
예
아니오

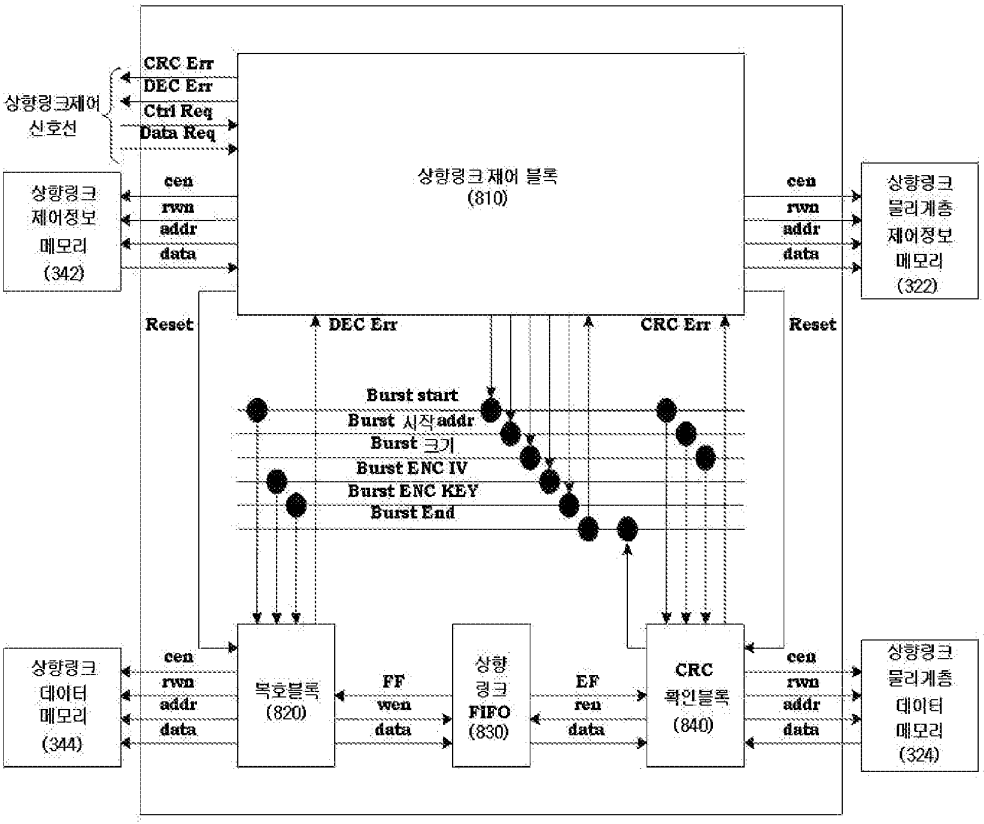
도면6


시작
제어 메시지 및 시작 메시지 수신
S610
버스트 읽기 위한 메모리 포인터 위치 설정 및 PDU 누적 레지스터 초기화
S620
PDU 개수 = 0 ?
예
S630
아니오
버스트 크기 < PDU 크기 누적분 ?
아니오
S632
예
암호화 여부를 판단한 뒤 암호화 실행
S640
암호 블록 오류 신호 출력
S634
하향 링크 FIFO에 출력
S650
끝
메모리 포인터 위치 재설정 및 PDU 크기 누적
S660
PDU 개수 - 1
S670

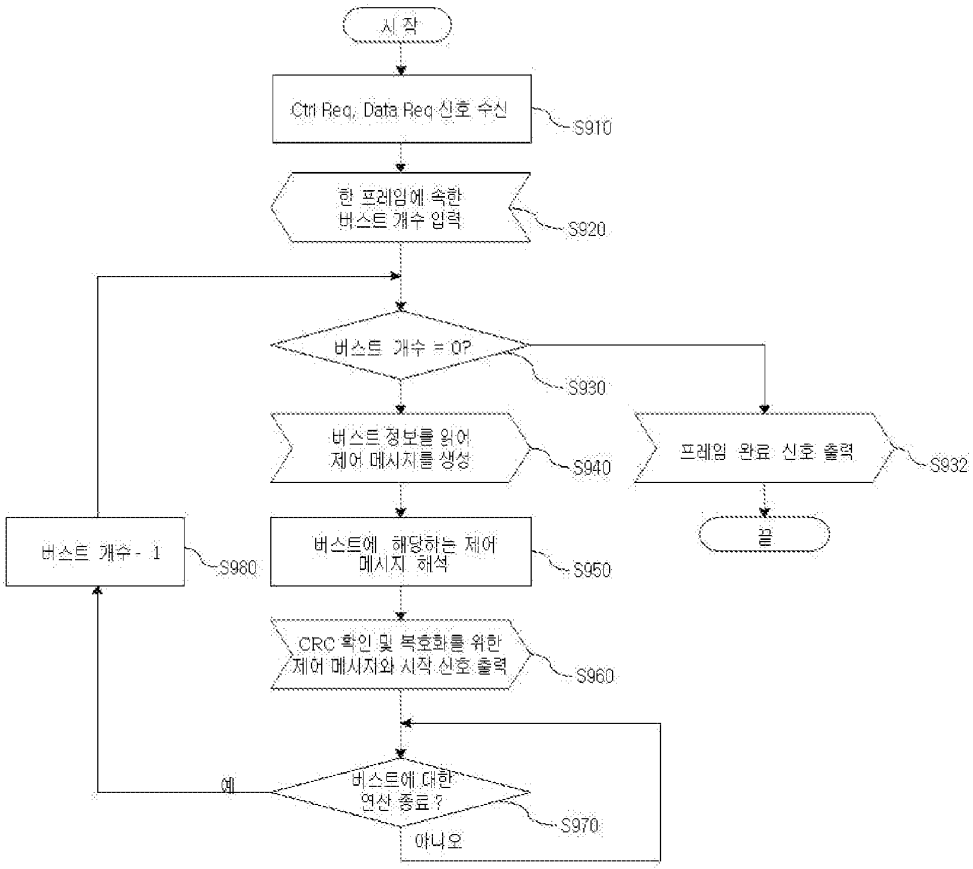
도면7


시작
제어 메시지, 시작 메시지 및 FIFO Empty 신호 수신
S710
PDU 저장 위한 메모리 포인터 위치 설정 및 PDU 누적 레지스터 초기화
S720
PDU 개수 = 0 ?
예
S730
버스트 크기 < PDU 크기 누적분 ?
아니오
S732
아니오
예
CRC 생성 여부를 판단한 뒤 CRC 생성
S740
CRC 생성 블록 오류 신호 출력
S736
하향 링크 제어 블록에 완료 신호 출력
S734
PDU 마지막 부분에 CRC 첨가하여 출력
S750
끝
메모리 포인터를 PDU 만큼 증가 및 PDU 크기 누적
S760
PDU 개수 - 1
S770

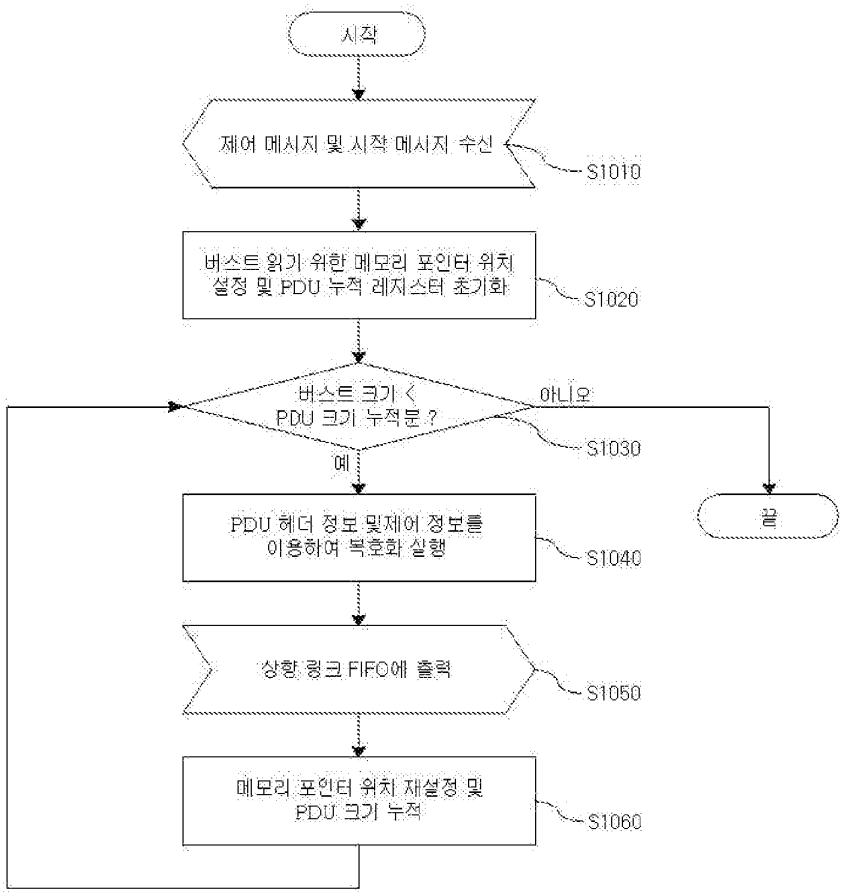
도면8


CRC Err
DEC Err
Ctrl Req
Data Req
상향링크제어
신호선
상향링크 제어 블록
(810)
상향링크
제어정보
메모리
(342)
cen
rwn
addr
data
상향링크
물리계층
제어정보
메모리
(322)
Reset
DEC Err
CRC Err
Reset
Burst start
Burst 시작addr
Burst 크기
Burst ENC IV
Burst ENC KEY
Burst End
상향링크
데이터
메모리
(344)
복호블록
(820)
FF
wen
data
상향
링크
FIFO
(830)
EF
ren
data
CRC
확인블록
(840)
상향링크
물리계층
데이터
메모리
(324)

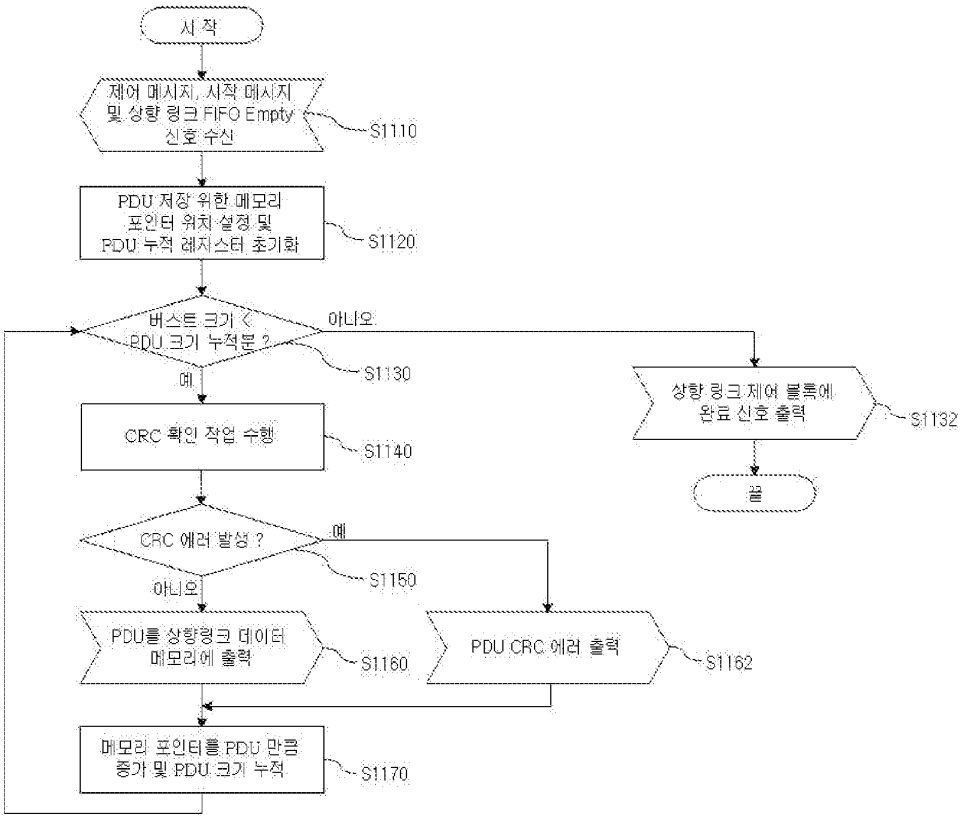
도면9


시작
Ctrl Req, Data Req 신호 수신
S910
한 프레임에 속한
버스트 개수 입력
S920
버스트 개수 = 0?
S930
버스트정보를 읽어
제어 메시지를 생성
S940
프레임 완료 신호 출력
S932
끝
버스트 개수 - 1
S980
버스트에 해당하는 제어
메시지 해석
S950
CRC 확인 및 복호화를 위한
제어 메시지와 시작 신호 출력
S960
예
버스트에 대한
연산 종료?
S970
아니오

도면10


시작
제어 메시지 및 시작 메시지 수신
S1010
버스트 읽기 위한 메모리 포인터 위치 설정 및 PDU 누적 레지스터 초기화
S1020
버스트 크기 < PDU 크기 누적분 ?
아니오
S1030
예
끝
PDU 헤더 정보 및제어 정보를 이용하여 복호화 실행
S1040
상향 링크 FIFO에 출력
S1050
메모리 포인터 위치 재설정 및 PDU 크기 누적
S1060

도면11


시작
제어 메시지, 시작 메시지 및 상향 링크 FIFO Empty 신호 수신
S1110
PDU 저장 위한 메모리 포인터 위치 설정 및 PDU 누적 레지스터 초기화
S1120
버스트 크기 < PDU 크기 누적분 ?
S1130
아니오
예
상향 링크 제어 블록에 완료 신호 출력
S1132
끝
CRC 확인 작업 수행
S1140
CRC 에러 발생 ?
S1150
예
아니오
PDU를 상향링크 데이터 메모리에 출력
S1160
PDU CRC 에러 출력
S1162
메모리 포인터를 PDU 만큼 증가 및 PDU 크기 누적
S1170

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	New Application
Confirmation No.:	
First-Named Inventor:	Sai C. Manapragada
Filing Date:	
Group Art Unit:	Not Yet Known
Examiner:	Not Yet Known
Attorney Docket No.:	020505-000010
Title:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

INFORMATION DISCLOSURE STATEMENT TRANSMITTAL

1. List of All Patents, Publications, U.S. Applications, or Other Information

Pursuant to the provisions of 37 C.F.R. §§ 1.56, 1.97, and 1.98, applicant requests consideration of the references listed on the attached PTO/SB/08 form(s) [commonly referred to as a PTO-1449 form] and/or the additional information identified below.

2. Enclosed Legible Copies

2a. A legible copy of each foreign patent document and publication listed on the PTO/SB/08 form is enclosed:

☐ i. except, pursuant to MPEP 609.02, a copy is not provided for each reference previously cited by or submitted to the Patent Office in prior US Patent Application No(s). _____, filed _____, from which the present application claims priority under 35 U.S.C. § 120.

☐ ii. except, a copy is not provided for each cumulative reference and enclosed reference identified below:

_____

☐ 2b. A copy of the specification and drawings for each cited unpublished U.S. application.

☐ 2c. A copy of a Search Report or Written Opinion from a foreign patent office is also enclosed.

☐ 2d. Consideration of the enclosed additional and/or below discussed information is requested.

3. Concise Explanation of Relevance for Non-English Language Information

For each non-English language reference listed on the attached PTO/SB/08 form(s), reference is made to:

☐ 3a. an English language translation submitted herewith,

☐ 3b. a foreign patent office Search Report (in the English language) submitted herewith,

☐ 3c. an English language translation of a foreign patent office Search Report submitted herewith,

☐ 3d. the concise explanation contained in the present application at page(s) _____,

☒ 3e. the concise explanation set forth in the attached English language abstract,

☐ 3f. a copy of a related patent publication (in the English language) cited herewith,

Foreign Patent Document	Corresponding English Language Patent Document

☒ 3g. the following concise explanation: The TW I500350B document itself contains an English version of the abstract..

4. Time for Filing

☒ 4a. This Information Disclosure Statement is submitted:

☒ i. for U.S. national applications or national stage PCT applications (not including CPAs and RCEs), within three months of filing or entry into national stage;

☒ ii. for U.S. national applications, national stage PCT applications, CPAs, or RCEs before the first Office Action on the merits;
and/or

☐ iii. before the mailing of an Office Action on the merits after the filing of a Request for Continued Examination (RCE) under § 1.114,

and thus no certification and/or fee is required.

☐ 4b. This information Disclosure Statement is submitted after three months from the filing date and after the first Office Action on the merits but prior to the mailing date of a final Office Action or Notice of Allowance, and thus:

☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below, or

☐ ii. the fee set forth in 37 C.F.R. § 1.17(p) is enclosed.

☐ 4c. This Information Disclosure Statement is submitted after the mailing date of a final Office Action or Notice of Allowance and prior to payment of the issue fee, and thus:

☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below and the fee set forth in 37 C.F.R. § 1.17(p) is enclosed, or

☐ ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.

☐ 4d. This Information Disclosure Statement is submitted after payment of the issue fee, and thus:

i. a Petition to Withdraw from Issue pursuant to 37 C.F.R. § 1.313(c)(2) has been filed, and

ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.

5. Certification- Statement Under 37 C.F.R. 1.97(e)

☐ 5a. It is hereby certified that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

☐ 5b. It is hereby certified that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

The filing of this Information Disclosure Statement shall not be construed as an admission that the information cited is, or is considered to be, material to patentability as defined

in § 1.56(b). It is believed that no additional fees are required. Should any other fee be required, however, please charge such fee to Deposit Account No. 23-3030, but not to include any payment of issue fees.

Respectfully submitted,

By /Blake R. Hartz, Reg. No. 73453/
Blake R. Hartz, Reg. No. 73453
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
Telephone: (317) 634-3456 Fax: (317) 637-7561
Email: bhartz@uspatent.com

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: XiFi Networks R&D Inc.

Application No./Patent No.: _____ / _____ Filed/Issue Date: _____ / _____

Titled: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

XiFi Networks R&D Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 065801, Frame 0024, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

020505-000010

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Blake R. Hartz, Reg. No. 73453/	March 4, 2024
Signature	Date
Blake R. Hartz	73453
Printed or Typed Name	Title or Registration Number

020505-000010

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 174 323 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
14.11.2018 Bulletin 2018/46

(51) Int Cl.:
H04W 8/26 *(2009.01)*

(21) Application number: **16196719.5**

(22) Date of filing: **18.04.2012**

(54) **METHODS AND APPARATUS FOR USE IN FACILITATING COMMUNICATIONS OVER FIRST AND SECOND WIRELESS CONNECTIONS OF A WIRELESS TRANSCEIVER**

VERFAHREN UND VORRICHTUNG ZUR VERWENDUNG BEI DER BEREITSTELLUNG VON KOMMUNIKATIONEN ÜBER ERSTE UND ZWEITE DRAHTLOSVERBINDUNGEN EINES DRAHTLOSEN SENDEEMPFÄNGERS

PROCÉDÉS ET APPAREILS DESTINÉS À FACILITER LES COMMUNICATIONS VIA LES PREMIÈRE ET SECONDE CONNEXIONS SANS FIL D'UN ÉMETTEUR-RÉCEPTEUR SANS FIL

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
31.05.2017 Bulletin 2017/22

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
12164555.0 / 2 654 331

(73) Proprietor: **BlackBerry Limited**
Waterloo, ON N2K 0A7 (CA)

(72) Inventor: **MONTEMURRO, Michael Peter**
Mississauga, Ontario L4W 0B5 (CA)

(74) Representative: **Jarrett, Daniel Phillip et al**
Kilburn & Strode LLP
Lacon London
84 Theobalds Road
London WC1X 8NL (GB)

(56) References cited:
WO-A1-2007/110473
JP-A- 2012 009 964
US-A1- 2008 013 539
US-A1- 2009 034 498
US-A1- 2011 134 894

- **SETHOM K ET AL: "Distributed virtual network interfaces to support intra-PAN and PAN-to-infrastructure connectivity", GLOBAL TELECOMMUNICATIONS CONFERENCE, 2005. GLOBECOM '05. IEEE ST. LOIUS, MO, USA 28 NOV.-2 DEC. 2005, PISCATAWAY, NJ, USA,IEEE, vol. 6, 28 November 2005 (2005-11-28), pages 3554-3558, XP010882301, DOI: 10.1109/GLOCOM.2005.1578434 ISBN: 978-0-7803-9414-8**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 3 174 323 B1

Description

BACKGROUND

Field Of The Technology

[0001] The present disclosure relates generally to communication devices configured for wireless communications, such as IEEE 802.11 type communications, including techniques for facilitating communications over first and second wireless connections of a wireless transceiver.

Description Of The Related Art

[0002] A wireless communication device, such as a portable battery-powered wireless telephony device, may be configured to communicate in wireless communication networks. For example, such a device may communicate via access points (APs) of wireless local area networks (WLANs) in accordance with IEEE 802.11 standards or the like. Such devices may also communicate using peer-to-peer communication techniques, for example, in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification, and/or be certified as a "Wi-Fi Direct" device.

[0003] There is a need for efficiently facilitating communications in these and similar environments.

[0004] In a paper titled "Distributed Virtual Network Interfaces to support intra-PAN and PAN-to-infrastructure Connectivity" by Kaouthar Sethom et al, IEEE Globecom 2005, it is proposed to assign a single unique virtual MAC address to all link layers of a terminal supporting multiple physical interfaces of different standards.

[0005] WO 2007/110473 proposes the use of Bluetooth higher layers on top of WLAN lower layers, with a virtual device in between, mapping, e.g., a Bluetooth address to an Ethernet address.

[0006] US 2008/0013539 proposes the use of a common logical MAC address for different physical interfaces having their own respective hardware MAC addresses.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments of present disclosure will now be described by way of example with reference to attached figures, wherein:

FIG. 1 is an illustrative representation of a communication system which includes wireless communication networks (e.g. WLANs) with which a wireless communication device may communicate;
FIG. 2 is an example of a schematic block diagram of the wireless device of FIG. 1;
FIGs. 3 and 4 are some examples of different types of wireless devices of the present disclosure, which include a smartphone (FIG. 3) and a tablet computer (FIG. 4);
FIG. 5 is an illustrative representation of a part of the communication system of FIG. 1 which may include different types of wireless networks (e.g. WLAN, and Wi-Fi Peer-to-Peer (P2P) networks);
FIG. 6 is an illustrative representation of a portion of memory of the wireless device, where the memory has a plurality of profiles stored therein where each profile is associated with a first type of wireless connection (e.g. a WLAN-STA type of wireless connection) or a second type of wireless connection (e.g. a Wi-Fi P2P type of wireless connection);
FIG. 7 is a schematic block diagram of relevant components of the wireless device which pertain to communications over first and second wireless connections of a wireless transceiver of the wireless device, especially communications over concurrent wireless connections;
FIG. 8 is an illustration of the format of a Media Access Control (MAC) address which may be utilized for identifying the device for communications;
FIG. 9 is an example of a format of a data frame which may be utilized for communications to and/or from the wireless device;
FIG. 10 is another schematic block diagram of relevant components of the wireless device which pertain to communications over first and second wireless connections of the wireless transceiver, which may be concurrent wireless connections, in accordance with techniques of the present disclosure;
FIG. 11 is a flowchart for describing a method for use in facilitating communications over first and second wireless connections of the wireless transceiver of the wireless device; and
FIG. 12 is another flowchart for describing another method for use in facilitating communications over the first and second wireless connections of the wireless transceiver of the wireless device.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0008] A wireless communication device of the present disclosure includes a first wireless transceiver and a second wireless transceiver. The wireless device is configured for communicating via the first wireless transceiver over a first wireless connection with a first device, where communications to and from the wireless device are addressed with a first (universally administered) hardware address assigned to the first wireless transceiver. The wireless device is further configured for communicating via the first wireless transceiver over a second wireless connection with a second device, where communications to and from the wireless device are addressed with a second (universally administered) hardware address assigned to the second wireless transceiver. The first and second hardware addresses may be Media Access Control (MAC) addresses of the first and the second wireless transceivers, respectively. In some embodiments, the

first wireless transceiver may be configured for communications in accordance with an IEEE 802.11 standard, and the second wireless transceiver may be configured for communications in accordance with a BLUETOOTH® standard. The first wireless connection may be a wireless local area network (WLAN) infrastructure (or WLAN-STA) connection, and the second wireless connection may be a WiFi Peer-to-Peer (P2P) connection. Thus, in some embodiments, the wireless device may utilize the MAC address of the IEEE 802.11 transceiver for identifying the device in association with WLAN-STA connections of the IEEE 802.11 transceiver, and utilize the MAC address of the BLUETOOTH transceiver for identifying the device in association with Wi-Fi P2P connections of the IEEE 802.11 transceiver. The first and the second wireless connections may be concurrent wireless connections.

[0009] Example Environment. To illustrate one environment within which the techniques of the present disclosure may be practiced, FIG. 1 illustrates a wireless communication device 201 which may communicate in a communication system 100. In the communication system 100, wireless device 201 may communicate with one or more wireless communication networks. For example, wireless device 201 may communicate with a wireless communication network 104 which is a wireless local area network (WLAN). Here, wireless network 104 and wireless device 201 may operate in accordance with IEEE 802.11 standards.

[0010] In this example, wireless network 104 has a plurality of wireless access points (APs) 112, 114, and 116 for wireless communications with wireless device 201. WLANs may be identified by a wireless device 201 with use of a wireless network identifier which is communicated from the WLAN. The wireless network identifier may be, for example, a Set Service Identifier (SSID) or Extended SSID (ESSID). In this example, wireless network 104 includes one or more servers 106, a redirect server 108, and a gateway 110. Server 106 may provide data, applications, and/or functionality for communication services for wireless device 201.

[0011] Wireless network 104 may be a public Wi-Fi "hotspot" for public use, and include what may be referred to as a "captive portal" or "walled garden." For devices connected in wireless network 104 via one of wireless APs 112, 114, and 116, gateway 110 is configured to permit or deny access to the data, applications, and/or functionality, as well as to permit or deny external access outside of wireless network 104 to Internet 120. To do this, gateway 110 has a set of IP address filters which define a set of addresses that are permissible/impermissible, if any at all, for access by devices. Access by a device depends on whether or not a device has been authorized and what access rights are given upon authorization.

[0012] Typically, when a request by a device in wireless network 104 is made prior to proper authorization, gateway 110 is configured to redirect the request to redirect server 108. In response, redirect server 108 is configured to respond to wireless device 201 to provide data for producing information (e.g. Web page information) which is rendered in a visual display of wireless device 201 via a Web browser application. The information may solicit a user response. For example, the information may solicit a user registration or login with user fields for entering a user name and/or password information. Gateway 110 identifies whether the received user response is sufficient (e.g. whether the user name and password match prestored user name and password information, whether the user payment is accepted, whether the user acceptance is confirmed, etc.). If the user response is deemed sufficient, gateway 110 permits access to the data, applications, and/or functionality in or outside of wireless network 104.

[0013] Wireless device 201 may also operate for communications in other different wireless networks, such as a wireless network 122 which is also a WLAN. In this example, wireless network 122 is a private communication network of an enterprise (e.g. an organization, a company, a corporation, etc.) of wireless device 201. Similar to wireless network 104, wireless network 122 has a plurality of wireless APs 128, 130 and 132, one or more servers 124, and a gateway 126. For devices connected in wireless network 122 via one of wireless APs 128, 130, and 132, gateway 126 may be configured to permit or deny access to the data, applications, and/or functionality offered via wireless network 122 depending on whether or not a device has been authorized and what access rights are given upon authorization. For devices attempting to access wireless network 122 via Internet 120, gateway 126 is configured to permit or deny internal access to the data, applications, and/or functionality in wireless network 122.

[0014] Such wireless networks (e.g. infrastructure WLANs) may provide or allow access to various data and communication services to its terminals. For example, the wireless networks may provide for communication access to Internet 120 via the Web browser application, or voice telephony communication service with use of Voice over IP (VoIP) communication, or other communication services. For "push-type" data or message synchronization services, for example, wireless device 201 may be enabled to maintain data synchronization with a server (e.g. server 106 or 118) for user data of an application associated with a user account. The application of wireless device 201 and the server may be or include, for example, an electronic mail (e-mail) application program for the communication of e-mail messages.

[0015] Wireless device 201 may be additionally configured to access communication services via a Public Land Wireless Network (PLMN) 136 (e.g. a cellular telecommunications network). PLMN 136 includes a core network 134, a plurality of base station controllers such as a base station controller (BSC) 138 coupled to core network 134, and a plurality of base stations such as a base station (BS) 140 and a base station 142 coupled to

associated BSCs 138. Core network 134, BSC 138, and BS 140 operate in a conventional fashion as well-documented. Other PLMNs in the environment have a similar or the same architecture as PLMN 136. For communication with PLMNs, wireless device 201 may be configured in accordance with one or more cellular telecommunication standards, such as Global Systems for Mobile (GSM) and/or General Packet Radio Service (GPRS) technologies. However, such wireless device may additionally or alternatively operate in accordance with other such cellular standards, such as Enhanced Data rates for GSM Evolution (EDGE) or Enhanced GPRS (EGPRS), Universal Mobile Telecommunications System (UMTS), Long-Term Evolution (LTE), or EVolution-Data Only (EV-DO) (for CDMA) technologies, as a few examples.

[0016] Further, in additional to being operative for communications with infrastructure WLANs (e.g. IEEE 802.11 infrastructure WLANs), wireless device 201 may additionally or alternatively communicate using peer-to-peer communication techniques, for example, in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification, and/or be certified as a "Wi-Fi Direct" device. The Wi-Fi Peer-To-Peer (P2P) Technical specification is hereby incorporated by reference herein.

[0017] Accordingly, illustrating further in FIG. 1, wireless device 201 and one or more other wireless devices 195 and 197 in FIG. 1 may be operative to establish Wi-Fi P2P wireless network connections with each other in a Wi-Fi P2P wireless network. Here, one of the communicate devices may be configured to enter into an AP mode of operation, so that other communication devices may associate with them for direct RF communications therebetween. An AP mode of operation, which may be referred to as a "wireless AP mode" or the like, provides a benefit due to the high data rates available over WLAN links. Here, again, data may be communicated directly between the wireless devices without the data traversing any wireless network infrastructure, where one of the devices is set to operate or serve as an AP (switching operation from as an end terminal) and the other device operates as an end terminal to associate and connect with the AP (i.e. wireless device 201 operating as an AP) for communications. Wireless device 201 may operate such that, when in the AP mode of operation with other communication devices 195 and 197, it also operates as a client with another AP.

[0018] Reference will now be made to FIG. 2 which illustrates one example of a schematic block diagram of wireless device 201 in which example embodiments may be applied. In the illustrated example embodiment, wireless device 201 is a communication device and, more particularly, is a mobile communication device having data and voice communication capabilities, and configured to communicate with other computer systems (e.g. via the Internet). It will, however, be appreciated that wireless device 201 may take other forms.

[0019] Depending on the functionality provided by wireless device 201, in various example embodiments wireless device 201 may be a multiple-mode communication device configured for both data and voice communication, a mobile telephone, such as a smartphone, a wearable computers such as a watch, a tablet computer such as a slate computer, a personal digital assistant (PDA), or a computer system. Wireless device 201 may take other forms apart from those specifically listed above. The electronic device may also be referred to as a mobile communications device, a communication device, a mobile device and, in some cases, as a device.

[0020] Wireless device 201 includes a controller including one or more processor 240 (such as a microprocessor) which controls the overall operation of wireless device 201. The processor 240 interacts with device subsystems such as a wireless communication subsystem 211 for exchanging radio frequency signals with wireless network 104 to perform communication functions. The processor 240 is communicably coupled with additional device subsystems including one or more output interfaces 205 (such as a display 204 and/or a speaker 256 and/or electromagnetic (EM) radiation source 257), one or more input interfaces 206 (such as a camera 253, microphone 258, keyboard (not shown), control buttons (not shown), a navigational input device (not shown), and/or a touch-sensitive overlay (not shown)) associated with a touchscreen display 204, an orientation subsystem 249, memory (such as flash memory 244, random access memory (RAM) 246, read only memory (ROM) 248, etc.), auxiliary input/output (I/O) subsystems 250, a data port 252 (which may be a serial data port, such as a Universal Serial Bus (USB) data port), a near field communications (NFC) subsystem 265, a short-range communication subsystem 262 and other device subsystems generally designated as 264. Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions.

[0021] In at least some example embodiments, wireless device 201 may include a touchscreen display which acts as both an input interface 206 (i.e. touch-sensitive overlay) and an output interface 205 (i.e. display). The touchscreen display may be constructed using a touch-sensitive input surface which is connected to an electronic controller and which overlays the display 204. The touch-sensitive overlay and the electronic controller provide a touch-sensitive input interface 206 and the processor 240 interacts with the touch-sensitive overlay via the electronic controller. In at least some example embodiments, the touch-sensitive overlay may have a touch-sensitive input surface which is larger than the display 204. For example, in at least some example embodiments, the touch-sensitive overlay may extend overtop of a frame 312 (of FIG. 3) which surrounds the display 204. In such example embodiments, the frame 312 (of FIG. 3) may be referred to as an active frame since it is capable of acting as an input interface 206. In at least some example embodiments, the touch-sensitive overlay may extend to the sides of wireless device 201.

Samsung Ex. 1004, Page 419 of 563

[0022] As noted above, in some example embodiments, wireless device 201 may include a communication subsystem 211 which allows wireless device 201 to communicate over wireless network 104. The communication subsystem 211 includes a receiver 212, a transmitter 213, and associated components, such as one or more antenna elements 214 and 215, local oscillators (LOs) 216, and a processing module such as a digital signal processor (DSP) 217. The antenna elements 214 and 215 may be embedded or internal to wireless device 201 and a single antenna may be shared by both receiver and transmitter. The particular design of the wireless communication subsystem 211 depends on wireless network 104 in which wireless device 201 is intended to operate.

[0023] In at least some example embodiments, wireless device 201 may communicate with any one of a plurality of stations or access points (APs) of wireless network 104 within its geographic coverage area. Wireless device 201 may send and receive communication signals over wireless network 104 after the required network registration or activation procedures have been completed. Signals received by the antenna 214 through wireless network 104 are input to the receiver 212, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, etc., as well as analog-to-digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in the DSP 217. In a similar manner, signals to be transmitted are processed, including modulation and encoding, for example, by the DSP 217. These DSP-processed signals are input to the transmitter 213 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification, and transmission to wireless network 104 via the antenna 215. The DSP 217 not only processes communication signals, but may also provide for receiver and transmitter control. For example, the gains applied to communication signals in the receiver 212 and the transmitter 213 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 217.

[0024] In some example embodiments, the auxiliary input/output (I/O) subsystems 250 may include an external communication link or interface; for example, an Ethernet connection. Wireless device 201 may include other wireless communication interfaces for communicating with other types of wireless networks; for example, a wireless network such as an orthogonal frequency division multiplexed (OFDM) network. The auxiliary I/O subsystems 250 may include a vibrator for providing vibratory notifications in response to various events on wireless device 201 such as receipt of an electronic communication or incoming phone call, or for other purposes such as haptic feedback (touch feedback).

[0025] The data port 252 may be used for synchronization with a user's host computer system (not shown). The data port 252 enables a user to set preferences through an external device or software application and extends the capabilities of wireless device 201 by providing for information or software downloads to wireless device 201 other than through wireless network 104. The alternate download path may for example, be used to load an encryption key onto wireless device 201 through a direct, reliable and trusted connection to thereby provide secure device communication.

[0026] In at least some example embodiments, wireless device 201 also includes a device orientation subsystem 249 including at least one orientation sensor 251 which is connected to the processor 240 and which is controlled by one or a combination of a monitoring circuit and operating software. The orientation sensor 251 detects the orientation of the device 201 or information from which the orientation of the device 201 can be determined, such as acceleration. In some example embodiments, the orientation sensor 251 is an accelerometer, such as a three-axis accelerometer. An accelerometer is a sensor which converts acceleration from motion (e.g. movement of the device 201 or a portion thereof due to the strike force) and gravity which are detected by a sensing element into an electrical signal (producing a corresponding change in output). Accelerometers may be available in one, two or three axis configurations. Higher order axis configurations are also possible. Accelerometers may produce digital or analog output signals depending on the type of accelerometer.

[0027] An orientation sensor 251 may generate orientation data which specifies the orientation of wireless device 201. The orientation data, in at least some example embodiments, specifies the orientation of the device 201 relative to the gravitational field of the earth.

[0028] In some example embodiments, the orientation subsystem 249 may include other orientation sensors 251, instead of or in addition to accelerometers. For example, in various example embodiments, the orientation subsystem 249 may include a gravity sensor, a gyroscope, a tilt sensor, an electronic compass or other suitable sensor, or combinations thereof. In some example embodiments, the device orientation subsystem 249 may include two or more orientation sensors 251 such as an accelerometer and an electronic compass.

[0029] Wireless device 201 may, in at least some example embodiments, include a near field communications (NFC) subsystem 265. The NFC subsystem 265 is configured to communicate with other wireless devices 201 and/or tags, using an NFC communications protocol. NFC is a set of short-range wireless technologies which typically require a distance of 4 cm or less for communications. The NFC subsystem 265 may include an NFC chip and an NFC antenna.

[0030] Wireless device 201 may include a microphone and/or one or more speakers. In at least some example embodiments, wireless device 201 may include a plurality of speakers 256. For example, in some example embodiments, wireless device 201 may include two or more speakers 265. The two or more speakers 256 may, for

Samsung Ex. 1004, Page 420 of 563

example, be disposed in spaced relation to one another. That is, in at least some example embodiments, wireless device 201 may include a first speaker and a second speaker and the first speaker and the second speaker may be spatially separated from one another within wireless device 201. In at least some example embodiments, the display 204 may be disposed between the first speaker and the second speaker of the electronic device. In such example embodiments, the first speaker may be located at one side of the display 204 and the second speaker may be located at another side of the display which is opposite the side of the display where the first speaker is located. For example, the first speaker may be disposed at a left side of the display and the second speaker may be disposed at a right side of the display. In at least some example embodiments, each speaker 256 may be associated with a separate audio channel. The multiple speakers may, for example, be used to provide stereophonic sound (which may also be referred to as stereo).

[0031] Wireless device 201 may also include one or more cameras 253. The one or more cameras 253 may be capable of capturing images in the form of still photographs or motion video. In at least some example embodiments, wireless device 201 includes a front facing camera 253. A front facing camera is a camera which is generally located on a front face of wireless device 201. The front face is typically the face on which a display 204 is mounted. That is, the display 204 is configured to display content which may be viewed from a side of wireless device 201 where the camera 253 is directed. The front facing camera 253 may be located anywhere on the front surface of the electronic device; for example, the camera 253 may be located above or below the display 204. The camera 253 may be a fixed position camera which is not movable relative to the display 204 of wireless device 201 and/or the housing of wireless device 201. In such example embodiments, the direction of capture of the camera is always predictable relative to the display 204 and/or the housing. In at least some example embodiments, the camera may be provided in a central location relative to the display 204 to facilitate image acquisition of a face.

[0032] In at least some example embodiments, wireless device 201 includes an electromagnetic (EM) radiation source 257. In at least some example embodiments, the EM radiation source 257 is configured to emit electromagnetic radiation from the side of the electronic device which is associated with a camera 253 of that wireless device 201. For example, where the camera is a front facing camera 253, wireless device 201 may be configured to emit electromagnetic radiation from the front face of wireless device 201. That is, in at least some example embodiments, the electromagnetic radiation source 257 is configured to emit radiation in a direction which may visible by the camera. That is, the camera 253 and the electromagnetic radiation source 257 may be disposed on wireless device 201 so that electromagnetic radiation emitted by the electromagnetic radiation source 257 is visible in images obtained by the camera.

[0033] In some example embodiments, the electromagnetic radiation source 257 may be an infrared (IR) radiation source which is configured to emit infrared radiation. In at least some example embodiments, the electromagnetic radiation source 257 may be configured to emit radiation which is not part of the visible spectrum. The camera 253 may be a camera which is configured to capture radiation of the type emitted by the electromagnetic radiation source 257. Accordingly, in at least some example embodiments, the camera 253 is configured to capture at least some electromagnetic radiation which is not in the visible spectrum.

[0034] In some example embodiments, wireless device 201 is provided with a service routing application programming interface (API) which provides an application with the ability to route traffic through a serial data (i.e., USB) or Bluetooth® (Bluetooth® is a registered trademark of Bluetooth SIG, Inc.) connection to a host computer system using standard connectivity protocols. When a user connects their wireless device 201 to the host computer system via a USB cable or Bluetooth® connection, traffic that was destined for wireless network 104 is automatically routed to wireless device 201 using the USB cable or Bluetooth® connection. Similarly, any traffic destined for wireless network 104 is automatically sent over the USB cable Bluetooth® connection to the host computer system for processing.

[0035] Wireless device 201 also includes a battery 238 as a power source, which is typically one or more rechargeable batteries that may be charged for example, through charging circuitry coupled to a battery interface 236 such as the data port 252. The battery 238 provides electrical power to at least some of the electrical circuitry in wireless device 201, and the battery interface 236 provides a mechanical and electrical connection for the battery 238. The battery interface 236 is coupled to a regulator (not shown) which provides a regulated voltage V to the circuitry for powering wireless device 201.

[0036] Wireless device 201 includes a short-range communication subsystem 262 which provides for wireless communication between wireless device 201 and other wireless devices 201. The short-range communication subsystem 262 may be used to provide a preferred device mode between wireless device 201 and another wireless device 201 which may, in at least some example embodiments, be a wireless device which is the same or similar to wireless device 201 discussed with reference to FIG. 1. In at least some example embodiments, the short-range communication subsystem 262 is a wireless bus protocol compliant communication mechanism such as a Bluetooth® communication module to provide for communication with similarly-enabled systems and devices.

[0037] Wireless device 201 stores data 227 in an erasable persistent memory, which in one example embodiment is the flash memory 244. In various example em-

Samsung Ex. 1004, Page 421 of 563

bodiments, the data 227 includes service data including information required by wireless device 201 to establish and maintain communication with wireless network 104. The data 227 may also include user application data such as email messages, address book and contact information, calendar and schedule information, notepad documents, image files, and other commonly stored user information stored on wireless device 201 by its user, and other data. The data 227 stored in the persistent memory (e.g. flash memory 244) of wireless device 201 may be organized, at least partially, into one or more databases or data stores. The databases or data stores may contain data items of the same data type or associated with the same application. For example, email messages, contact records, and task items may be stored in individual databases within the device memory.

[0038] Wireless device 201 may, in some example embodiments, be a mobile communication device which may provide two principal modes of communication: a data communication mode and a voice communication mode. In the data communication mode, a received data signal such as a text message, an email message, or Web page download will be processed by the communication subsystem 211 and input to the processor 240 for further processing. For example, a downloaded Web page may be further processed by a browser application or an email message may be processed by an email messaging application and output to the display 204. A user of wireless device 201 may also compose data items, such as email messages; for example, using the input devices in conjunction with the display 204. These composed items may be transmitted through the communication subsystem 211 over wireless network 104.

[0039] In the voice communication mode, wireless device 201 provides telephony functions and operates as a typical cellular phone. The overall operation is similar, except that the received signals would be output to the speaker 256 and signals for transmission would be generated by a transducer such as the microphone 258. The telephony functions are provided by a combination of software/firmware (i.e., a voice communication module) and hardware (i.e., the microphone 258, the speaker 256 and input interfaces 206). Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on wireless device 201. Although voice or audio signal output is typically accomplished primarily through the speaker 256, the display screen 204 may also be used to provide an indication of the identity of a calling party, duration of a voice call, or other voice call related information.

[0040] The processor 240 operates under stored program control and executes software modules 221 stored in memory such as persistent memory; for example, in the flash memory 244. As illustrated in FIG. 1, the software modules 221 include operating system software 223 and other software applications 225 such as preferred device mode module 260. In the example embodiment of FIG. 1, the preferred device mode module 260 is implemented as a stand-alone application 225. However, in other example embodiments, the preferred device mode module 260 could be implemented as part of the operating system 223 or another application 225.

[0041] The software applications 225 on wireless device 201 may also include a range of additional applications, including for example, a notepad application, Internet browser application, voice communication (i.e. telephony) application, mapping application, or a media player application, or any combination thereof. Each of the software applications 225 may include layout information defining the placement of particular fields and graphic elements (e.g. text fields, input fields, icons, etc.) in the user interface (e.g. the display 204) according to the application.

[0042] The software modules 221 or parts thereof may be temporarily loaded into volatile memory such as the RAM 246. The RAM 246 is used for storing runtime data variables and other types of data or information, as will be apparent to those skilled in the art. Although specific functions are described for various types of memory, this is merely one example, and those skilled in the art will appreciate that a different assignment of functions to types of memory could also be used.

[0043] A predetermined set of applications that control basic device operations, including data and possibly voice communication applications will normally be installed on wireless device 201 during or after manufacture. Additional applications and/or upgrades to the operating system 223 or software applications 225 may also be loaded onto wireless device 201 through wireless network 104, the auxiliary I/O subsystem 250, the data port 252, the short-range communication subsystem 262, or other suitable subsystem 264. The downloaded programs or code modules may be permanently installed; for example, written into the program memory (i.e. the flash memory 244), or written into and executed from the RAM 246 for execution by the processor 240 at runtime.

[0044] Example Smartphone Electronic Device. Referring now to FIG. 3, a front view of an example wireless device 201 which is a smartphone 100 is illustrated. The smartphone 100 is a mobile phone which offers more advanced computing capability than a basic non-smartphone cellular phone. For example, the smartphone 100 may have the ability to execute third party applications which are stored on the smartphone.

[0045] The smartphone 100 may include the components discussed above with reference to FIG. 2 or a subset of those components. The smartphone 100 includes a housing 294 which houses at least some of the components discussed above with reference to FIG. 2.

[0046] In the example embodiment illustrated, the smartphone includes a display 204, which may be a touchscreen display which acts as an input interface 206. The display 204 is disposed within the smartphone 100 so that it is viewable at a front side 292 of the smartphone 100. That is, a viewable side of the display 204 is disposed on the front side 292 of the smartphone. In the

Samsung Ex. 1004, Page 422 of 563

example embodiment illustrated, the display 204 is framed by the housing 294.

[0047] The example smartphone 100 also includes other input interfaces 206 such as one or more buttons, keys or navigational input mechanisms. In the example illustrated, at least some of these additional input interfaces 206 are disposed for actuation at the front side 292 of the smartphone.

[0048] The example smartphone also includes a speaker 256. In the example embodiment illustrated, the smartphone includes a single speaker 256 which is disposed vertically above the display 204 when the smartphone 100 is held in a portrait orientation where its height is longer than its width. The speaker 256 may be disposed on the front face of the smartphone 100.

[0049] While the example smartphone 100 of FIG. 3 includes a single speaker 256, in other example embodiments, the smartphone 100 may include a greater number of speakers 256. For example, in at least some example embodiments, the smartphone 100 may include a second speaker 256 which is disposed vertically below the display 204 when the smartphone is held in a portrait orientation where its height is longer than its width (i.e. the orientation illustrated in FIG. 3).

[0050] The example smartphone 100 also includes a microphone 258. In the example illustrated, the microphone 258 is vertically disposed below the display 204 when the smartphone is held in the portrait orientation. The microphone 258 and at least one speaker 256 may be arranged so that the microphone is in close proximity to a user's mouth and the speaker 256 is in close proximity to a user's ear when the user holds the phone to their face to converse on the smartphone.

[0051] The example smartphone 100 also includes a front facing camera 253 which may be located vertically above the display 204 when the smartphone 100 is held in a portrait orientation where its height is longer than its width. The front facing camera 253 is located so that it may capture images of objects which are located in front of and/or surrounding the front side of the smartphone 100.

[0052] The example smartphone 100 also includes an electromagnetic radiation source 257. The electromagnetic radiation source 257 is disposed on the front side 292 of the smartphone 100. In this orientation, electromagnetic radiation which is produced by the electromagnetic radiation source 257 may be projected onto objects which are located in front of and/or surrounding the front side of the smartphone 100. Such electromagnetic radiation (or the projection of electromagnetic radiation onto objects) may be captured on images obtained by the camera 253.

[0053] Example Tablet Electronic Device. The wireless device may be a tablet computer 300 ("tablet"), one of which is illustrated in FIG. 4. Tablet computer 300 of FIG. 4 may include many of the same features and components of the smartphone 100 of FIG. 3. However, tablet computer 300 of FIG. 3 is generally larger than the smartphone 100 of FIG. 3. Tablet computer 300 may include the components discussed above with reference to FIG. 2 or a subset of those components. Tablet computer 300 includes a housing 394 which houses at least some of the components discussed above with reference to FIG. 2.

[0054] Tablet computer 300 includes a display 304, which may be a touchscreen display which acts as an input interface 206. The display 304 is disposed within tablet computer 300 so that it is viewable at a front side 302 of tablet computer 300. That is, a viewable side of the display 304 is disposed on the front side 302 of tablet computer 300. In the example embodiment illustrated, the display 304 is framed by the housing 394, with use of a frame 312 which surrounds the display 304. The frame 312 is portion of the housing 394 which provides a border around the display 304. In at least some example embodiments, the frame 312 is an active frame 312. That is, the frame has a touch sensitive overlay which allows wireless device 201 to detect a touch applied to the frame, thereby allowing the frame 312 to act as an input interface 206 (of FIG. 1).

[0055] The example tablet computer 300 includes a plurality of speakers 256. In the example embodiment illustrated, the tablet includes two speakers 256. The two speakers 256 are disposed on opposing sides of the display 304. More particularly, when tablet computer 300 is held in a landscape orientation (such as the orientation illustrated in FIG. 3) where its width is longer than its height, one of the two speakers is disposed on a right side 306 of the display 304 and one of the speakers is disposed on the left side 308 of the display 304. Both speakers 256 are disposed on the front side 302 of tablet computer 300.

[0056] The example tablet computer 300 also includes a microphone 258. In the example illustrated, the microphone 258 is vertically disposed below the display 304 when the tablet computer is held in the landscape orientation illustrated in FIG. 4. The microphone 258 may be located in other locations in other example embodiments.

[0057] The example tablet computer 300 also includes a front facing camera 253 which may be located vertically above the display 304 when tablet computer 300 is held in a landscape orientation (i.e. the orientation of FIG. 3). The front facing camera 253 is located so that it may capture images of objects which are located in front of and/or surrounding the front side of tablet computer 300.

[0058] The example tablet computer 300 also includes an electromagnetic radiation source 257. The electromagnetic radiation source 257 is disposed on the front side 304 of tablet computer 300. In this orientation, electromagnetic radiation which is produced by the electromagnetic radiation source 257 may be projected onto objects which are located in front of and/or surrounding the front side 302 of tablet computer 300. Such electromagnetic radiation (or the projection of electromagnetic radiation onto objects) may be captured on images obtained by the camera 253.

Samsung Ex. 1004, Page 423 of 563

[0059] Although a specific wireless device 201 has just been described, any suitable wireless communication device or terminal may be part of the methods and apparatus which will be described in fuller detail below. Also, although the description of the architecture relates to a specific example for illustration, where the wireless network or WLAN is an IEEE 802.11-based network, different environments may be applicable as well. The wireless network may be a WiMAX-based network (i.e. IEEE 802.16), or an Ultra-WideBand (UWB)-based network (i.e. IEEE 802.15), as a few examples.

[0060] Example Wireless Network Configurations/Connections. FIG. 5 is an illustrative representation of a part of the communication system 100 of FIG. 1, which illustrates different types of wireless network configurations which may involve wireless device 201. Wireless networks 104 and 122 are WLANs of the traditional "WLAN infrastructure" type, which typically provide for external network connectivity, as described earlier in relation to FIG. 1. For example, wireless networks 104 and 122 are configured to provide or facilitate access to the Internet 120 (or other communication network, such as a public communication network) for wireless device 201 when connected therewith. In this case, wireless device 201 may make use of its WLAN profiles for connecting with such WLANs.

[0061] Other wireless networking configurations include Wi-Fi peer-to-peer (P2P) wireless networking configurations. For example, in FIG. 5 it is shown that wireless device 201 may establish a Wi-Fi P2P wireless connection with a display device 504 (or monitor) which includes a wireless transceiver 502. Such Wi-Fi P2P wireless network connection may be suitable for applications such as, for example, a streaming media application, or a display or presentation application.

[0062] It is also shown that wireless device 201 may establish a Wi-Fi P2P wireless network connection with a printer device 508 which includes a wireless transceiver 506. Such Wi-Fi P2P wireless network connection may be suitable for applications such as, for example, a print application or a facsimile application.

[0063] Even further, it is shown that wireless device 201 may establish a Wi-Fi P2P wireless network connection with a tablet 514 which includes a wireless transceiver 512. An example tablet was previously shown and described in relation to FIG. 4. Such Wi-Fi P2P wireless network connection may be suitable for an applications such as, for example, a "bridge" or "bridging" application, where wireless device 201 is further configured for cellular telecommunications (e.g. equipped with a cellular transceiver) but tablet 514 is not. In such application, tablet 514 is able to achieve external network (e.g. Internet) connectivity, being connected to wireless device 201 for communications via the cellular telecommunication network.

[0064] It is further shown in FIG. 5 that wireless device 201 may establish a Wi-Fi P2P wireless network connection in an ad hoc wireless network 550 which includes one or more other wireless devices 520, 522, and 524. Such Wi-Fi P2P wireless network connection may be suitable for applications such as, for example, a file sharing application, a conference meeting application, a game or gaming application, or a military application. In many instances, such ad hoc wireless networks provide no external network connectivity.

[0065] When wireless device 201 is connected as such, using one or more Wi-Fi P2P wireless network connections, data may be communicated "directly" between wireless device 201 and the other devices (i.e. without the data traversing any fixed wireless network infrastructure).

[0066] Profiles For Applications Which Make Use Of Wi-Fi P2P Wireless Connections. As described earlier, wireless device 201 has different types of applications stored therein. These applications may include, as examples, a messaging application, a voice telephony application, a Web browsing application, a streaming media application, a file sharing application, a game application, a printer application, a facsimile application, a display or presentation application, a military application, as examples. Wireless device 201 is optimized to establish the appropriate wireless networks based on which type of application is invoked.

[0067] Referring ahead to FIG. 6, an illustrative representation of another portion of memory 224 of wireless device 201 is shown. Memory 224 is shown to store a plurality of profiles for wireless networking. The profiles include one or more profiles 602 associated with WLAN infrastructure networks, and/or one or more profiles 604 associated with applications and/or services which utilize Wi-Fi P2P wireless network connections. In FIG. 6, profiles 602 are shown to include profiles 605, 615, and 625, whereas profiles 604 are shown to include profiles 610, 620, and 630. Profiles 602 may be or be referred to as WLAN profiles, whereas profiles 604 may be or be referred to as Wi-Fi P2P wireless networking profiles or Wi-Fi Direct profiles.

[0068] Each one of profiles 602 is associated with a particular WLAN infrastructure network, and includes a plurality of parameters and/or properties for accessing the particular WLAN. The WLAN information may include an identification which identifies the WLAN to access (e.g. a SSID or ESSID). The WLAN information may also include authentication and/or security information for obtaining access to the WLAN (e.g. a network key, passkey, security key, etc.). One of the WLANs appropriate WLAN from profiles 602 will be selected for communication when available, as prioritized in a prioritized list of the profiles 602. When not connected in a WLAN, the wireless device normally operates to search for WLANs identified in its stored profiles 602. Conversely, the wireless device normally refrains from searching for and communicating in WLANs other than those WLANs identified in stored profiles 602.

[0069] On the other hand, each one of profiles 604 is associated with one of the applications and/or services

Samsung Ex. 1004, Page 424 of 563

which utilizes a particular type and/or configuration of Wi-Fi P2P wireless network (or Wi-Fi Direct network). Each one of profiles 604 includes parameters and/or properties associated with establishing the particular type and/or configuration of Wi-Fi P2P wireless network for the application and/or service. Profiles 604 may be created, viewed, updated, enabled, and disabled, as described in the present disclosure (see e.g. discussion in relation to FIG. 10).

[0070] Properties in profiles 604 may include the following. Properties may include a device type property which indicates a device type of the device for the Wi-Fi P2P wireless network connection to be established. The device type may be the device type that is being searched for in the discovery. Note that there may be two device types specified in the profile: a primary device type and a secondary device type. The device types may be or include the appropriate device types in the Wi-Fi Direct Network as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex B thereof). The device types may be or include the predefined values as set forth therein. The device type may be or include category identification (ID) and/or subcategory identification (ID). Examples of such types are as follows: a computer, an input device, a printer, a camera, a display (monitor), a gaming device, an audio device, a multimedia device, or a telephone device.

[0071] Properties may additionally or alternatively include an advertised device type property which indicates the device type of wireless device 201. The advertised device type may be the device type to be advertised by wireless device 201. Note that there may be two advertised device types specified in the profile: a primary advertised device type, and a secondary advertised device type. The advertised device types may be or include the appropriate device types in the Wi-Fi Direct Network as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex B thereof). The device types may be or include the predefined values as set forth therein. The advertised device type may be or include category identification (ID) and/or subcategory identification (ID). Examples of such types are as follows: a computer, an input device, a printer, a camera, a display (monitor), a gaming device, an audio device, a multimedia device, or a telephone device.

[0072] Properties in profiles 604 may additionally or alternatively include a service type property which indicates a service type which identifies the service associated with the device. For example, the service types may be or include the appropriate service types as described in the Wi-Fi Peer-To-Peer (P2P) Technical specification (e.g. in Annex E thereof). Examples of such types are as follows: a file sharing service, or a printing service. Alternatively, examples of such types are as follows: Apple File Sharing (AFP) service (or AFP over TCP service), or IP Printing (IPP) Bonjour service.

[0073] Properties in profiles 604 may additionally or alternatively include a discovery mode property which indicates a mode utilized for the discovery of devices for the Wi-Fi P2P wireless network connection. The discovery mode property may be set to one of the following: a triggered mode of discovery, or a periodic mode of discovery. Alternatively, the discovery mode may be set to one of the following: a triggered mode of discovery, a periodic mode of discovery, or a Group Owner (GO) mode of discovery.

[0074] Properties in profiles 604 may additionally or alternatively include a persistent property or indication which indicates whether or not the Wi-Fi P2P wireless network is persistent. If the network is persistent, when an application is opened or activated, the wireless device connects to a previously-established Wi-Fi P2P wireless network.

[0075] Properties in profiles 604 may additionally or alternatively include a coexistence indication or property which indicates whether the Wi-Fi P2P wireless network connection associated with this profile may be maintained while the wireless device operates as a client in an infrastructure network. Properties may additionally or alternatively include another coexistence indication or property which indicates whether the Wi-Fi P2P wireless network connection associated with this profile may be maintained while maintaining another Wi-Fi P2P wireless network connection.

[0076] Note that properties in profiles 604 may omit a device identifier which identifies any particular device for connection, and/or may omit a wireless network identifier which identifies any particular wireless network for connection. Rather, properties in at least some of profiles 604 indicate connection with particular types of devices (and/or services), and/or indicate connection with particular types of networks, as opposed to specifically identified devices, or specifically identified networks.

[0077] More On Use Cases: Additional/Alternative Profile Details. It is noted that many peer-to-peer "use cases" for Wi-Fi P2P wireless networking lend themselves to different modes of operation. For example, if a wireless device supports a network gateway feature (e.g. a mobile hotspot or MHO feature), then the wireless device may be configured to establish a persistent Wi-Fi P2P wireless network when the service is enabled. As another example, the same wireless device may require a printer service to allow an application to print a document. In this case, the Wi-Fi P2P wireless network may be established on-demand based on an application trigger. In another example, a social networking application may periodically search for other communication devices running the same social networking application, which may result in the wireless device operating in a periodic discovery mode for other devices which advertise the same service.

[0078] To accommodate for such various use cases, profiles associated with the various application/services utilizing Wi-Fi P2P wireless networks are created and stored on the wireless device. These profiles are enabled when needed, such as enabled in response to an acti-

Samsung Ex. 1004, Page 425 of 563

vation of an application associated therewith. Further, the profiles may be enabled concurrently.

[0079] In one embodiment, the profiles may have data structures defined for compatibility with the Wi-Fi Peer-To-Peer (P2P) Technical specification. Each profile may include information specific to Wi-Fi P2P wireless network operation, including device discovery behavior, service discovery options, co-existence with infrastructure connectivity, as well as operational characteristics of the network (e.g. whether it is persistent, or triggered on application launch).

[0080] These profiles may be provisioned as defaults in the wireless device, and/or may be configured by applications when installed. Further, the profiles may be configured via the user interface of the wireless device with use of a human-machine interface (HMI) application that provides management of the profiles. This HMI application may be configured to provide the ability to search for and identify any Wi-Fi P2P wireless networks.

[0081] The profiles are used to manage the behavior of the WLAN or Wi-Fi driver of the wireless device to accommodate for the various application/services. The driver may be configured to support each particular use case. More particularly, the driver may use the profile information to manage peer-to-peer communications on the wireless device, as well as to arbitrate between Wi-Fi P2P wireless network and other modes of connectivity (e.g. infrastructure STA mode). The driver may be further configured to support other application requirements, such as sleep modes, discovery modes, and/or co-existence with an infrastructure network connection over WLAN, etc. An example set of properties and/or parameters relating to the behavioral characteristics were provided earlier above.

[0082] FIG. 7 illustrates that wireless device 201 may operate as a P2P concurrent device in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification. In this case, wireless device 201 has a first MAC entity 902 operating as a "WLAN-STA" and a second MAC entity 904 operating as a "P2P Device". Dual MAC functionality may be implemented as, for example, two virtual MAC entities over one physical layer (PHY) entity. Thus, wireless device 201 may operate to concurrently maintain two different types of wireless connections via the same wireless transceiver or PHY entity. However, wireless device 201 may only have a single Media Access Control (MAC) address assigned to the wireless transceiver for identifying communications to and from wireless device 201.

[0083] Note that, in section 2.4.3 ("P2P Device addressing") of the Wi-Fi P2P Technical specification, it is described that "[a] P2P Device shall have a P2P Device Address, conforming to the format as described in §7.1.3.3.1 of IEEE Std 802.11-2007 [1], which is used to uniquely reference that P2P Device. The P2P Device Address of a P2P Device shall be its globally administered MAC address, or its globally administered MAC address with the locally administered bit set. The P2P Device Address shall be used as the receiver address (RA) for all frames sent to a P2P Device during P2P Discovery, with the sole exception of using a broadcast receiver address in a Probe Request. The P2P Device Address shall be used as the transmitter address (TA) for all frames sent by a P2P Device during P2P Discovery."

[0084] FIG. 8 is an illustration of a format associated with a hardware address 800 which is a MAC address. The hardware or MAC address may be or be referred to as a layer-2 address of the device. The MAC address is a code that is assigned to an interface of a device, which essentially represents a code for uniquely identifying the device. MAC is used for access to the physical layer from the data link layer according to the ISO/OSI model. Most layer-2 protocols utilize one of three numbering spaces governed by the IEEE: MAC-48, EUI-48, and EUI-64 (where EUI stands for Extended Unique Identifier). They are all designed to be globally unique, even if not all the communication protocols require such feature.

[0085] The original IEEE 802 MAC address utilizes MAC-48. With MAC-48, there are 2^{48} (i.e., 281,474,976,710,656) possible MAC addresses. In its most common format, the 48-bit code of the MAC address is divided into 12 hex digits. The hexadecimal notation is used at least to differentiate it from IP addresses that use decimal notation. The first 6 hex digits identify the manufacturer of the device, while the later 6 hex digits are the serial number of the device. The MAC address is usually written in 6 octets separated by a hyphen (e.g. 00-50-FC-B0-67-2C), where the first 3 octets are referred to as the Organizationally Unique Identifier (OUI).

[0086] An address may either be a "universally administered address" or a "locally administered address". A universally or globally administered address is assigned to the device by its manufacturer and may also be referred to as a "burned-in address." The first three octets (in transmission order) identify the organization or producer that issued the identifier, and represent the OUI. The next three octets (MAC-48 and EUI-48), or five octets (EUI-64), are assigned by the producer only has to respect the constraint of uniqueness. On the other hand, a locally administered address is assigned to a component by a network administrator, overriding the burned-in address. Locally administered addresses do not contain OUIs. Universally administered and locally administered addresses are distinguished by setting the second-least-significant bit of the most significant byte of the address. This bit is also referred to as a Universal/Local (U/L) bit, which identifies how the address is administered. If the bit is "0", the address is universally administered. If the bit is "1", the address is locally administered.

[0087] FIG. 9 is an example format of a data frame 900 which may be utilized for communications to and/or from the wireless device of the present disclosure. In this example, data frame 900 has a format suitable for communication in accordance with IEEE 802.11. Data frame 900 includes one or more address fields for the identification of devices associated with the communications, and a

Samsung Ex. 1004, Page 426 of 563

payload field 910 for carrying a payload of data. A device may be identified by its hardware address (e.g. its MAC address) (see e.g. FIG. 8). A destination address field 902 is generally populated with a destination address which is the hardware address assigned to the device that is receiving data frame 900. A source address field 904 is generally populated with a source address which is the hardware address assigned to the device that is transmitting data frame 900. Other address fields may be included as well, such as an address field 906 which is populated with the hardware address of the router interface to which the associated AP is attached, and/or an address field 910 which is populated with the hardware address for ad hoc mode.

[0088] FIG. 10 is a block diagram of a portion of relevant components of wireless device 201 which is in communication with other wireless devices 1010 and 1012. In general, wireless device 201 of the present disclosure includes a first wireless transceiver 1002 and a second wireless transceiver 1004 for communications. First wireless transceiver 1002 may represent communication subsystem 211 in FIG. 2, whereas second wireless transceiver 1004 may represent communication subsystem 262 in FIG. 2.

[0089] First wireless transceiver 1002 may be operative in accordance with an IEEE 802.11 communication standard. First wireless transceiver 1002 may further be operative in accordance with the Wi-Fi Peer-To-Peer (P2P) Technical specification, such that wireless device 201 is configured to operate as a P2P concurrent device as described earlier above (e.g. in relation to FIG. 7). On the other hand, second wireless transceiver 1004 may be operative in accordance with a BLUETOOTH communication standard.

[0090] As illustrated, wireless device 201 is configured for communicating via first wireless transceiver 1002 over a first wireless connection 1020 with a first device 1010 (e.g. a wireless AP of a WLAN). Here, communications to and/or from wireless device 201 are addressed with a first hardware address assigned to first wireless transceiver 1002. The first hardware address may be the universally administered hardware address or MAC address assigned to first wireless transceiver 1002. Wireless device 201 is further configured for communicating via first wireless transceiver 1002 over a second wireless connection 1022 with a second device 1012 (e.g. a Wi-Fi P2P device). Here, communications to and/or from wireless device 201 are addressed with a second hardware address assigned to second wireless transceiver 1004. The second hardware address may be the universally administered hardware address or MAC address assigned to second wireless transceiver 1004.

[0091] The first wireless connection 1020 may be a wireless local area network (WLAN) infrastructure connection (where wireless device 201 operates as a WLAN-STA), and the second wireless connection 1022 may be a WiFi Peer-to-Peer (P2P) connection. The first and second wireless connections may be concurrent wireless connections.

[0092] Note further that wireless device 201 may be additionally configured for communicating via second wireless transceiver 1004 over a third wireless connection 1024 with second device 1012 or a third device (e.g. a BLUETOOTH device). In this case, communications to and/or from wireless device 201 are addressed with the second hardware address assigned to second wireless transceiver 1004. The third wireless communication 1024 may be a BLUETOOTH connection. Note that the first and the third wireless connections 1020 and 1024 are point-to-point connections.

[0093] FIG. 11 is a flowchart for describing a method for use in facilitating communications over first and second wireless connections of a wireless transceiver. The method of FIG. 11 may be performed by wireless device 201 described in relation to FIGs. 1-10 above, and relates to an initialization procedure of the wireless device. The wireless device includes a first wireless transceiver (e.g. IEEE 802.11) and a second wireless transceiver (e.g. BLUETOOTH). In such technique, the wireless device may operate in accordance with or be compatible with the Wi-Fi P2P wireless network protocols in the Wi-Fi Peer-To-Peer (P2P) Technical specification. Each wireless transceiver may be contained within a hardware transceiver module or chip (e.g. IC) in the wireless device, or alternatively both wireless transceivers may be contained within the same hardware transceiver module or chip. Each module or chip includes a memory for storing one or more hardware addresses assigned to the one or more wireless transceivers.

[0094] The techniques described in relation to the flowchart of FIG. 11 may be performed by one or more controllers or processors of the wireless device along with its wireless or RF transceiver(s). A computer program product which may embody the technique may include a computer readable medium (e.g. memory of the communication device, computer disk, CD-ROM, etc.) having computer instructions stored therein which are executable by the one or more processors of the wireless device for performing the technique.

[0095] In the technique of FIG. 11, the wireless device performs an initialization procedure for initialization (step 1102 of FIG. 11). This initialization procedure may be performed in response to the wireless device being powered "on" or reset, for example, or from other suitable event or condition. Amongst other initialization tasks, the wireless device reads, from memory of the first wireless transceiver, a first hardware address assigned to the first wireless transceiver (step 1104 of FIG. 11). The wireless device stores this first hardware address in its device memory (e.g. flash memory 244 of FIG. 2) for subsequent use in identifying communications to and/or from the device via the first wireless transceiver for a first type of wireless connection (step 1106 of FIG. 11).

[0096] In addition, the wireless device reads, from memory of the second wireless transceiver, a second hardware address assigned to the second wireless trans-

Samsung Ex. 1004, Page 427 of 563

ceiver (step 1108 of FIG. 11). The wireless device stores this second hardware address in its device memory (e.g. flash memory 244 of FIG. 2) for subsequent use in identifying communications to and/or from the device via the first wireless transceiver for a second type of wireless connection (step 1110 of FIG. 11). Note further that the wireless device may also store this second hardware address in its device memory (e.g. flash memory 244 of FIG. 2) for subsequent use in identifying communications to and/or from the device via the second wireless transceiver for a third type of wireless connection. The flowchart ends at an end block 1112.

[0097] In some embodiments, the first and second hardware addresses are universally administered hardware addresses that are assigned to the first and the second wireless transceivers, respectively. These universally administered hardware addresses may be the MAC addresses assigned to the wireless transceivers during manufacture.

[0098] Also, the first wireless transceiver may be configured to communicate in accordance with an IEEE 802.11 communications standard, and the second wireless transceiver may be configured to communicate in accordance with a BLUETOOTH® communications standard. Thus, in some embodiments, the wireless device may utilize the MAC address of the IEEE 802.11 transceiver for identifying communications to and/or from via the IEEE 802.11 transceiver for WLAN-STA connections, and utilize the MAC address of the BLUETOOTH transceiver for identifying communications to and/or from via the IEEE 802.11 transceiver for Wi-Fi P2P connections. The wireless device may also utilize the MAC address of the BLUETOOTH transceiver for identifying communications to and/or from the device via the BLUETOOTH transceiver for BLUETOOTH connections. The first and second wireless connections may be concurrent wireless connections.

[0099] FIG. 12 is another flowchart for describing another method for use in facilitating communications over first and second wireless connections of a wireless transceiver. The method of FIG. 12 may be performed by wireless device 201 described in relation to FIGs. 1-10, with use of or without the technique of FIG. 11. The wireless device includes a first wireless transceiver (e.g. IEEE 802.11) and a second wireless transceiver (e.g. BLUETOOTH). In such technique, the wireless device may operate in accordance with or be compatible with the Wi-Fi P2P wireless network protocols in the Wi-Fi Peer-To-Peer (P2P) Technical specification. Each wireless transceiver may be contained within a hardware transceiver module or chip (e.g. IC) in the wireless device, or alternatively both wireless transceivers may be contained within the same hardware transceiver module or chip. Each module or chip includes a memory for storing one or more hardware addresses assigned to the one or more wireless transceivers.

[0100] The techniques described in relation to the flowchart of FIG. 12 may be performed by one or more controllers or processors of the wireless device along with its wireless or RF transceiver(s). A computer program product which may embody the technique may include a computer readable medium (e.g. memory of the communication device, computer disk, CD-ROM, etc.) having computer instructions stored therein which are executable by the one or more processors of the wireless device for performing the technique.

[0101] Beginning at a start block 1202 of FIG. 12, the wireless device operates to communicate via the first wireless transceiver over a first wireless connection with a first device (step 1204 of FIG. 12). The communications to and from the wireless device over the first wireless connection of the first wireless transceiver are addressed with a first hardware address that is assigned to the first wireless transceiver. This first hardware address may be the address that was read from memory of the first wireless transceiver and stored in device memory as described in relation to steps 1104 and 1106 of FIG. 11.

[0102] During communications in relation to step 1204, the wireless device may receive, via the first wireless transceiver over the first wireless connection, data in one or more data frames having a destination address which is the first hardware address. Additionally or alternatively, the wireless device may send, via the first wireless transceiver over the first wireless connection, data in one or more data frames having a source address which is the first hardware address. See e.g. the discussion in relation to FIG. 9. Also additionally or alternatively, the wireless device may operate to advertise its presence and/or availability to surrounding devices (e.g. in a discovery procedure), via the first wireless transceiver, using the first hardware address to identify itself.

[0103] In addition, the wireless device operates to communicate via the first wireless transceiver over a second wireless connection with a second device (step 1206 of FIG. 6). The communications to and from the wireless device over the second wireless connection of the first wireless transceiver are addressed with a second hardware address that is assigned to the second wireless transceiver. This second hardware address may be the address that was read from memory of the second wireless transceiver and stored in device memory as described in relation to steps 1108 and 1110 of FIG. 11.

[0104] During communications in relation to step 1204, the wireless device may receive, via the first wireless transceiver over the second wireless connection, data in one or more data frames having a destination address which is the second hardware address. Additionally or alternatively, the wireless device may send, via the first wireless transceiver over the second wireless connection, data in one or more data frames having a source address which is the second hardware address. See again e.g. the discussion in relation to FIG. 9. Also, for example, the wireless device may operate to advertise its presence and/or availability to surrounding devices (e.g. in a discovery procedure), via the first transceiver, using the second hardware address to identify itself.

Samsung Ex. 1004, Page 428 of 563

[0105] The first and second hardware addresses may be the universally administered hardware addresses that are assigned to the first and the second wireless transceivers, respectively. These universally administered hardware addresses may be the MAC addresses assigned to the wireless transceivers during manufacture. The first wireless transceiver may be configured to communicate in accordance with an IEEE 802.11 communications standard, and the second wireless transceiver may be configured to communicate in accordance with a BLUETOOTH® communications standard. Thus, in some embodiments, the wireless device may utilize the MAC address of the IEEE 802.11 transceiver for identifying the device for communications via the IEEE 802.11 transceiver for WLAN-STA connections, and utilize the MAC address of the BLUETOOTH transceiver for communications via the IEEE 802.11 transceiver for Wi-Fi P2P connections. The wireless device may also utilize the MAC address of the BLUETOOTH transceiver for identifying the device in association with BLUETOOTH connections via the BLUETOOTH transceiver.

[0106] The first and the second wireless connections in steps 1204 and 1206 may be concurrently maintained by the wireless device. For example, the wireless device may operate as a concurrent device in accordance with or be compatible with the Wi-Fi P2P wireless network protocols in the Wi-Fi Peer-To-Peer (P2P) Technical specification.

[0107] In some embodiments, one or more additional steps may be included in the method of FIG. 12. In one embodiment, wireless device operates to communicate via the second wireless transceiver over a third wireless connection with a third device. The communications to and from the wireless device over the third wireless connection of the second wireless transceiver are addressed with the second hardware address that is assigned to the second wireless transceiver. During these communications, the wireless device may receive, via the second wireless transceiver over the second wireless connection, data in one or more data frames having a destination address which is the second hardware address. Additionally or alternatively, the wireless device may send, via the second wireless transceiver over the second wireless connection, data in one or more data frames having a source address which is the second hardware address. Also alternatively, for example, the wireless device may operate to advertise its presence and/or availability to surrounding devices (e.g. in a discovery procedure), via the second transceiver, using the second hardware address to identify itself.

[0108] In such embodiments, the wireless device may further operate to concurrently maintain the first, the second, and the third wireless connections via the first and the second wireless transceivers. Here, the same second hardware address is utilized for identifying the communications to and/or from the wireless device over the second and the third wireless connections. In this case, the device operates to mark the communications for one of the wireless connections for distinguishing therebetween. For example, the device may mark the locally administered bit for the MAC address for use of the third wireless connection.

[0109] In further embodiment, the wireless device may operate to switch from communicating via the first wireless transceiver over the second wireless connection with the second device to communicating via the second wireless transceiver over the third wireless connection with the second device. This switching may be performed, for example, in order to reduce power consumption of the wireless device while maintaining communications with the second device. Accordingly, the wireless device may subsequently operate to switch back from communicating via the second wireless transceiver over the third wireless connection to the first wireless transceiver over the second wireless connection. This switching back may be performed for example, in order to increase data throughput of the wireless device.

[0110] Thus, as described herein, a wireless communication device of the present disclosure includes a first wireless transceiver and a second wireless transceiver. The wireless device is configured for communicating via the first wireless transceiver over a first wireless connection with a first device, where communications to and from the wireless device are identified using a first (universally administered) hardware address assigned to the first wireless transceiver. The wireless device is further configured for communicating via the first wireless transceiver over a second wireless connection with a second device, where communications to and from the wireless device are identified with a second (universally administered) hardware address assigned to the second wireless transceiver. The first and second hardware addresses may be Media Access Control (MAC) addresses of the first and the second wireless transceivers. The first and the second wireless connections may be concurrent wireless connections. In some embodiments, the first wireless transceiver may be configured for communications in accordance with an IEEE 802.11 standard, and the second wireless transceiver may be configured for communications in accordance with a BLUETOOTH® standard. The first wireless connection may be a wireless local area network (WLAN) infrastructure connection, and the second wireless connection may be a WiFi Peer-to-Peer (P2P) connection. Thus, in some embodiments, the wireless device may utilize the MAC address of the IEEE 802.11 transceiver for identifying communications to and/or from the device via the IEEE 802.11 transceiver for WLAN-STA connections, and utilize the MAC address of the BLUETOOTH transceiver for identifying communications to and/or from the device via the IEEE 802.11 transceiver for Wi-Fi P2P connections.

[0111] In other embodiments, a wireless device of the present disclosure is configured for reading from memory of the first wireless transceiver a first hardware address that is assigned to the first wireless transceiver, and storing in device memory the first hardware address for sub-

Samsung Ex. 1004, Page 429 of 563

sequent use in identifying communications to and/or from the wireless device via the first wireless transceiver for a first type of wireless connection. The wireless device is further configured for reading from memory of the second wireless transceiver a second hardware address that is assigned to the second wireless transceiver, and storing in the device memory the second hardware address for subsequent use in identifying communications to and/or from the wireless device via the first wireless transceiver for a second type of wireless connection. The first and second hardware addresses may be Media Access Control (MAC) addresses of the first and the second wireless transceivers. The first and the second types of wireless connections may be types of concurrent wireless connections. In some embodiments, the first wireless transceiver may be configured for communications in accordance with an IEEE 802.11 standard, and the second wireless transceiver may be configured for communications in accordance with a BLUETOOTH® standard. The first type of wireless connection may be a wireless local area network (WLAN) infrastructure type of connection, and the second wireless connection may be a WiFi Peer-to-Peer (P2P) type of connection. Thus, in some embodiments, the wireless device may utilize the MAC address of the IEEE 802.11 transceiver for identifying communications to and/or from the device via the IEEE 802.11 transceiver for WLAN-STA type of connections, and utilize the MAC address of the BLUETOOTH transceiver for identifying communications to and/or from the device via the IEEE 802.11 transceiver for Wi-Fi P2P type of connections.

[0112] The above-described embodiments of the present disclosure are intended to be examples only. Those of skill in the art may affect alterations, modifications and variations to the particular embodiments without departing from the scope of the application. Although the description relates to specific examples for illustration, where the WLAN is an IEEE 802.11-based network, for example, different environments may be applicable as well. As a few other examples, the wireless networking may be based on a WiMAX network (i.e. IEEE 802.16), or an Ultra-WideBand (UWB) network (i.e. IEEE 802.15). The invention described herein in the recited claims intends to cover and embrace all suitable changes in technology.

[0113] Examples are set out in the following list of numbered clauses.

1. A method in a wireless communication device which includes a first wireless transceiver and a second wireless transceiver, the method comprising:

   communicating via the first wireless transceiver over a first wireless connection with a first device, where communications to and/or from the wireless device are addressed with a first universally administered hardware address assigned to the first wireless transceiver; and

   communicating via the first wireless transceiver over a second wireless connection with a second device, where communications to and/or from the wireless device are addressed with a second universally administered hardware address assigned to the second wireless transceiver.

2. The method of clause 1, further comprising:

   concurrently maintaining the first and the second wireless connections via the first wireless transceiver.

3. The method of any one of clauses 1 or 2, further comprising:

   communicating via the second wireless transceiver over a third wireless connection with a third device, where communications to and from the wireless device are addressed with the second universally administered hardware address assigned to the second wireless transceiver.

4. The method of any one of clauses 1 or 2, further comprising:

   communicating via the second wireless transceiver over a third wireless connection with the second device, where communications to and from the wireless device are addressed with the second universally administered hardware address assigned to the second wireless transceiver.

5. The method of clause 4, further comprising:

   switching from communicating via the first wireless transceiver over the second wireless connection with the second device to communicating via the second wireless transceiver over the third wireless connection with the second device.

6. The method of any one of clauses 1-5, wherein the first universally administered hardware address comprises a first Media Access Control (MAC) address assigned to the first wireless transceiver, and the second universally administered hardware address comprises a second MAC address assigned to the second wireless transceiver.

7. The method of any one of clauses 1-6, wherein the first wireless transceiver is configured to communicate in accordance with an IEEE 802.11 communications standard.

8. The method of any one of clauses 1-7, wherein

Samsung Ex. 1004, Page 430 of 563

the second wireless transceiver is configured to communicate in accordance with a BLUETOOTH® communications standard.

9. The method of any one of clauses 1-8, wherein the first wireless connection comprises a wireless local area network (WLAN) infrastructure connection.

10. The method of any one of clauses 1-9, wherein the second wireless connection comprises a WiFi Peer-to-Peer (P2P) connection.

11. A computer program product, comprising:

a non-transitory computer readable medium;
computer instructions stored in the non-transitory computer readable medium; and
the computer instructions being executable by one or more processors of a wireless communication device which includes a first wireless transceiver and a second wireless transceiver, for performing the method of any one of clauses 1-10.

12. A wireless communication device, comprising:

one or more processors;
first and second wireless transceivers coupled to the one or more processors; and
the one or more processors being configured for performing the method of any one of clauses 1-10.

13. A method in a wireless communication device which includes a first wireless transceiver and a second wireless transceiver, the method comprising:

reading, from memory of the first wireless transceiver, a first universally administered hardware address assigned to the first wireless transceiver;
storing, in device memory of the wireless device, the first hardware address for use in identifying communications to and/or from the wireless device via the first wireless transceiver for a first type of wireless connection;
reading, from memory of the second wireless transceiver, a second universally administered hardware address assigned to the second wireless transceiver; and
storing, in the device memory, the second universally administered hardware address for use in identifying communications to and/or from the wireless device via the first wireless transceiver for a second type of wireless connection.

14. The method of clause 13, wherein the first wireless transceiver is configured to communicate in accordance with an IEEE 802.11 communications standard, and the second wireless transceiver is configured to communicate in accordance with a BLUETOOTH® communications standard.

15. The method of any one of clauses 13 or 14, wherein the first type of wireless connection comprises a wireless local area network (WLAN) infrastructure connection, and the second type of wireless connection comprises a WiFi Peer-to-Peer (P2P) connection.

Claims

1. A method in a wireless communication device (201) which includes a first wireless transceiver (1002) and a second wireless transceiver (1004), the method comprising:

communicating via the first wireless transceiver (1002) over a first wireless connection (1020) with a first device (1010), where communications to and/or from the wireless device are addressed with a first universally administered hardware address assigned to the first wireless transceiver (1002); and
communicating via the first wireless transceiver (1002) over a second wireless connection (1022) with a second device (1012), where communications to and/or from the wireless device are addressed with a second universally administered hardware address assigned to the second wireless transceiver (1004),
wherein the first wireless transceiver (1002) is configured to communicate in accordance with a first communications standard and the second wireless transceiver (1004) is configured to communicate in accordance with a second communications standard, wherein the first and second communications standards are different communications standards.

2. The method of claim 1, further comprising:

concurrently maintaining the first (1020) and the second (1022) wireless connections via the first wireless transceiver (1002).

3. The method of any one of claims 1 or 2, further comprising:

communicating via the second wireless transceiver (1004) over a third wireless connection (1024) with a third device, where communications to and from the wireless device are addressed with the second universally adminis-

Samsung Ex. 1004, Page 431 of 563

tered hardware address assigned to the second wireless transceiver (1004).

4. The method of any one of claims 1 or 2, further comprising:

communicating via the second wireless transceiver (1004) over a third wireless connection (1024) with the second device (1012), where communications to and from the wireless device are addressed with the second universally administered hardware address assigned to the second wireless transceiver (1004).

5. The method of claim 4, further comprising:

switching from communicating via the first wireless transceiver (1002) over the second wireless connection (1022) with the second device (1012) to communicating via the second wireless transceiver (1004) over the third wireless connection (1024) with the second device (1012).

6. The method of any one of claims 1-5, wherein the first universally administered hardware address comprises a first Media Access Control, MAC, address assigned to the first wireless transceiver (1002), and the second universally administered hardware address comprises a second MAC address assigned to the second wireless transceiver (1004).

7. The method of any one of claims 1-6, wherein the first wireless connection (1020) comprises a wireless local area network, WLAN, infrastructure connection.

8. The method of any one of claims 1-7, wherein the second wireless connection (1022) comprises a WiFi Peer-to-Peer, P2P, connection.

9. A computer program product, comprising:

a non-transitory computer readable medium;
computer instructions stored in the non-transitory computer readable medium; and
the computer instructions being executable by one or more processors of a wireless communication device (201) which includes a first wireless transceiver (1002) and a second wireless transceiver (1004), for performing the method of any one of claims 1-8.

10. A wireless communication device (201), comprising:

one or more processors;
first (1002) and second (1004) wireless transceivers coupled to the one or more processors; and
the one or more processors being configured for performing the method of any one of claims 1-8.

Patentansprüche

1. Verfahren in einer drahtlosen Kommunikationsvorrichtung (201), die einen ersten drahtlosen Transceiver (1002) und einen zweiten drahtlosen Transceiver (1004) enthält, welches Verfahren enthält:

Kommunizieren mittels des ersten drahtlosen Transceivers (1002) über eine erste drahtlose Verbindung (1020) mit einer ersten Einrichtung (1010), wobei die Kommunikation zu der und/oder von der drahtlosen Einrichtung mit einer ersten universell vorgegebenen Hardwareadresse adressiert wird, die dem ersten drahtlosen Transceiver (1002) zugewiesen ist; und
Kommunizieren mittels des ersten drahtlosen Transceivers (1002) über eine zweite drahtlose Verbindung (1022) mit einer zweiten Einrichtung (1012), wobei die Kommunikation zu der und/oder von der drahtlosen Einrichtung mit einer zweiten universell vorgegebenen Hardwareadresse adressiert wird, die dem zweiten drahtlosen Transceiver (1004) zugewiesen ist,
wobei der erste drahtlose Transceiver (1002) dafür konfiguriert ist, in Übereinstimmung mit einem ersten Kommunikationsstandard zu kommunizieren, und der zweite drahtlose Transceiver (1004) dafür konfiguriert ist, in Übereinstimmung mit einem zweiten Kommunikationsstandard zu kommunizieren, wobei der erste und der zweite Kommunikationsstandard unterschiedliche Kommunikationsstandards sind.

2. Verfahren nach Anspruch 1, ferner enthaltend:

gleichzeitiges Aufrechterhalten der ersten (1020) und der zweiten (1022) drahtlosen Verbindung mittels des ersten drahtlosen Transceivers (1002).

3. Verfahren nach einem der Ansprüche 1 oder 2, ferner enthaltend:

Kommunizieren mittels des zweiten drahtlosen Transceivers (1004) über eine dritte drahtlose Verbindung (1024) mit einer dritten Einrichtung, wobei die Kommunikation zu der und von der drahtlosen Einrichtung mit der zweiten universell vorgegebenen Hardwareadresse adressiert wird, die dem zweiten drahtlosen Transceiver (1004) zugewiesen ist.

Samsung Ex. 1004, Page 432 of 563

4. Verfahren nach einem der Ansprüche 1 oder 2, ferner enthaltend:

   Kommunizieren mittels des zweiten drahtlosen Transceivers (1004) über eine dritte drahtlose Verbindung (1024) mit der zweiten Einrichtung (1012), wobei die Kommunikation zu der und von der drahtlosen Einrichtung mit der zweiten universell vorgegebenen Hardwareadresse adressiert wird, die dem zweiten drahtlosen Transceiver (1004) zugewiesen ist.

5. Verfahren nach Anspruch 4, ferner enthaltend:

   Umschalten von der Kommunikation mittels des ersten drahtlosen Transceivers (1002) über die zweite drahtlose Verbindung (1022) mit der zweiten Einrichtung (1012) auf die Kommunikation mittels des zweiten drahtlosen Transceivers (1004) über die dritte drahtlose Verbindung (1024) mit der zweiten Einrichtung (1012).

6. Verfahren nach einem der Ansprüche 1-5, wobei die erste universell vorgegebene Hardwareadresse eine erste Media Access Control-Adresse (MAC) umfasst, die dem ersten drahtlosen Transceiver (1002) zugewiesen ist, und die zweite universell vorgegebene Hardwareadresse eine zweite MAC-Adresse umfasst, die dem zweiten drahtlosen Transceiver (1004) zugewiesen ist.

7. Verfahren nach einem der Ansprüche 1-6, wobei die erste drahtlose Verbindung (1020) eine Verbindung einer drahtlosen lokalen Netz-Infrastruktur (WLAN) umfasst.

8. Verfahren nach einem der Ansprüche 1-7, wobei die zweite drahtlose Verbindung (1022) eine Wifi-Peer-to-Peer-Verbindung (P2P) umfasst.

9. Computerprogrammprodukt, enthaltend:

   ein nichtflüchtiges computerlesbares Medium;
   in dem nichtflüchtigen computerlesbaren Medium gespeicherte Computeranweisungen; und
   wobei die Computeranweisungen durch einen oder mehrere Prozessoren einer drahtlosen Kommunikationsvorrichtung (201) ausführbar sind, die einen ersten drahtlosen Transceiver (1002) und einen zweiten drahtlosen Transceiver (1004) aufweist, um das Verfahren nach einem der Ansprüche 1-8 auszuführen.

10. Drahtlose Kommunikationsvorrichtung (201), enthaltend:

    einen oder mehrere Prozessoren;
    einen ersten (1002) und einen zweiten (1004) drahtlosen Transceiver, die mit dem einen oder den mehreren Prozessoren gekoppelt sind; und
    wobei der eine oder die mehreren Prozessoren dafür konfiguriert sind, das Verfahren nach einem der Ansprüche 1-8 auszuführen.

Revendications

1. Procédé dans un dispositif de communication sans fil (201) qui comporte un premier émetteur-récepteur sans fil (1002) et un deuxième émetteur-récepteur sans fil (1004), le procédé comprenant le fait :

   de communiquer via le premier émetteur-récepteur sans fil (1002) sur une première connexion sans fil (1020) avec un premier dispositif (1010), où les communications vers et/ou depuis le dispositif sans fil sont adressées avec une première adresse matérielle universellement administrée attribuée au premier émetteur-récepteur sans fil (1002) ; et
   de communiquer via le premier émetteur-récepteur sans fil (1002) sur une deuxième connexion sans fil (1022) avec un deuxième dispositif (1012), où les communications vers et/ou depuis le dispositif sans fil sont adressées avec une deuxième adresse matérielle universellement administrée attribuée au deuxième émetteur-récepteur sans fil (1004),
   dans lequel le premier émetteur-récepteur sans fil (1002) est configuré pour communiquer selon une première norme de communication et le deuxième émetteur-récepteur sans fil (1004) est configuré pour communiquer selon une deuxième norme de communication, où les première et deuxième normes de communication sont des normes de communication différentes.

2. Procédé de la revendication 1, comprenant en outre le fait :

   de maintenir simultanément les première (1020) et deuxième (1022) connexions sans fil via le premier émetteur-récepteur sans fil (1002).

3. Procédé de l'une quelconque des revendications 1 et 2, comprenant en outre le fait :

   de communiquer via le deuxième émetteur-récepteur sans fil (1004) sur une troisième connexion sans fil (1024) avec un troisième dispositif, où les communications vers et depuis le dispositif sans fil sont adressées avec la deuxième adresse matérielle universellement administrée attribuée au deuxième émetteur-récepteur sans fil (1004).

Samsung Ex. 1004, Page 433 of 563

4. Procédé de l'une quelconque des revendications 1 et 2, comprenant en outre le fait :

de communiquer via le deuxième émetteur-récepteur sans fil (1004) sur une troisième connexion sans fil (1024) avec le deuxième dispositif (1012), où les communications vers et depuis le dispositif sans fil sont adressées avec la deuxième adresse matérielle universellement administrée attribuée au deuxième émetteur-récepteur sans fil (1004).

5. Procédé de la revendication 4, comprenant en outre le fait :

de commuter de la communication via le premier émetteur-récepteur sans fil (1002) sur la deuxième connexion sans fil (1022) avec le deuxième dispositif (1012) à la communication via le deuxième émetteur-récepteur sans fil (1004) sur la troisième connexion sans fil (1024) avec le deuxième dispositif (1012).

6. Procédé de l'une quelconque des revendications 1 à 5, dans lequel la première adresse matérielle universellement administrée comprend une première adresse de contrôle d'accès au support, MAC, attribuée au premier émetteur-récepteur sans fil (1002), et la deuxième adresse matérielle universellement administrée comprend une deuxième adresse MAC attribuée au deuxième émetteur-récepteur sans fil (1004).

7. Procédé de l'une quelconque des revendications 1 à 6, dans lequel la première connexion sans fil (1020) comprend une connexion d'infrastructure de réseau local sans fil, WLAN.

8. Procédé de l'une quelconque des revendications 1 à 7, dans lequel la deuxième connexion sans fil (1022) comprend une connexion WiFi poste à poste, P2P.

9. Produit de programme informatique comprenant :

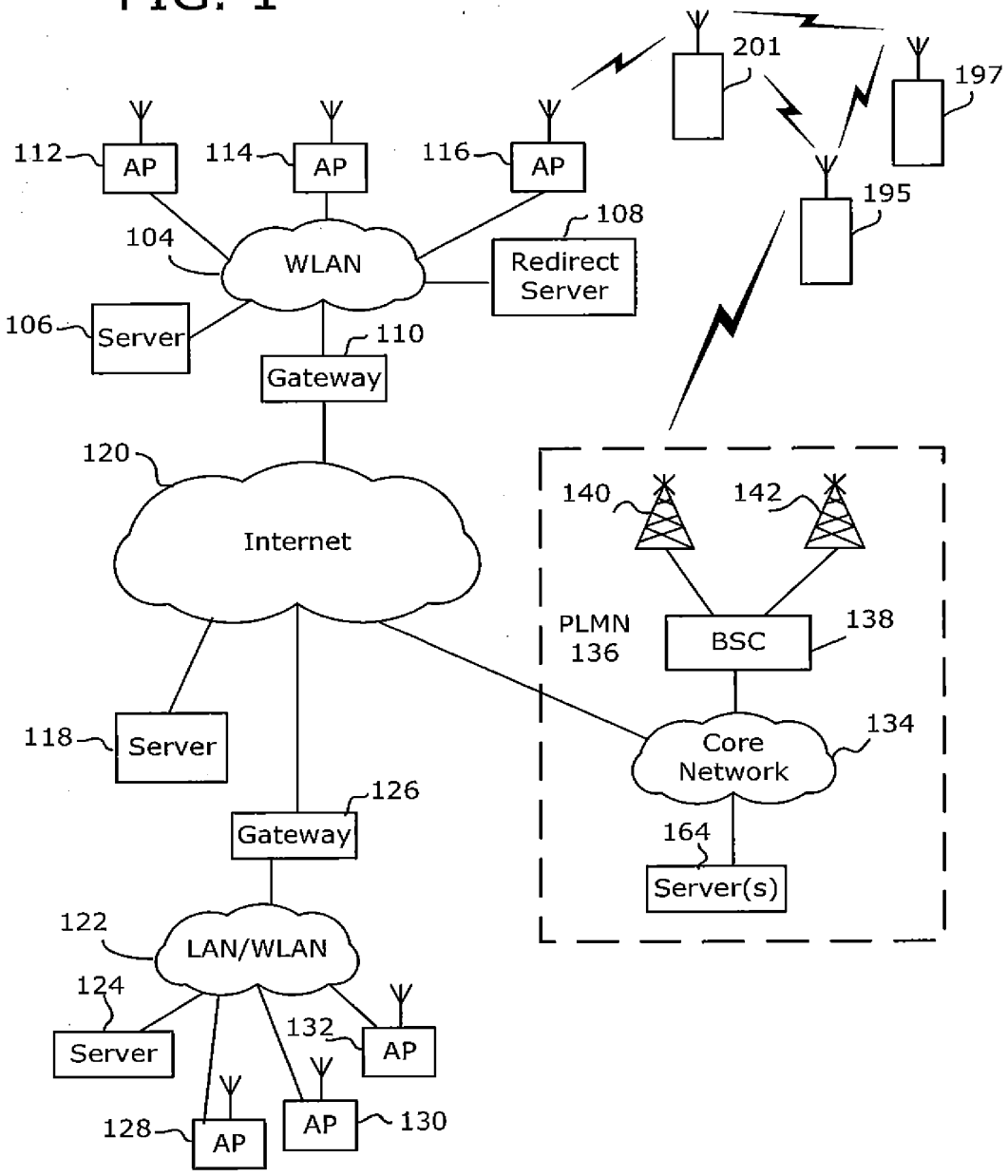
un support non transitoire lisible par ordinateur ;
des instructions informatiques stockées dans le support non transitoire lisible par ordinateur ; et
les instructions informatiques pouvant être exécutées par un ou plusieurs processeur(s) d'un dispositif de communication sans fil (201) qui comporte un premier émetteur-récepteur sans fil (1002) et un deuxième émetteur-récepteur sans fil (1004), pour mettre en oeuvre le procédé de l'une quelconque des revendications 1 à 8.

10. Dispositif de communication sans fil (201) comprenant :

un ou plusieurs processeur(s) ;
des premier (1002) et deuxième (1004) émetteurs-récepteurs sans fil couplés au ou aux plusieurs processeur(s) ; et
le ou les plusieurs processeur(s) étant configuré(s) pour mettre en oeuvre le procédé de l'une quelconque des revendications 1 à 8.

Samsung Ex. 1004, Page 434 of 563

FIG. 1


201
197
195
112
AP
114
AP
116
AP
104
WLAN
108
Redirect Server
106
Server
110
Gateway
120
Internet
140
142
PLMN 136
BSC
138
118
Server
134
Core Network
126
Gateway
164
Server(s)
122
LAN/WLAN
124
Server
132
AP
128
AP
AP
130
100

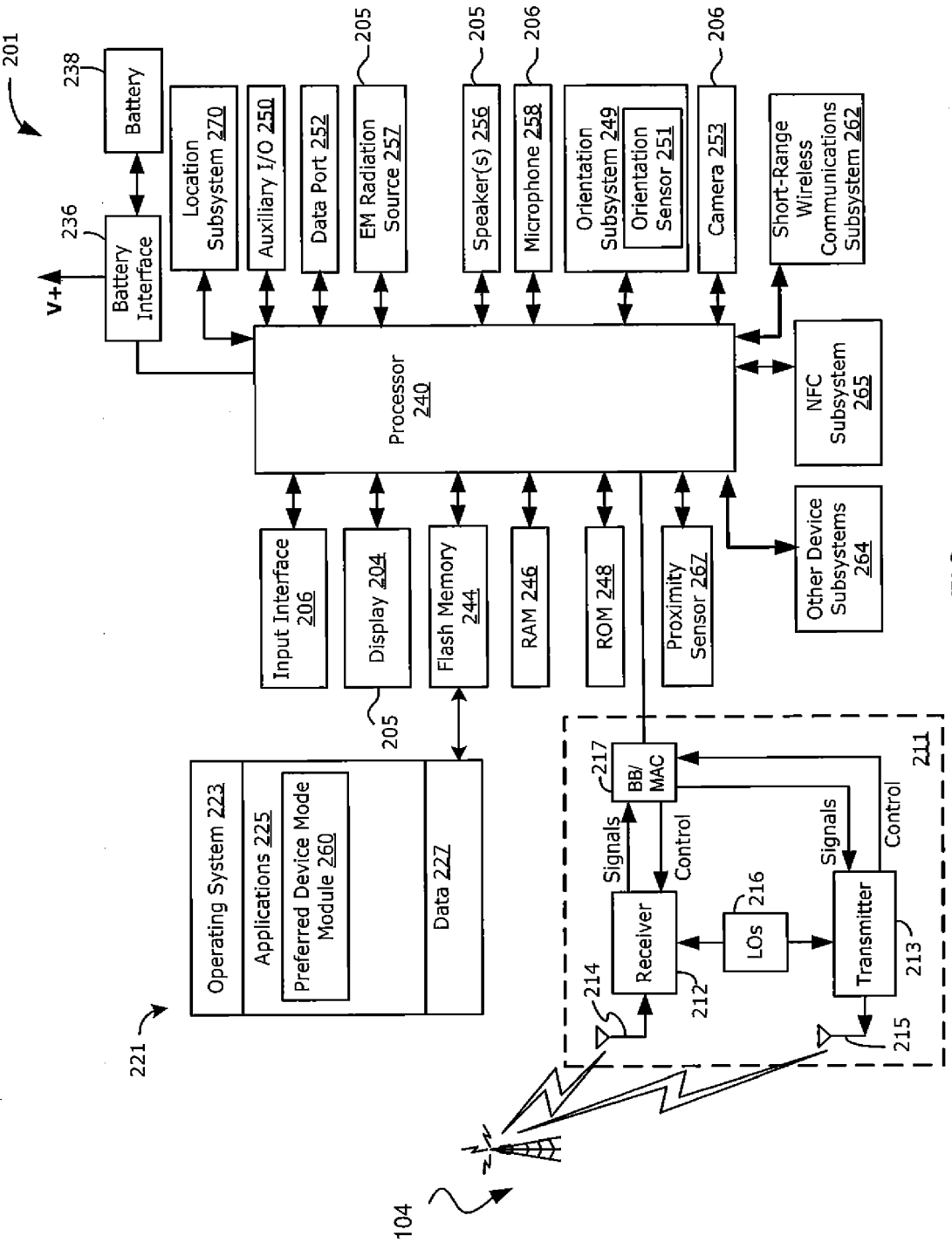

201
238
Battery
236
Battery Interface
V+
Location Subsystem 270
Auxiliary I/O 250
Data Port 252
205
EM Radiation Source 257
205
Speaker(s) 256
206
Microphone 258
Orientation Subsystem 249
Orientation Sensor 251
206
Camera 253
Short-Range Wireless Communications Subsystem 262
Processor 240
NFC Subsystem 265
Other Device Subsystems 264
Input Interface 206
Display 204
205
Flash Memory 244
RAM 246
ROM 248
Proximity Sensor 267
Operating System 223
Applications 225
Preferred Device Mode Module 260
Data 227
221
217
BB/ MAC
211
Signals
Control
Signals
Control
Receiver
212
LOs
216
Transmitter
213
214
215
104

FIG. 2

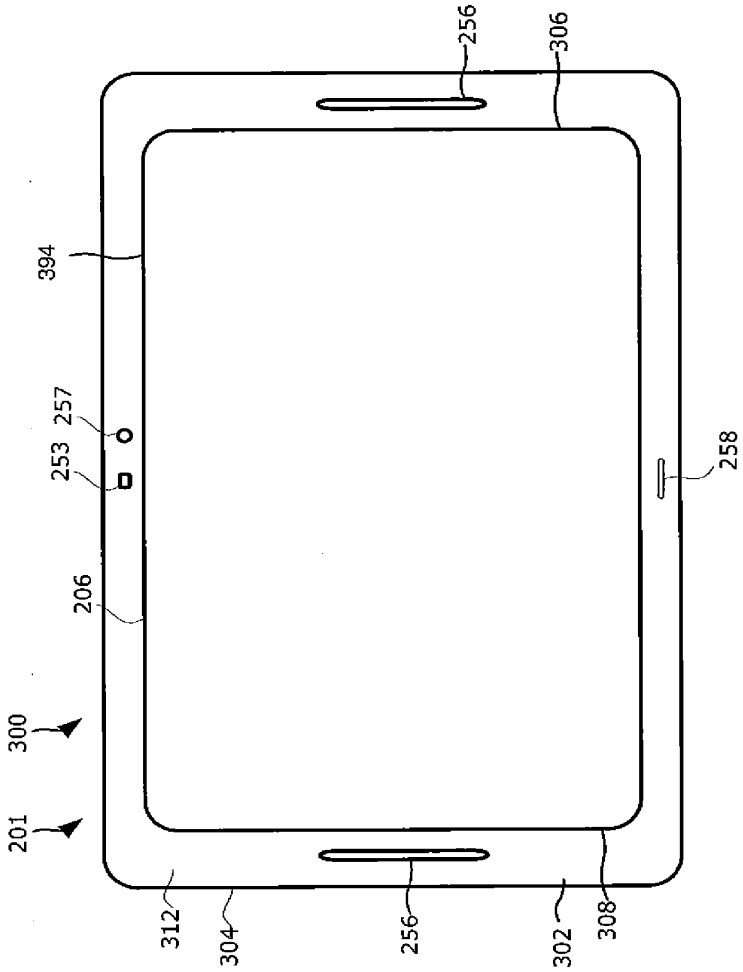

256
306
394
257
253
258
206
300
201
312
304
256
302
308

FIG. 4

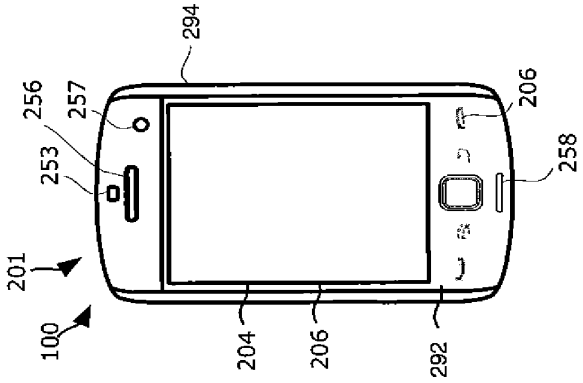

294
256
257
206
253
258
201
100
204
206
292

FIG. 3

FIG. 5

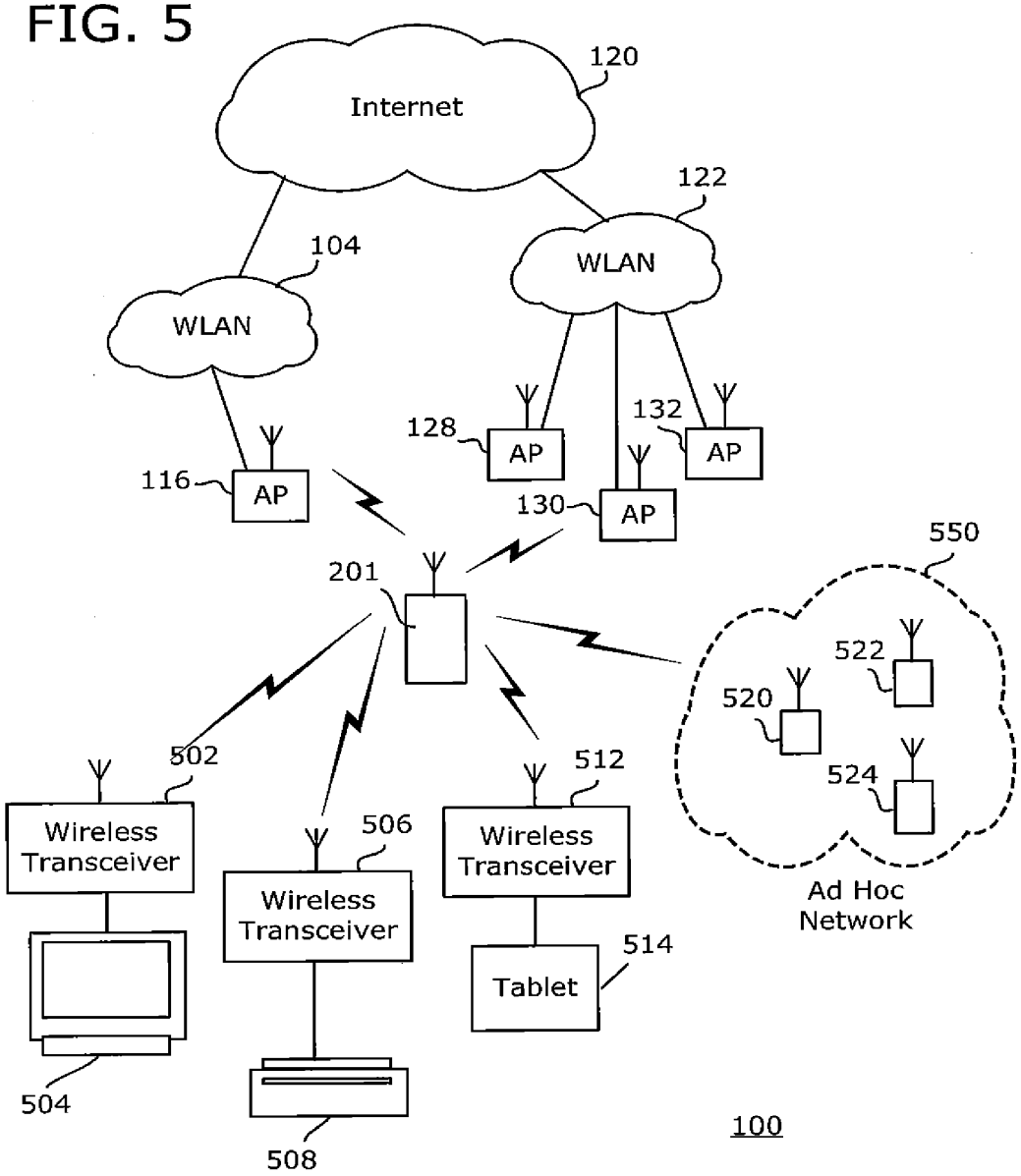

Internet
120
122
WLAN
104
WLAN
128
AP
132
AP
116
AP
130
AP
201
550
522
520
524
Ad Hoc
Network
502
512
506
Wireless
Transceiver
Wireless
Transceiver
Wireless
Transceiver
514
Tablet
504
508
100

FIG. 6

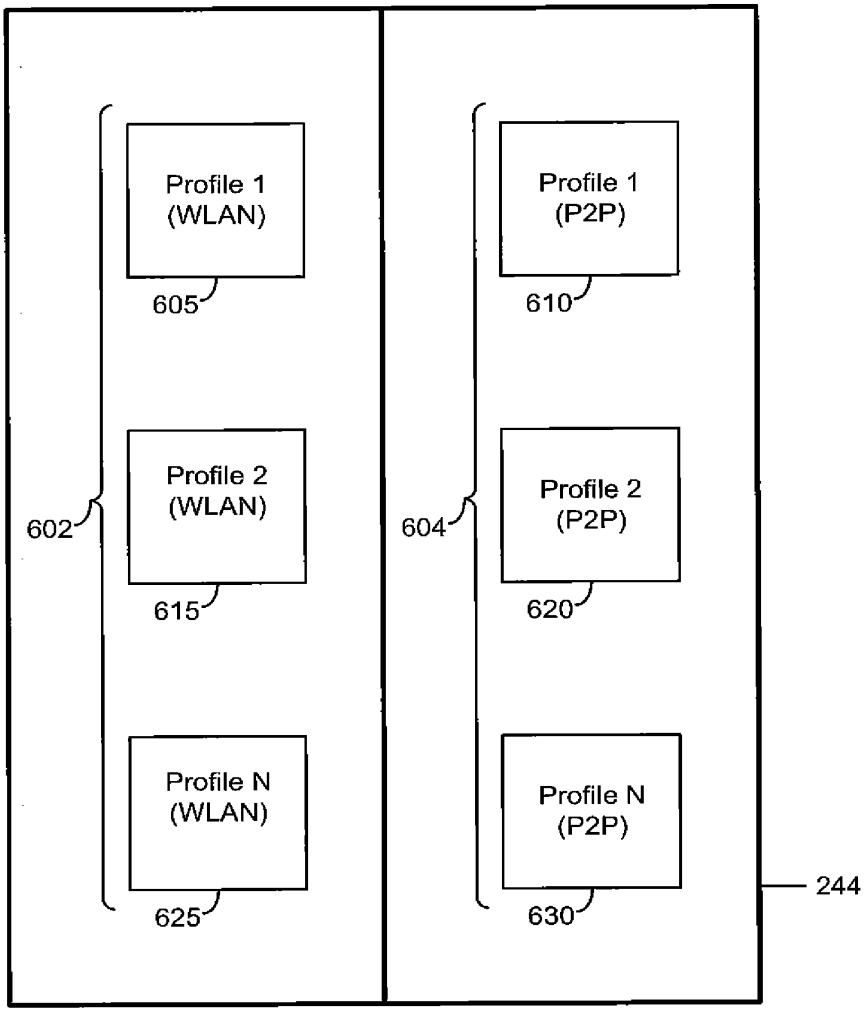
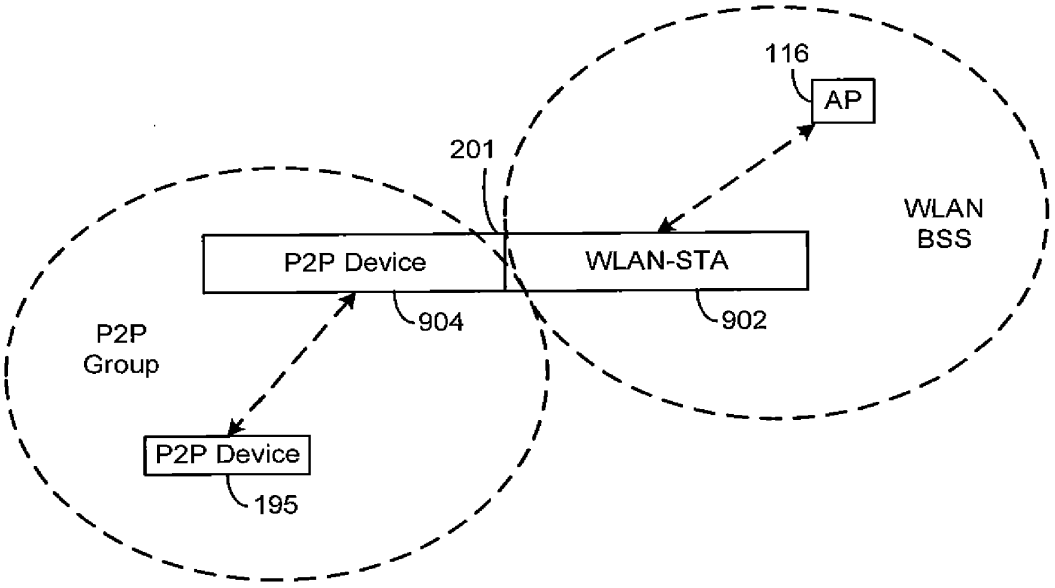

Profile 1
(WLAN)
605
Profile 2
(WLAN)
615
Profile N
(WLAN)
625
602
Profile 1
(P2P)
610
Profile 2
(P2P)
620
Profile N
(P2P)
630
604
244

FIG. 7


116
AP
201
WLAN
BSS
P2P Device
WLAN-STA
904
902
P2P
Group
P2P Device
195

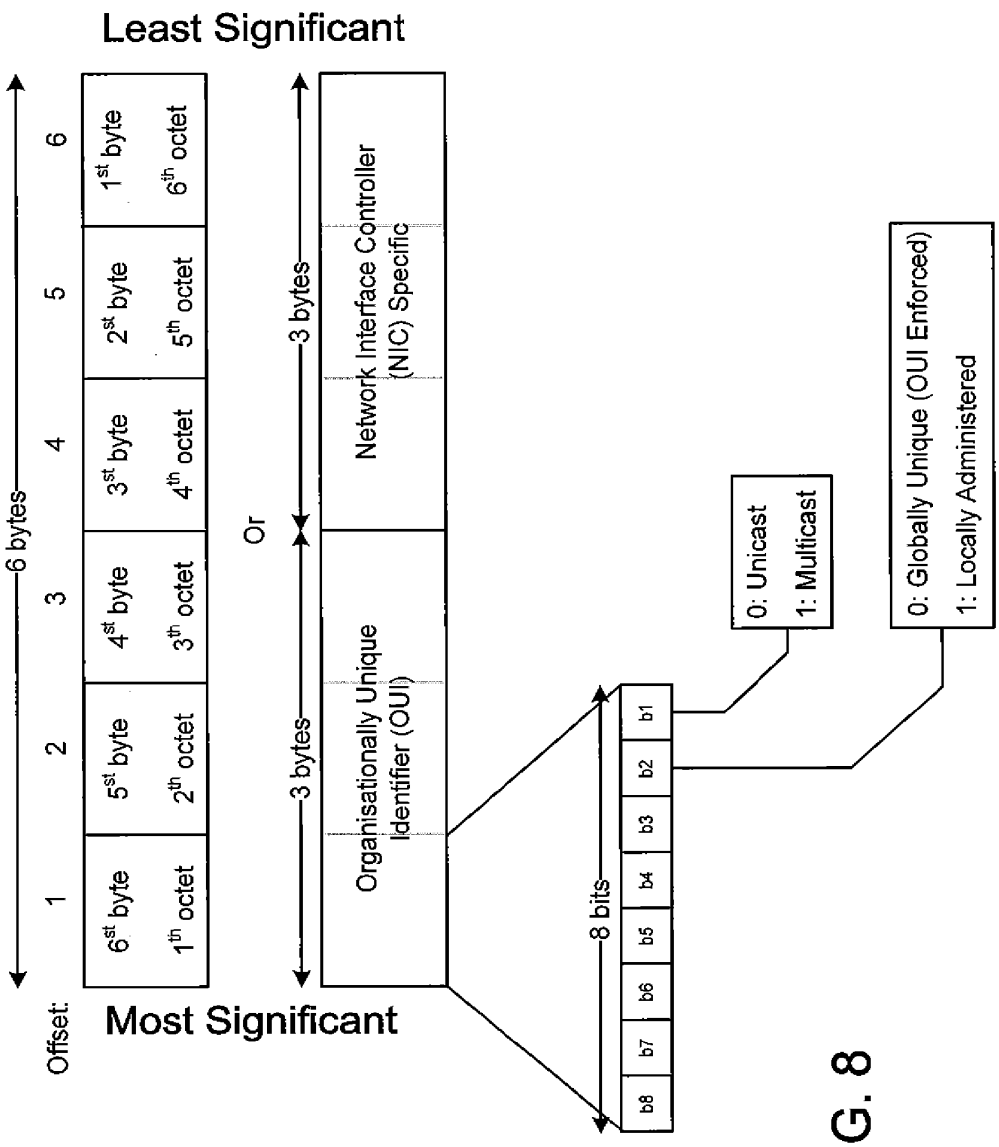

Least Significant
Most Significant
Offset:
1
2
3
4
5
6
6 bytes
6st byte
1th octet
5st byte
2th octet
4st byte
3th octet
3st byte
4th octet
2st byte
5th octet
1st byte
6th octet
Or
3 bytes
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b1
b2
b3
b4
b5
b6
b7
b8
0: Unicast
1: Multicast
0: Globally Unique (OUI Enforced)
1: Locally Administered
800

FIG. 8

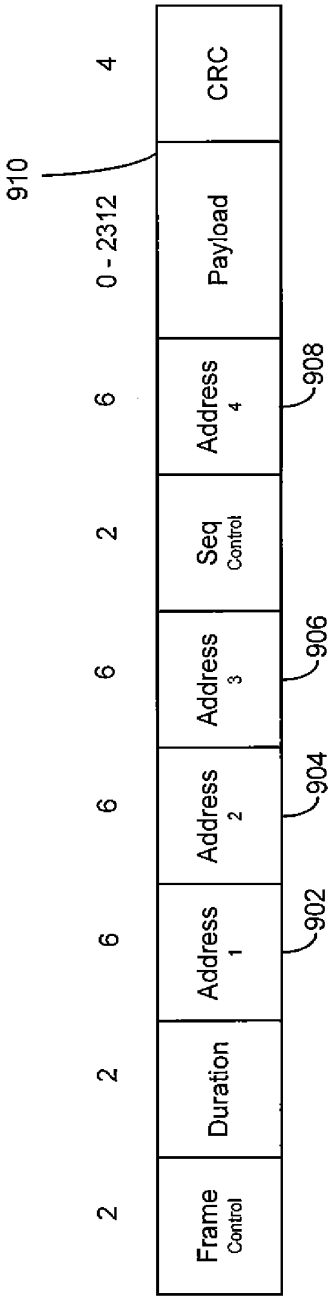

Frame Control
2
Duration
2
Address 1
6
902
Address 2
6
904
Address 3
6
906
Seq Control
2
Address 4
6
908
Payload
0 - 2312
910
CRC
4
900

FIG. 9

FIG. 10

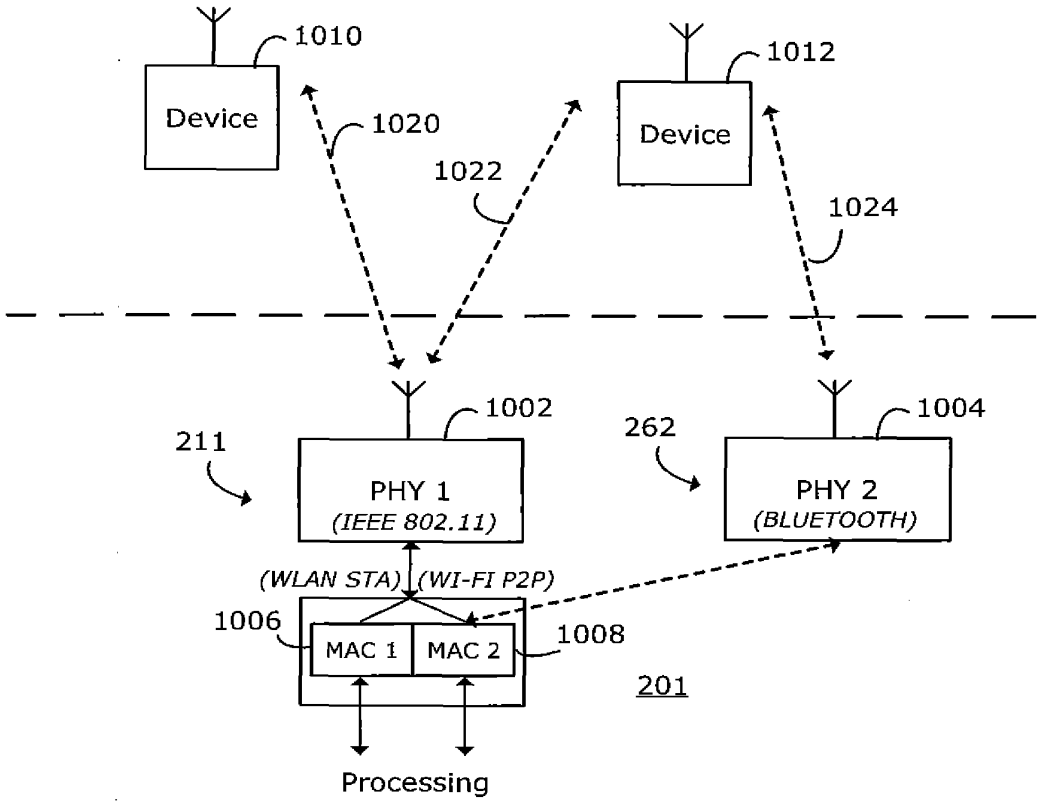

1010
Device
1020
1022
1012
Device
1024
1002
211
PHY 1
(IEEE 802.11)
1004
262
PHY 2
(BLUETOOTH)
(WLAN STA)
(WI-FI P2P)
1006
MAC 1
MAC 2
1008
201
Processing

FIG. 11

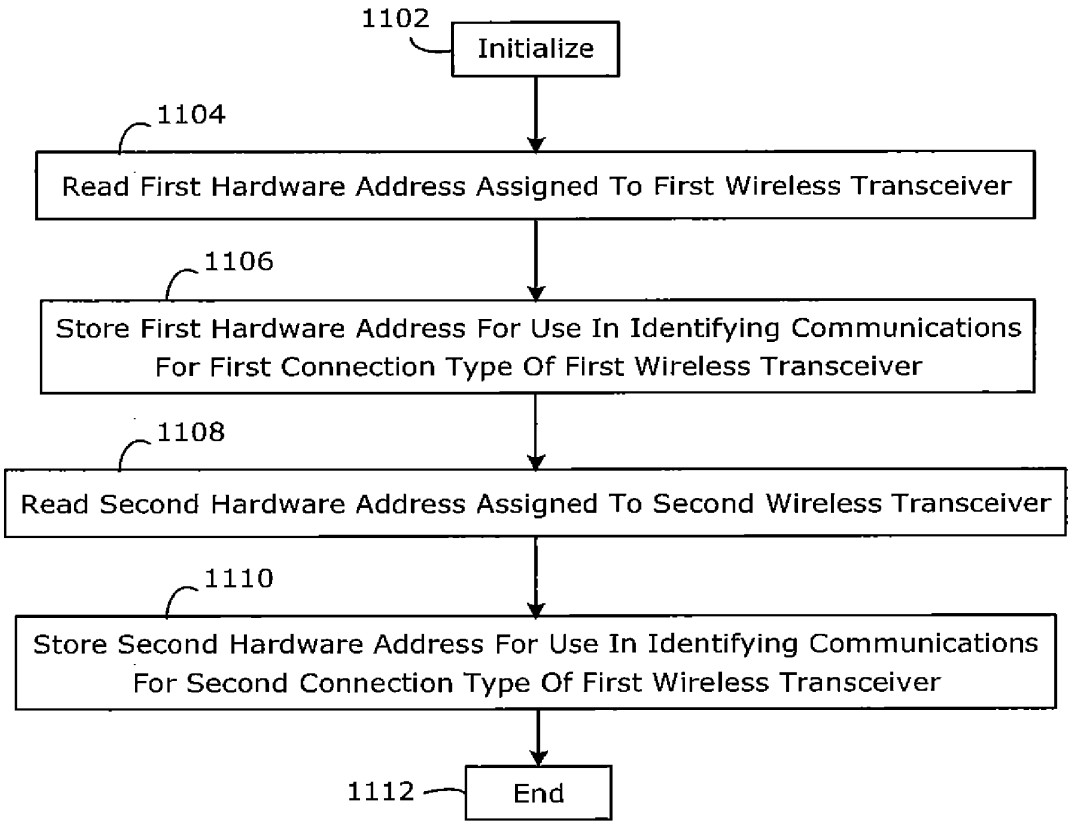
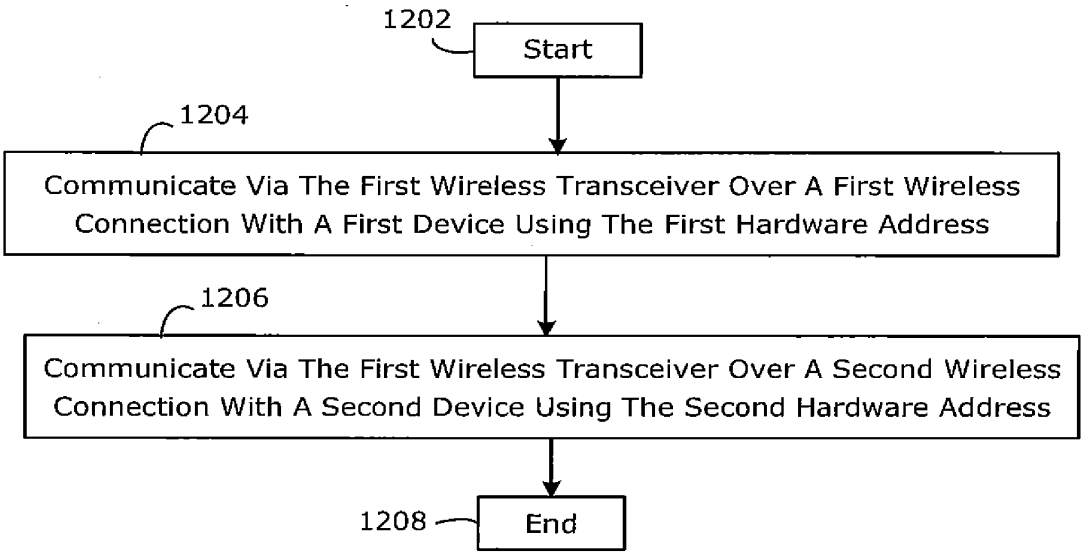

1102
Initialize
1104
Read First Hardware Address Assigned To First Wireless Transceiver
1106
Store First Hardware Address For Use In Identifying Communications For First Connection Type Of First Wireless Transceiver
1108
Read Second Hardware Address Assigned To Second Wireless Transceiver
1110
Store Second Hardware Address For Use In Identifying Communications For Second Connection Type Of First Wireless Transceiver
1112
End

FIG. 12


1202
Start
1204
Communicate Via The First Wireless Transceiver Over A First Wireless Connection With A First Device Using The First Hardware Address
1206
Communicate Via The First Wireless Transceiver Over A Second Wireless Connection With A Second Device Using The Second Hardware Address
1208
End

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2007110473 A **[0005]**
- US 20080013539 A **[0006]**

Samsung Ex. 1004, Page 446 of 563

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-10034147 B2	07-24-2018	Shelby et al.	
	2	US-10044613 B2	08-07-2018	Kazmi et al.	
	3	US-10912083 B2	02-02-2021	Amini et al.	
	4	US-11,115,834 B2	09-07-2021	Manapragada	
	5	US-11115834 B2	09-07-2021	Manapragada	
	6	US-11429407 B2	08-30-2022	Smith et al.	
	7	US-20020152305 A1	10-17-2002	Jackson et al.	
	8	US-20040053602 A1	03-18-2004	Wurzburg	
	9	US-20050089064 A1	04-28-2005	Zimmerman et al.	
	10	US-20050195821 A1	09-08-2005	YUN et al.	
	11	US-2006/0140123 A1	06-29-2006	Conner et al.	
	12	US-20060114851 A1	06-01-2006	Gupta et al.	
	13	US-20060140123 A1	06-29-2006	Conner et al.	
	14	US-2007/0242695 A1	10-18-2007	Xu	
	15	US-20070110198 A1	05-17-2007	Skarby et al.	
	16	US-20070121573 A1	05-31-2007	Zuckerman et al.	
	17	US-20070180119 A1	08-02-2007	Khivesara et al.	
	18	US-20070242695 A1	10-18-2007	Xu	
	19	US-20070270121 A1	11-22-2007	Shao et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
	20	EP 1878169 B1	01-16-2008	Rune		
	21	KR 20070061684A	06-14-2007	Jeonghoon Oh		✓
	22	WO 2014020407 A1	02-06-2014	Huang et al.		
	23	EP 2016750 B1	01-21-2009	Lee et al.		
	24	EP 2055072 B1	05-06-2009	Falk et al.		✓
	25	GB 2516132A	01-14-2015	Stephens et al.		

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	26	US-2008/0002631 A1	01-03-2008	Ramachandran	
	27	US-2008/0084855 A1	04-10-2008	Rahman	
	28	US-20080002631 A1	01-03-2008	Ramachandran	
	29	US-20080084855 A1	04-10-2008	Rahman	
	30	US-20090034460 A1	02-05-2009	Moratt et al.	
	31	US-20090074051 A1	03-19-2009	Manapragada et al.	
	32	US-20090141691 A1	06-04-2009	Jain	
	33	US-20090180451 A1	07-16-2009	Alpert et al.	
	34	US-20090290524 A1	11-26-2009	Seok	
	35	US-2010/0128630 A1	05-27-2010	Barak et al.	
	36	US-20100128630 A1	05-27-2010	Barak et al.	
	37	US-2011/0110289 A1	05-12-2011	Venkatachalam et al.	
	38	US-2011/0128919 A1	06-02-2011	Kim et al.	
	39	US-2011/0211541 A1	09-01-2011	Yuk et al.	
	40	US-20110110289 A1	05-12-2011	Venkatachalam et al.	
	41	US-20110128919 A1	06-02-2011	KIM et al.	
	42	US-20110211541 A1	09-01-2011	Yuk et al.	
	43	US-20110286404 A1	11-24-2011	Abraham et al.	
	44	US-20120113320 A1	05-10-2012	PLATZER	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
	45	EP 2555578A1	02-06-2013	Deb et al.		
	46	EP 2713670 A1	04-02-2014	Smadi		
	47	EP 3174323 B1	11-14-2018	Montemurro		
	48	EP 3220697 B1	06-06-2018	Kiukkonen		
	49	TW I500350B	04-16-2015	Yen et al.		✓

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	50	US-2013/0281049 A1	10-24-2013	Lee et al.	
	51	US-20130028150 A1	01-31-2013	Ma et al.	
	52	US-20130196653 A1	08-01-2013	Morrison	
	53	US-20130201847 A1	08-08-2013	Chincholi et al.	
	54	US-20130258921 A1	10-03-2013	Gevorkov et al.	
	55	US-20130281049 A1	10-24-2013	Lee et al.	
	56	US-2014/0056209 A1	02-27-2014	Park et al.	
	57	US-2014/0075189 A1	03-13-2014	Abraham et al.	
	58	US-2014/0269610 A1	09-18-2014	Hiben et al.	
	59	US-20140003449 A1	01-02-2014	Li	
	60	US-20140056209 A1	02-27-2014	Park et al.	
	61	US-20140075189 A1	03-13-2014	Abraham et al.	
	62	US-20140075523 A1	03-13-2014	TUOMAALA et al.	
	63	US-20140213219 A1	07-31-2014	MOHEBBI	
	64	US-20140269505 A1	09-18-2014	Medard et al.	
	65	US-20140269560 A1	09-18-2014	Jain et al.	
	66	US-20140269610 A1	09-18-2014	HIBEN et al.	
	67	US-20140321282 A1	10-30-2014	Pragada et al.	
	68	US-2015/0023245 A1	01-22-2015	Du et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	69	US-2015/0098359 A1	04-09-2015	Yen et al.	
	70	US-2015/0110036 A1	04-23-2015	Zhang et al.	
	71	US-20150023245 A1	01-22-2015	Du et al.	
	72	US-20150098359 A1	04-09-2015	YEN et al.	
	73	US-20150110036 A1	04-23-2015	Zhang et al.	
	74	US-20150181486 A1	06-25-2015	Vallabhu et al.	
	75	US-20150237667 A1	08-20-2015	GHAI et al.	
	76	US-20160014127 A1	01-14-2016	Mohebbi	
	77	US-5073899	12-17-1991	Collier et al.	
	78	US-5818830	10-06-1998	Daane et al.	
	79	US-7373443 B2	05-13-2008	Seto	
	80	US-7664072 B1	02-16-2010	Ho et al.	
	81	US-7784076 B2	08-24-2010	Demircin et al.	
	82	US-7797723 B2	09-14-2010	Demircin et al.	
	83	US-8175539 B2	05-08-2012	Diener et al.	
	84	US-8279876 B2	10-02-2012	Chang et al.	
	85	US-8363597 B2	01-29-2013	Abraham et al.	
	86	US-8411608 B2	04-02-2013	Chandra et al.	
	87	US-8565178 B2	10-22-2013	Cheng et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	88	US-8718558 B2	05-06-2014	Montemurro	
	89	US-8767726 B2	07-01-2014	Petry et al.	
	90	US-8818276 B2	08-26-2014	Kiukkonen et al.	
	91	US-8837454 B2	09-16-2014	Hegde	
	92	US-8923816 B2	12-30-2014	Lee et al.	
	93	US-8982762 B2	03-17-2015	Smadi et al.	
	94	US-8989101 B1	03-24-2015	Mishra	
	95	US-9160396 B2	10-13-2015	Soltanian et al.	
	96	US-9198184 B2	11-24-2015	Yeh et al.	
	97	US-9241370 B2	01-19-2016	Amini et al.	
	98	US-9258712 B2	02-09-2016	Kiukkonen et al.	
	99	US-9294926 B2	03-22-2016	Pragada et al.	
	100	US-9408254 B2	08-02-2016	Jain	
	101	US-9467379 B2	10-11-2016	Merlin et al.	
	102	US-9516540 B2	12-06-2016	Emmanuel et al.	
	103	US-9526022 B2	12-20-2016	Gupta	
	104	US-9560656 B2	01-31-2017	Damnjanovic et al.	
	105	US-9560661 B2	01-31-2017	Elhaddad et al.	
	106	US-9603192 B2	03-21-2017	Mohebbi	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

U.S. PATENT DOCUMENTS

Examiner initial *	Cite No.	Document Number Number - Kind Code [2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
	107	US-9706383 B2	07-11-2017	Kiukkonen et al.	
	108	US-9736714 B2	08-15-2017	Zhao et al.	
	109	US-9743345 B2	08-22-2017	Yen et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country [3] Code Number [4] Kind Code (if known) [5]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not Considered. Include copy of this form with next communication to applicant. 1. Applicant's unique citation design number (optional). 2 See Kinds Codes of USPTO patent Documents. at www.uspto.gov or MPEP 901.04. 3. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4. For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 6. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	110	Choi et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part I". IEEE 11-14/0804r1. [PowerPoint presentation].	
	111	Choi et al. (November 11, 2013) "Discussion on OFDMA in HEW". LG Electronics. [PowerPoint presentation].	
	112	English Abstract of TWI500350B obtained from Espacenet.net on July 7, 2023.	
	113	English Translation of EP2055072B1 obtained from Google Patents on September 1, 2023.	
	114	English Translation of KR20070061684A obtained from Google Patents on January 9, 2024.	
	115	Gong, D.; Yang, Y; and Li, H. "An Efficient Cooperative Retransmission MAC Protocol for IEEE 802.11n Wireless LANs" in: IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, 2013. pp. 191-199.	
	116	Hiertz et al. (November 12, 2013) "Proposed direction and priorities for HEW". IEEE 11-13-1331-01. [PowerPoint presentation].	
	117	Huang et al. (September 16, 2013) "DL-MU-MIMO Transmission with Unequal Bandwidth". IEEE 802.11-13/1154r1. [PowerPoint presentation].	
	118	IEEE std 802.11ac(tm)-2013. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancemenets for Very High Throughput for Operation in Bands below 6 GHz. IEEE Computer Society. (2013).	
	119	Inoue et al. (March 19, 2013) "Beyond 802.11ac – A Very High Capacity WLAN". IEEE 11-13/0287r3. [PowerPoint presentation].	

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	120	Kakumanu, S. and Sivakumar, R. "Glia: A Practical Solution for Effective High Datarate Wifi-Arrays". MobiCom '09, September 20-25, 2009.	
	121	Kim et al. (September 16, 2013) "Multicast Transmission for HEW". IEEE 802.11-13/1061r0. [PowerPoint presentation].	
	122	Koskela et al. (July 15, 2013) "Discussion on Potential Techniques for HEW". IEEE 802.11-13/0871r0. [PowerPoint presentation].	
	123	Li, H. and Xie, J. "A Channel Splitting Strategy for Reducing Handoff Delay in Internet-Based Wireless Mesh Networks" in: IEEE Transactions on Vehicular Techonolgy, (July 2012), vol 61, no. 6. pp. 2740-2752.	
	124	Lim et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part II". IEEE 11-14/0801r0. [PowerPoint presentation].	
	125	Liu et al. (May 9, 2013) "Discussions on 11ac PHY Efficiency". IEEE 802.11-13/0544r3. [PowerPoint presentation].	
	126	Prasad, S.S; Shukla, C.K.; and Chisab, R.F. "Performance Analysis of OFDMA in LTE" in: IEEE (July 26-28, 2012).	
	127	Raman, V. and Vaidya, N.H. "WiSP: A Protocol for Overcoming MAC Overheads Using Packet Size Dependent Channel Widths" in: 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2011. pp. 28-36.	
	128	Selvakumar, V.; Nemalladinne, S.S.; and Arumugam, P. "Analysis of LTE Radio Frame by eliminating Cyclic Prefix in OFDM and comparison of QAM and Offset-QAM". Degree project. Linnaeus University, September 10, 2012.	
	129	U.S. Provisional Patent Application No. 61/835,488, entitled "WLAN SENSOR GATEWAY WITH COEXISTENCE SOLUTION", filed Jun. 14, 2013	

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	9	of	9

Complete if Known	
Application Number	New Application
Filing Date	March 04, 2024
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000010

NON PATENT LITERATURE DOCUMENTS

Examiner initial *	Cite No. [1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	130	U.S. Provisional Patent Application No. 61/836,571, entitled "COEXISTENCE AND TRAFFIC MANAGEMENT FOR USING MULTIPLE WLAN RADIOS IN A SYSTEM", filed Jun. 18, 2013	
	131	U.S. Provisional Patent Application No. 61/870,762, entitled "COEXISTENCE AND TRAFFIC MANAGEMENT WITH ALIGNMENT OF PACKETS AND CHANNEL STEERING", filed Aug. 27, 2013	
	132	U.S. Provisional Patent Application No. 61/888,692, entitled "WIRELESS DESIGN FOR USING A ROUTERS OR RESIDENTIAL GATEWAY AS SENSOR GATEWAY", filed Oct. 9, 2013	
	133	U.S. Provisional Patent Application No. 61/890,713 entitled "SIMULTANEOUS USAGE OF DIFFERENT WLAN MODULES", filed Oct. 14, 2013	
	134	U.S. Provisional Patent Application Ser. No. 61/824,338 entitled "ADVANCED WIRELESS COMMUNICATION SYSTEMS AND TECHNIQUES", filed May 16, 2013	
	135	Wee et al. "Discretionary bandwidth granting scheme for homogenous real-time applications". EURASIP Journal on Wireless Communications and Networking (2013). http://jwcn.eurasipjournals.com/content/203/1/135	
	136	Yang et al. (September 18, 2013) "Discussion on Access Mechanism for HEW". IEEE 11-13/1105r0. [PowerPoint presentation].	

Examiner Signature		Date Considered	

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1. Applicants unique citation designation number. (optional) 2. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Cheif Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450 Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assisstance in completing the form, call 1-800-PTO-9199 and select option 2.

APPLICATION DATA SHEET

APPLICATION INFORMATION

Application number::	
Filing Date::	
Application Type::	Non-Provisional
Subject Matter::	Utility
Suggested classification::	
Suggested Group Art Unit::	
CD-ROM or CD-R?::	
Number of CD disks::	
Number of copies of CDs::	
Sequence submission?::	
Computer Readable Form (CRF)?::	
Number of copies of CRF::	
Title::	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS
Attorney Docket Number::	020505-000010
Request For Early Publication?::	
Request for Non-Publication?::	
Suggested Drawing Figure::	1
Total Drawing Sheets::	11
Small Entity?::	Yes
Licensed US Govt. Agency::	No
Contract or Grant Numbers::	
Secrecy Order in Parent Appl.?::	

INVENTOR INFORMATION

Given Name::	Sai
Middle Name::	C.
Family Name::	Manapragada

APPLICATION DATA SHEET

Name Suffix::	
City of Residence::	Cypress
State or Province of Residence::	TX
Country of Residence::	United States
Street of mailing address::	21214 Chelton Beach Drive
City of mailing address::	Cypress
State or Province of mailing address::	TX
Country of mailing address::	United States
Postal or Zip Code of mailing address::	77433

CORRESPONDENCE INFORMATION

Correspondence Customer Number::	30565
Phone number::	317-634-3456
Fax Number::	317-637-7561

REPRESENTATIVE INFORMATION

Representative Customer Number::	30565

DOMESTIC PRIORITY INFORMATION

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	18/532,175	2023-12-07
18/532,175	Continuation of	18/448,281	2023-08-11
18/448,281	Continuation of	17/468,509	2021-09-07
17/468,509	Continuation of	16/039,660	2018-07-19
16/039,660	Continuation of	14/526,799	2014-10-29
14/526,799	Claims the benefit of	61/897,219	2013-10-30
14/526,799	Claims the benefit of	61/897,216	2013-10-30

FOREIGN PRIORITY INFORMATION

Country::	Application Number::	Filing Date::	Priority Claimed::	Access Code::

APPLICATION DATA SHEET

STATEMENT UNDER 37 CFR 1.55 OR 1.78 FOR AIA (FIRST INVENTOR TO FILE) TRANSITION APPLICATIONS

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

AUTHORIZATION OR OPT-OUT OF AUTHORIZATION TO PERMIT ACCESS

When this Application Data Sheet is properly signed and filed with the application, Applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, application **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) – Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO – Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

APPLICATION DATA SHEET

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of the search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information and identified in subsection 1A above.

☐ B. Applicant **does not** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

APPLICANT INFORMATION

Applicant name::	XiFi Networks R&D Inc.
Street of mailing address::	21214 Chelton Beach Drive
City of mailing address::	Cypress
State or Province of mailing address::	TX
Country of mailing address::	United States
Postal or Zip Code of mailing address::	77433

SIGNATURE

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Respectfully submitted,

By /Blake R. Hartz, Reg. No. 73453/
Blake R. Hartz, Reg. No. 73453
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700, Indianapolis, Indiana 46204-5137
Telephone (317) 634-3456 Fax (317) 637-7561 Email: bhartz@uspatent.com

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 555 578 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.02.2013 Bulletin 2013/06

(51) Int Cl.:
H04W 74/08 *(2009.01)*

(21) Application number: **11306013.1**

(22) Date of filing: **04.08.2011**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **Alcatel Lucent**
75007 Paris (FR)

(72) Inventors:
- **Deb, Supratim**
  560045 BANGALORE (IN)
- **Chatterjee, Avhishek**
  560045 BANGALORE (IN)
- **C n, Kanthi**
  560045 BANGALORE (IN)
- **Srinivasan, Vikram**
  560045 BANGALORE (IN)

(74) Representative: **Benezeth, Philippe J.L. M. et al**
Feray Lenne Conseil
Le Centralis
63 Avenue du Général Leclerc
92340 Bourg La Reine (FR)

(54) Wireless networks over frequency agil radio systems

(57) Exemplary embodiments relate to a node, and related network, having at least one frequency agile data radio system(s), called data radio system(s). Said node also comprises at least one control radio system. Said node comprises control means including dividing means, for dividing a set of generalized links in at least high priority generalized links and low priority generalized links, and prioritized CSMA based MAC scheduling protocol module configured for making said generalized links contend for a channel corresponding to their frequency band by executing said CSMA based MAC scheduling protocol so that an high priority generalized link loses channel access trough a contention resolution only to another high priority generalized link. Exemplary embodiments also relate to a corresponding method for communicating data.

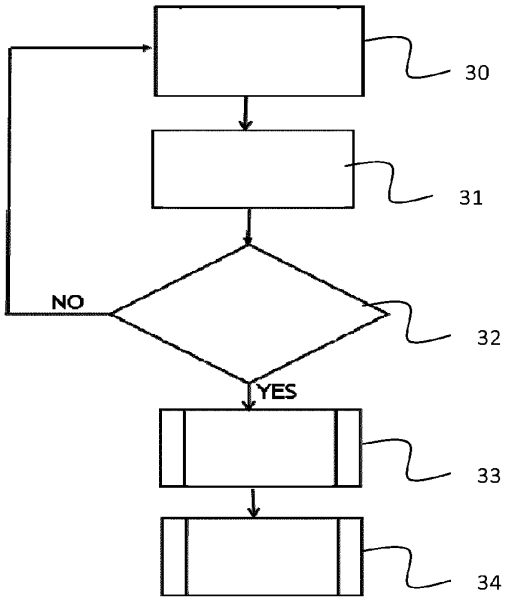


FIG.3

EP 2 555 578 A1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] Embodiments disclosed herein relate generally to wireless nodes and related wireless telecommunications networks.

BACKGROUND

[0002] With the proliferation of diverse frequency bands, there is tremendous interest of frequency-agile wireless nodes and networks. "Frequency-agile" means that the transmitter and the receiver of a radio system of a node have the ability to tune across large swathes of spectrum.

[0003] Recent advances in radio technology make it possible for radio systems to tune their center frequencies across large swathes of spectrum, for example from 100 MHz to 8 GHz.

[0004] These radio systems can not only tune their center frequency, but also adapt the operating bandwidth. However, while it is possible for a radio system to tune to a wide swathe of spectrum, the bandwidth over which it can operate is limited. Typically, when a radio system is tuned to a given center frequency, the operating bandwidth associated with said center frequency is limited to 40 MHz about, what limits the exploitation of the diverse spectrum available.

[0005] Different frequency bands have different propagation properties. The lower frequency bands propagate a lot farther than the higher frequency bands. This implies that lower frequency bands provide better data rates at a fixed distance. It also implies that the lower frequency bands create higher interference to neighboring links.

[0006] For example, considering a 6 MHz of spectrum available from 100-106 MHz and another 6 MHz of spectrum available from 500-506 MHz. Wireless signals incur much less path loss over a lower frequency band and thus propagates further. Hence, frequency band 100-106 MHz will result in a higher data rate compared to frequency band 500-506 MHz, provided the ambient interference experienced in both the bands is around the same level.

[0007] IEEE 802.11a/b/g/n standard, called IEEE 802.11 standard, proposes CSMA based MAC protocol for wireless networks. But IEEE 802.11 standard does not account for specific spectrum characteristics. IEEE 802.11 standard assumes that spectrum is homogeneous.

[0008] Q-CSMA is an evolution of IEEE 802.11 standard that still has the drawbacks of being non adapted for tacking account of specific spectrum characteristics. Also, it has the additional drawback that it requires mesh nodes to be time synchronous. A detailed explanation of what is Q-CSMAis accessible in the publication referenced "Q-CSMA J. Ni, B. Tan, and R. Srikant. Q-CSMA: Queue length based csma/ca algorithms for achieving maximum throughput and low delay in wireless networks. In IEEE Infocom Mini-Conference, 2010".

[0009] There is thus a need to propose a multiband network which enables to determine, at each instant, which set of communicating node pairs should operate over which frequency band to transmit data with improved reliability and efficiency. There is also a need to propose a multiband network with wireless nodes which better exploits the diverse spectrum available.

SUMMARY

[0010] Example embodiments provide wireless nodes and related wireless networks adapted to transmit data with improved reliability and efficiency.

[0011] An aspect of the invention relates to a node for a wireless network, said node having at least one, preferably two, frequency agile transmitter/receiver radio system(s), called data radio system(s), allowing said node to communicate with at least another node of said wireless network over different selectable frequency bands. Said node and said other node which are able to communicate over different selected frequency bands form a generalized links, a general link being defined as a link formed by a frequency agile transmitter radio system of a node, called transmitter node, and a frequency agile receiver radio system of another node, called receiver node, and a frequency band over which said link is able to communicate. Said node also comprises at least one control radio system for exchanging control messages with said at least another node of said wireless network over a control frequency band different from the frequency band used by said at least one data radio system. Said node comprises control means for executing a medium access control, called MAC, scheduling protocol based on a Carrier Sense Multiple Access, called CSMA, protocol to control communication between said node and said other node of said wireless network. Said control means comprise dividing means, for dividing a set of generalized links in at least high priority generalized links, called HP generalized link, and low priority generalized links, called LP generalized link. Said node comprises prioritized CSMA based MAC scheduling protocol module configured for making said generalized links contend for a channel corresponding to their frequency band by executing said CSMA based MAC scheduling protocol so that an HP generalized link loses channel access trough a contention resolution only to another HP generalized link.

[0012] Thus a higher priority generalized link is never beaten by a lower priority generalized link.

[0013] In various embodiments, said dividing means are also configured for dividing said set of generalized links in said HP generalized links and LP generalized links, and also in medium priority generalized links, called MP generalized links, and prioritized CSMA based MAC scheduling protocol module is also configured to ensure that a MP generalized link loses channel access trough

Samsung Ex. 1004, Page 461 of 563

a contention resolution only to an HP generalized link or to another MP generalized link.

[0014] According to another aspect, control means also comprise priority assigning means configured for assigning priorities to said generalized links in function of the physical-layer data rate of the frequency band associated with said generalized link.

[0015] In various embodiments, priority assigning means are configured to set a generalized link as a HP generalized link when gain of this generalized link is maximal compared to the gain of others generalized links.

[0016] According to a further aspect, priority assigning means are configured to choose a random frequency band from time to time and to determine the identity of the generalized link which has maximum gain over said chosen frequency band, said determined maximal gain generalized link being set as a HP generalized link.

[0017] According to some embodiments, said node is also configured to broadcast over the control channel the identity of the chosen frequency band, the identity of the determined maximal-gain generalized link, and, if any, the generalized link which has to be deactivated for allowing said maximal-gain generalized link to be active over the chosen frequency band.

[0018] According to another aspect, said gain of a generalized link is the gain in weight that the link of said generalized link operating in a particular frequency band can have by switching to a new frequency band corresponding to the frequency band of said generalized link.

[0019] According to a further aspect, the weight of a generalized link is defined by the multiplication of the queue-length of the transmitter node of the generalized link and the physical-layer data rate of the generalized link in the frequency band of said generalized link, said queue-length corresponding to the number of packets awaiting for transmission by the transmitter node of the corresponding generalized link.

[0020] In various embodiments, priority assigning means are configured to compute gain, noted gain(1), of a generalized link noted 1, whose transmitter node, noted v, is able to activate said generalized link 1 over a frequency band noted fj, as follows :

gain (1) over frequency band fj = weight of generalized link 1 over fj - loss(v)

wherein loss(v) is a loss value of the transmitter node v which is computed as follows:

Case-1: if there exists some other active generalized link denoted l' for which v is also a transmitter node over frequency band fj, then loss(v) is set equal to the weight of generalized link l' over said frequency band fj ;

Case-2: if condition of Case-1 does not hold and if there is a spare transmitter radio system at node v, then loss(v) is set equal to 0 ;

Case-3: if the conditions of Case-1 and Case-2 do not hold, then loss(v) is set to the minimum weight of all active generalized links over all frequency bands for which v is the transmitter node.

[0021] According to another aspect, said node comprises means for determining the queue length of a generalized link from information embedded in Request to Send / Clear to Send messages, called RTS/ CTS messages, sent by the node pair of said generalized link on the control channel trough the control radio systems of the node pair.

[0022] According to another aspect, priority assigning means are configured to, whenever Request to Send / Clear to Send messages, called RTS/ CTS messages, transmitted over a generalized link, are overheard on the control channel by said node, update the set of active generalized links.

[0023] According to a further aspect, said node comprises list maintaining means configured to maintain three lists of generalized links, namely HP list containing HP generalized links, MP list containing MP generalized links and LP list containing LP generalized links.

[0024] In various embodiments, said list maintaining means are configured to, when said node hears a broadcast from another node of the network indicating that said node is either the transmitter node or the receiver node of a HP generalized link, add said generalized link to the HP list.

[0025] In other embodiments, wherein said list maintaining means are configured to remove a HP generalized link from the HP list once said HP generalized link gets activated for the first time.

[0026] According to another aspect, said list maintaining means are configured so that any generalized link that gets removed from the HP list is added to the MP list of the same node, a generalized link in the MP list being removed only when it loses contention of the channel over the frequency band corresponding to said generalized link.

[0027] According to a further aspect, said list maintaining means are configured so that each generalized link that is not a part of the HP list or the MP list belongs to the LP list.

[0028] In various embodiments, said prioritized CSMA based MAC scheduling protocol module is configured to, whenever said or one of said data radio system(s) of said node becomes free, performing the steps of :

- visiting the lists in order of priority and pick the first inactive generalized link that has non-zero queue length ;
- making said data radio system switch to the selected generalized link's frequency band and assess if the channel is free ;
- if said channel is free, transmitting an RTS message over the control channel at a time slot selected uniformly:

Samsung Ex. 1004, Page 462 of 563

between [0 ; CW/2 - 1] if said generalized link that has been picked is an HP generalized link,
between [CW/2; 3CW/4 - 1] if said generalized link that has been picked is an MP generalized link,
and between [3CW/4;CW - 1] if said generalized link that has been picked is an LP generalized link,
CW being a predetermined size of a contention window;
said RTS message containing the following information :

(i) the identity of the receiver node of the picked generalized link and the corresponding frequency band, and
(ii) queue length of said picked generalized link.

[0029] According to a another aspect, said prioritized CSMA based MAC scheduling protocol module is also configured to command transmission over:

- a HP generalized link during a constant time interval, noted TXOPT, if contention has been won by said HP generalized link,
- over a MP generalized link, respectively a LP generalized link, during one packet duration if contention has been won by said MP generalized link, respectively said LP generalized link.

[0030] In various embodiments, said constant duration TXOPT is chosen so that multiple packets can be transmitted, typically a few milliseconds.

[0031] MAC scheduling issue in such node(s) and related networks is to determine, at each instant, which set of communicating node-pairs should operate over which frequency band and, preferably, over which data radio system. The proposed node and related network solve this issue by using a specific CSMA based MAC scheduling protocol which takes account of priorities assigned to generalized links. Said priorities are assigned to generalized links in function of frequency bands related to said generalized links what enables said node and related network to transmit data with improved reliability and efficiency and with better exploitation of the diverse spectrum available.

[0032] In various embodiments, said CSMA is a carrier senses multiple access protocol with collision avoidance (CSMA\CA).

[0033] According to various embodiments, wireless nodes and related networks are equipped with multiple frequency agile data radio systems and the nodes are not necessarily synchronized. CSMA based MAC scheduling protocol is adapted to determine which node should transmit to which node at which time over which frequency band and over which data radio system.

[0034] In some embodiments, the CSMA based MAC scheduling protocol is distributed and does not require synchrony among network nodes. According to a further aspect, the CSMA based MAC scheduling protocol incurs low overhead and is easy to implement. According to a further aspect, the CSMA based MAC scheduling protocol achieves high throughput and low network delay, and is robust against packet losses.

[0035] High-throughput means that the CSMA based MAC scheduling protocol is either throughput-optimal or achieve a constant fraction of the throughput-optimal region. The throughput-optimal region for a wireless network is the set of all arrival rates for which queue sizes or lengths remain bounded.

[0036] The CSMA based MAC scheduling protocol accounts for diverse spectrum characteristics, in particular for diverse propagation characteristics of the different frequency bands, and client locations.

[0037] In particular said CSMA based MAC scheduling protocol accounts for diverse frequency bands in three ways. Firstly, said protocol or algorithm has notion of weight that depends on the physical layer data rate of the operating frequency band. The weights capture the relative values of the frequency bands. Secondly, in various embodiments, the channel sensing for the protocol is performed over the actual frequency band and not based on RTS/CTS over control channel, what makes sure that the interference neighborhood is frequency band dependent. Finally, priorities are assigned to generalized links that depend on gain in switching to a particular band. Said protocol can be viewed as prioritized CSMA based MAC protocol. Roughly, in various embodiments, higher priority is assigned to nodes to large queue-lengths corresponding to the number of packets waiting for transmission in a MAC buffer of a transmitter node.

[0038] In various embodiments, said prioritized CSMA based MAC scheduling protocol provides very low network delay with a small sacrifice in throughput. Thus it is suited for video based and real-time applications that will be dominant in the near future.

[0039] According to another aspect, it is provided a wireless network including nodes as proposed above.

[0040] According to a further aspect, it is provided a method for communicating data through a wireless network as proposed above.

[0041] Various combinations and subset of the above aspects are provided.

BRIEF DESCRIPTION OF THE DRAWINGS

[0042] In order to better understand various exemplary embodiments, reference is made to the accompanying drawings, wherein:

[0043] FIG. 1 is a schematic architecture of the upper MAC and the lower MAC layers of a node ;

[0044] FIG.2 is a schematic topology of nodes in a wireless network according to an example embodiment ;

[0045] FIG.3 is a flowchart of a method carried out by

Samsung Ex. 1004, Page 463 of 563

a leader node to inform follower nodes about the identity of high priority generalized links.

DETAILED DESCRIPTION

[0046] Referring now to the drawings, there are disclosed broad aspects of various exemplary embodiments.

[0047] A brief explanation of what is CSMA and CSMA/CA is described below. Carrier sense multiple access CSMA, in computer networking, is a wireless network multiple access method in which a carrier sensing scheme is used. A node wishing to transmit data has to first listen to the channel for a predetermined amount of time to determine whether or not another node is transmitting on the channel within the wireless range. If the channel is sensed "idle," then the node is permitted to begin the transmission process. If the channel is sensed as "busy," the node defers its transmission for a random period of time.

[0048] Carrier sense multiple access with collision avoidance (CSMA/CA), is a modification of carrier sense multiple access CSMA. Collision avoidance is used to improve the performance of CSMA by attempting to divide the wireless channel equally among all transmitting nodes within the collision domain.

Network Model

[0049] According to an exemplary embodiment, a wireless network is considered with V as the set of nodes. In various embodiments, each node comprises at least two frequency agile data radio systems, called data radio systems. Thus data radio system resources available are multiple frequency bands with diverse propagation characteristics. Frequency band is meant a contiguous slice of spectrum of width at most Bmax, the maximum tunable range of a radio system. If there is a larger contiguous band available denoted W, than W is split into bands of equal width denoted Bmax, with the last band having width possibly less than Bmax. Since the frequency bands have diverse propagation characteristics, the data rate between a transmitter-receiver node pair in the network and the interfering neighbors of the transmitter-receiver node pair, are frequency dependent.

[0050] For instance, if Bmax = 40 MHz, each data radio system of a node of the related network is considered to be able to tune up to 40 MHz. Considering that in a location, there is whitespace spectrum available from 512 MHz-602MHz of width Wavailable =90 MHz. This band is split as multiple bands of width at most Bmax as follows: 512-552 MHz, 552-592 MHz, 592-602 MHz.

[0051] According to various embodiments, each data radio system of each network node is a half-duplex frequency data radio system capable of tuning across a large frequency range, for example from 100 MHz to 2.5 GHz. An half-duplex radio is a radio that can either transmit radio signals or receive radio signals at any time but cannot do both simultaneously. In various embodiments, said nodes are mesh nodes.

[0052] In some embodiments, the different nodes may have different number of data radio systems. For ease of exposition, in the embodiments described hereafter, the different nodes have equal number of data radio systems with each node. It is assumed that at any given time any data radio system can tune to only a single frequency band, e.g. 500MHz, 2.4GHz etc., and the bandwidth can range from 0 to Bmax.

Network and generalized links

[0053] It is assumed that the spectrum available over the network is fragmented and spans a large range, e.g., 50-700MHz, 2.4GHz and 5.2GHz. It is assumed that the frequency bands are ordered in the real axis from left to right, and in the description it will be simply used band fj ; j = 1; 2; ... ; M to mean the jth frequency band. M is the number of frequency bands.

[0054] According to radio propagation physics, if all other parameters remain same, the received signal strength at a receiver is inversely proportional to the square of the carrier frequency. In other words, it is possible that two nodes in the network may be able to communicate on a frequency band f1 but unable to communicate on frequency band f2.

[0055] The network connectivity in frequency band-j is modeled as a graph Gj(V; Ej); j = 1; 2; :::; M. V is the set of network nodes, and Ej is designed so that, for two nodes u and v, (u; v) belong to Ej if u can communicate with v over frequency band fj at a non-zero data rate.

[0056] A generalized link is defined by :

(i) the frequency band fj over which the link exists, and
(ii) the ordered node-pair (v; u) to indicate that node v is the transmitting node of the link and u is the receiving node of the link. More precisely, one of the radio systems of node v, respectively u, is the transmitting radio, respectively receiving radio.

[0057] An interference model is used. In this interference model, two links denoted l1 and 12 interfere over a frequency band fj if any one of the end points of l1 can decode messages from any one of the end points of 11, even at the lowest possible modulation and coding.

[0058] Each generalized link denoted l has a set of interfering links denoted by Il. Thus, if a generalized link denoted l' belongs to Il, l and l' cannot transmit simultaneously. The notion of generalized links easily accounts for the fact that the interfering node-pairs of a node-pair can be different in different frequency bands.

Architecture

[0059] One key principle is to ensure that a node with a large queue-length does not lose contention to another

Samsung Ex. 1004, Page 464 of 563

interfering node with a smaller queue-length. To guarantee this in a distributed manner for various embodiments, the network is partitioned in groups. In various embodiments, each group has one leader and followers. During the execution of the prioritized CSMA based MAC protocol detailed hereafter, the leader is responsible for decisions that apply to all group members. The followers listen through broadcasted messages to leader about these decisions.

[0060] In particular, there are two kinds of decisions the leaders take which are detailed hereafter:

(i) choosing from time to time a random frequency band over which high priority generalized links in the group will operate,
ii) facilitating the procedure for obtaining the maximal gain generalized link in the group and broadcasting its identity.

[0061] The leaders and their corresponding followers selection is a one-time procedure as described below. Once this step is performed, the prioritized CSMA based MAC protocol works like CSMA with the following twist: each generalized link contends for the channel instead of each link, where a generalized link is defined as 2-tuple of link and frequency band. As explained above, a link is a transmitter-receiver node pair.

[0062] For instance, considering a wireless network with simply two interfering links, 11 and 12, 11 and 12 being source destination pairs. I1 is defined as a link between two nodes noted A and B. It is supposed that A can potentially communicate with B, provided link 12 is silent, in three different frequency bands: f1 (512-518 MHz), f2 (524-530 MHz), andf3 (560-566 MHz). Then, there are three generalized links between A and B given by the tuples (11, f1), (11, f2), and (11, f3).

[0063] Certain links are assigned higher priority than others in a dynamic manner so that a higher priority generalized link never gets beaten by a lower priority generalized link in CSMA contention for access of a frequency band.

[0064] There are three priority classes, low, medium, and high. In the following, it is described how the priorities are decided for each data radio system of each node dynamically and how the prioritized CSMA based MAC protocol is designed to ensure the priority order in channel access through contention resolution.

[0065] The architecture of the control means of a node for executing said prioritized CSMA based MAC protocol is illustrated at figure 1.

[0066] Said architecture comprises a lower MAC layer 100 which includes a radio frequency hardware 101 for the control radio system and a radio frequency hardware 102 for data radio systems.

[0067] Said architecture also comprises an upper MAC layer 200 which includes a group control module 201, for group leaders, which forms priority assigning means. Said architecture also comprises a priority control module 202 which forms dividing means to maintain three priority lists for each data radio system. In various embodiments said dividing means 202 can be realized with a Finite State Module (FSM) module.

[0068] Said upper MAC layer 200 also comprises a prioritized CSMA based MAC scheduling protocol module 203, simply called Priority-CSMA module, and per-destination packet MAC buffer(s) 204.

[0069] The functioning of said architecture is described below using the following high level steps:

[0070] 1. In the beginning, groups of nodes are formed and each node is identified as a group leader or a follower as detailed hereafter. The group control module 201 at the leader also interacts with the control radio system 101 for broadcasting information relevant for the entire group.

[0071] 2. The group control module 201 at the group leader makes decisions that apply to the entire group, namely choosing frequency bands fj over which high priority generalized links operate and broadcasting said high priority generalized link's identity. This information is also fed to the priority control module 202.

[0072] 3. The priority control module 202 maintains for each data radio system of the related node, three lists of outgoing generalized links, high priority list, medium priority list, and low priority list, thus classifying which generalized links out of the node belongs to which priority class. The priority information is fed to the Priority-CSMA module 203.

[0073] 4. The Priority-CSMA module 203 performs prioritized CSMA based MAC protocol in a manner described later. The priority class of a generalized link is learned from the priority control module 202, also called priority control module, which maintains three priority lists for each data radio system. Once transmissions over a generalized link from a particular priority class happen, this information is also fed to the Priority Control module. In case of conceiving said Priority Control module 202 with a FSM module, said information related to transmissions over a generalized link from a particular priority class, is used for internal state transition of the FSM module.

[0074] 5. Once the Priority-CSMA module 203 wins contention, this information is fed to the lower MAC layer so that it can transmit packet over the generalized link that has gained channel access right.

[0075] The CSMA or CSMA\CA based MAC protocol carried out by the nodes of the network comprises the following steps.

[0076] At time 0, an independent dominating set is computed in G1(V;E1), i.e. on the network graph in the lowest frequency band. There are known techniques to compute a dominating independent set, as detailed in the publication of S. Parthasarathy and R. Gandhi, entitled "Distributed algorithms for coloring and domination in wireless ad hoc networks. In FSTTCS, 2004."

[0077] An independent dominating set on a graph Gj (V;Ej) is a set of nodes S such that every node v belonging

Samsung Ex. 1004, Page 465 of 563

to V\S has an edge to some node in S, no two nodes in S having an edge between them.

[0078] Thus, a set of nodes D is selected in f1 such that every other node is a neighbor of some node in D in G1(V; E1). The nodes in D are called leaders in the rest of the description. Every node not in D becomes a follower of any one neighboring leader. A leader with all its followers are referred to as a group.

[0079] An example of grouping is illustrated at figure 2 with a simple topology. Considering said topology at figure 2 comprising nodes v1 to v7, an edge between two nodes means these two nodes can talk to each other, and, furthermore, cannot be involved in different communications simultaneously. For instance (v2,v1) and (v4,v5) communications cannot happen simultaneously because there is an edge between v2 and v4. In this the set S={v2,v5} forms a dominating independent set. Thus, v2 and v5 can be designated as leaders. There are two groups: G1={v1,v2,v3} and G2={v4,v5,v6,v7}. The leader of group G1 is v2 and the leader of group G2 is v5.

[0080] An algorithm, called maximal gain algorithm, executed by the MAC architecture of a leader node for determining which generalized link presents maximal gain is detailed hereafter. In various embodiments, said maximal gain algorithm is used for wireless networks whose nodes could be asynchronous or where control packets could be lost.

[0081] In various embodiments, each wireless node has one extra radio system, called control radio system, for exchange of control messages on a dedicated frequency control band. Nodes use the control band to send RTS/CTS messages to reserve an intended frequency band, said intended frequency band being decided using an algorithm or protocol described hereafter. RTS/CTS message is the standard message used in Wi-Fi like systems which contains transmitters MAC id, intended receiver's MAC id, header, CRC, and control filed. In various embodiments, RTS/CTS messages sent by nodes have an additional field containing queue-length at the MAC buffer of the transmitter node. Said additional field could also be part of the frame control field.

[0082] The gain of the generalized link is mathematically defined later. In essence, this is the gain in weight, a link operating in a particular frequency band can have by switching to a new frequency band, said new frequency band being chosen by the leader. The weight of a generalized link is defined by the multiplication of the queue-length at the transmitter MAC buffer and the physical layer data rate of the generalized link in the operating frequency band. Thus the weight depends on the frequency band through the physical layer data rate of the frequency band.

[0083] In various embodiments, the leader in each group performs key functions as maintaining, updating, and broadcasting information about the group members, and selecting the maximum gain generalized link dynamically.

[0084] Information is updated as follows. Nodes send RTS/CTS messages over the control band for an intended generalized link. The choice of the intended generalized link is described later in the algorithm. Any RTS/CTS message contains the following: (i) queue-length information of the intended link, (ii) the frequency band of the intended generalized link, (iii) and the data rate of the intended generalized link.

[0085] Whenever a leader hears an RTS/CTS message from a group member over the control frequency band, it updates the queue length of the intended generalized link from the information embedded in the RTS/CTS messages, and if the data rate of the intended generalized link has changed, then this information is also updated.

[0086] In various embodiments, nodes also send queue length updates when change in queue length due to packet arrivals is beyond a threshold.

[0087] In various embodiments, the algorithm used to determine generalized links with maximal gain is a follows.

[0088] Every T units of time, the leader selects the maximal-gain link using the following steps:

i) the leader selects a random frequency band fj,

ii) in said frequency band fj, the leader computes the maximal gain link based on its information of the weight of each link and the current set of active links. As explained above, the weight of a link over band fj is defined as the multiplication of the physical-layer data rate of the link over fj and the queue length of the MAC buffer of the transmitter node.

[0089] The gain of a generalized link noted l is computed as follows. The transmitter node of generalized link l is denoted by v. First, a loss value denoted by loss(v) is computed as follows:

Case-1: if there exists some other active generalized link l' with transmitter node as v and frequency band as fj, then loss(v) is set equal to the weight of generalized link l' over fj. The active generalized link l'is said to be sub(l), i.e. the generalized link that will be substituted by generalized link l over fj.

Case-2: if condition of Case-1 does not hold and there is a spare radio system in the transmitter node v, then set loss(v)=0; there is no sub(l) in this case.

Case-3: if the condition of Case-1 and Case-2 do not hold, then loss(v) is set to the minimum weight of all active generalized links over all frequency bands for which v is the transmitter node. The generalized link with the minimum weight among all active generalized links is called sub(l).

[0090] The gain of any generalized link l over frequency band fj is computed as follows : gain(l) over fj = "weight of generalized link l over fj" -loss(v), where v is the transmitted node of generalized link 1.

[0091] The maximum gain generalized link, noted l*,

Samsung Ex. 1004, Page 466 of 563

is the generalized link in the leaders group with maximum gain over fj, i.e. gain(l*) = maxl "gain(l) over fj", where the maximum is taken over all links l whose transmitter node belongs to the leader's group.

[0092] The leader then broadcasts over the control channel the identity of the chosen frequency band fj, the maximal-gain generalized link l*, and sub(l*) if any. sub (l*) has to be deactivated for generalized link l to be active over the chosen frequency band.

[0093] In various embodiments, an alternative to picking a frequency band randomly is as follows. The leader computes the maximal-gain generalized link over all the frequency bands available. Then frequency band over which the gain of the maximal-gain link is highest, is chosen as the frequency band of choice by the leader. This approach requires more computation since the leader has to compute the maximal gain generalized link over every available frequency band and then compute their maximum.

[0094] Referring to figure 3, a flowchart carried out by a leader node is shown.

[0095] At step 30, the leader listens to RTS/CTS messages for queue length information from other group members. At step 31, whenever the leader hears an RTS/CTS message from a group member over the control band, it updates the queue length of the intended generalized link and it updates the set of active generalized links in its group. An active generalized link is a transmitter-receiver pair of data radio systems that is involved in successful communication over the frequency band of said generalized link.

[0096] At step 32 the leader node determines if a predetermined time duration has elapsed since last broadcast of the identity of a maximal gain generalized link. If the result is negative, the leader node returns to step 30. If the result is positive, the leader chooses at step 33 a random frequency band and computes maximal gain to determine the generalized link in its group which presents maximal gain for said chosen frequency band. At step 34, the leader node broadcasts the identity of the determined maximal gain generalized link, which is also referred as a high priority generalized link.

[0097] Each node maintains for each data radio system, a set of three lists of generalized links, namely High Priority (HP) list, Medium Priority (MP) list and Low Priority (LP) list.

[0098] Addition and deletion into HP, MP, LP lists are carried out by the Priority-Control Module 202 of the node. The lists are updated as follows for each data radio system of each node.

[0099] If a node hears a broadcast, over the control frequency band, from its leader indicating that it is the transmitter of the maximum-gain generalized link, it adds this generalized link to the HP list. A generalized link is removed from the HP list once it gets activated for the first time.

[0100] Any generalized link that gets removed from the HP list is added to the MP list of the same data radio system. A generalized link in MP list is removed only when it loses contention of the channel over the band corresponding to the generalized link.

[0101] Every other generalized link that is not a part of HP or MP list belongs to LP list. In various embodiments, a generalized link belongs to LP list of all data radio systems or none of the data radio systems of the corresponding node.

[0102] Whenever a data radio system becomes free, the prioritized CSMA based MAC protocol is carried out by Priority-CSMA Module 203 with the following steps:

Step-1: The data radio system visits the lists in order of priority, i.e. in first the HP list, followed by the MP list and then the LP list, and picks the first inactive link that has non-zero queue length.

Step-2: The data radio system switches to the selected generalized link's frequency band and assesses if the channel is free. If it is free, it transmits an RTS message over the control channel at a slot selected uniformly between [0;CW/2 - 1] if it is an HP generalized link, between [CW/2; 3CW/4 - 1] if it is an MP generalized link, and between [3CW/4;CW - 1] if it is an LP generalized link. CW is the contention window size. This is contention resolution slot as in CSMA-CA protocol over Wi-Fi. The RTS message contains the following information (i) the destination and communication band, and (ii) queue size of the link. When the destination node receives an RTS, it responds with a CTS if resources, data radio system and frequency band, are available to it. The CTS also echoes the information in the RTS.

Step-3: If the contention is successful, then transmission happens for a constant time interval, noted TXOPT, for HP generalized links, and for one packet duration for MP and LP generalized links. The constant duration TXOPT is chosen so that multiple packets can be transmitted, typically a few milliseconds.

[0103] It should be apparent from the foregoing description that various exemplary embodiments of the invention may be implemented in hardware, firmware, and/or software. Furthermore, various exemplary embodiments may be implemented as instructions stored on a machine-readable storage medium, which may be read and executed by at least one processor to perform the operations described in detail herein. A machine-readable storage medium may include any mechanism for storing information in a form readable by a machine, such as a computer, network node, router, switch, or similar device. Thus, a machine-readable storage medium may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and similar storage media.

[0104] Although the various exemplary embodiments have been described in detail with particular reference

Samsung Ex. 1004, Page 467 of 563

to certain exemplary aspects thereof, it should be understood that the invention is capable of other embodiments and its details are capable of modifications in various obvious respects. As is readily apparent to those skilled in the art, variations and modifications may be implemented while remaining within the spirit and scope of the invention. Accordingly, the foregoing disclosure, description, and figures are for illustrative purposes only and do not in any way limit the invention, which is defined only by the claims.

Claims

1. Node (v2) for a wireless network, said node having at least one, preferably two, frequency agile transmitter/receiver radio system(s), called data radio system(s), allowing said node to communicate with at least another node (v1) of said wireless network over different selectable frequency bands, said node (v2) and said other node (v1) which are able to communicate over different selected frequency bands forming generalized links, a general link being defined as a link formed by a frequency agile transmitter radio system of a node (v2), called transmitter node, and a frequency agile receiver radio system of another node (v1), called receiver node, and a frequency band over which said link is able to communicate, and at least one control radio system for exchanging control messages with said at least another node (v1) of said wireless network over a control frequency band different from the frequency band used by said at least one data radio system,
said node comprising control means for executing a medium access control, called MAC, scheduling protocol based on a Carrier Sense Multiple Access, called CSMA, protocol to control communication between said node (v2) and said other node (v1) of said wireless network,
said control means comprising :

dividing means (202), for dividing a set of generalized links in at least high priority generalized links, called HP generalized link, and low priority generalized links, called LP generalized link,
and prioritized CSMA based MAC scheduling protocol module (203) configured for making said generalized links contend for a channel corresponding to their frequency band by executing said CSMA based MAC scheduling protocol so that an HP generalized link loses channel access trough a contention resolution only to another HP generalized link.

2. A node according to claim 1, wherein said dividing means (202) are also configured for dividing said set of generalized links in said HP generalized links and LP generalized links, and also in medium priority generalized links, called MP generalized links,
prioritized CSMA based MAC scheduling protocol module (203) being also configured to ensure that a MP generalized link loses channel access trough a contention resolution only to an HP generalized link or to another MP generalized link.

3. A node according to any one of claims 1 or 2, wherein said control means also comprise priority assigning means (201) configured for assigning priorities to said generalized links in function of the physical-layer data rate of the frequency band associated with said generalized link.

4. A node according to any one of claims 1 to 3, wherein priority assigning means (201) are configured to set a generalized link as a HP generalized link when gain of this generalized link is maximal compared to the gain of others generalized links.

5. A node according to claim 4, wherein priority assigning means (201) are configured to choose a random frequency band from time to time and to determine the identity of the generalized link which has maximum gain over said chosen frequency band, said determined maximal gain generalized link being set as a HP generalized link.

6. A node according to any one of claims 4 or 5, wherein priority assigning means (201) are configured to compute gain, noted gain(l), of a generalized link noted l, whose transmitter node, noted v, is able to activate said generalized link l over a frequency band noted fj, as follows :

gain (l) over frequency band fj = weight of generalized link l over fj - loss(v)
wherein the weight of a generalized link is defined by the multiplication of the queue-length of the transmitter node of the generalized link and the physical-layer data rate of the generalized link in the frequency band of said generalized link, said queue-length corresponding to the number of packets awaiting for transmission by the transmitter node of the corresponding generalized link, and
wherein loss(v) is a loss value of the transmitter node v which is computed as follows:

Case-1: if there exists some other active generalized link denoted l' for which v is also a transmitter node over frequency band fj, then loss(v) is set equal to the weight of generalized link l' over said frequency band fj ;
Case-2: if condition of Case-1 does not hold and if there is a spare transmitter radio system at node v, then loss(v) is set equal to 0 ;
Case-3: if the conditions of Case-1 and

Samsung Ex. 1004, Page 468 of 563

Case-2 do not hold, then loss(v) is set to the minimum weight of all active generalized links over all frequency bands for which v is the transmitter node.

7. A node according to any one of claims 1 to 6 combined with claim 2, wherein said node comprises list maintaining means configured to maintain three lists of generalized links, namely HP list containing HP generalized links, MP list containing MP generalized links and LP list containing LP generalized links.

8. A node according to claim 7, wherein said prioritized CSMA based MAC scheduling protocol module (203) is configured to, whenever said or one of said data radio system(s) of said node becomes free, performing the steps of :

- visiting the lists in order of priority and pick the first inactive generalized link that has non-zero queue length ;
- making said data radio system switch to the selected generalized link's frequency band and assess if the channel is free ;
- if said channel is free, transmitting a Request to Send message, called RTS message, over the control channel at a time slot selected uniformly:

between [0 ; CW/2 - 1] if said generalized link that has been picked is an HP generalized link,
between [CW/2; 3CW/4 - 1] if said generalized link that has been picked is an MP generalized link,
and between [3CW/4;CW - 1] if said generalized link that has been picked is an LP generalized link,
CW being a predetermined size of a contention window;
said RTS message containing the following information :

(i) the identity of the receiver node of the picked generalized link and the corresponding frequency band, and
(ii) queue length of said picked generalized link.

9. A node according to claim 8, wherein said prioritized CSMA based MAC scheduling protocol module (203) is also configured to command transmission over:

- a HP generalized link during a constant time interval, denoted TXOPT, if contention has been won by said HP generalized link,
- over a MP generalized link, respectively a LP generalized link, during one packet duration if contention has been won by said MP generalized link, respectively said LP generalized link.

10. A wireless network comprising a group of nodes (v1, ...,v7) according to any one of claims 1 to 9.

11. A wireless network according to claim 10, wherein said group of nodes also includes at least one node (v2), called leader node, according to any one of claims 1 to 19 combined with claim 3, the other nodes (v1, v3) of said group being called follower nodes,
said leader node (v2) being configured to broadcast messages over the control channel containing identities of generalized links which are assigned high priority,
followers nodes of said group being configured to listen to said broadcast messages.

12. A wireless network according to any one of claims 10 or 11, each node of the group being according to claim 2, wherein each node comprises list maintaining means configured to maintain three lists of generalized links, namely HP list containing HP generalized links, MP list containing MP generalized links and LP list containing LP generalized links.

13. A wireless network according to claim 12, wherein prioritized CSMA based MAC scheduling protocol module (203) of each node is configured to, whenever said or one of said data radio system(s) of said node becomes free, performing the steps of :

- visiting the lists in order of priority and pick the first inactive generalized link that has non-zero queue length ;
- making said data radio system switch to the selected generalized link's frequency band and assess if the channel is free ;
- if said channel is free, transmitting a Request To Send message, called RTS message, over the control channel at a time slot selected uniformly:

between [0 ; CW/2 - 1] if said generalized link that has been picked is an HP generalized link,
between [CW/2; 3CW/4 - 1] if said generalized link that has been picked is an MP generalized link,
and between [3CW/4;CW - 1] if said generalized link that has been picked is an LP generalized link,
CW being a predetermined size of a contention window ;
said RTS message containing the following information :

Samsung Ex. 1004, Page 469 of 563

(i) the identity of the receiver node of the picked generalized link and the corresponding frequency band, and
(ii) queue length of said picked generalized link ;

said receiver node being configured to, after receiving said RTS message, respond with a Clear to Send message, called CTS message, if said receiver node and frequency band are available, said CTS message echoing the information contained in the RTS message.

14. Method for communicating data through a wireless network comprising a plurality of nodes, each node having at least one, preferably two, frequency agile transmitter/receiver radio system(s), called data radio system(s), allowing said node to communicate with at least another node (v1) of said wireless network over different selectable frequency bands, said node (v2) and said other node (v1) which are able to communicate over different selected frequency bands forming generalized links, a general link being defined as a link formed by a frequency agile transmitter radio system of a node (v2), called transmitter node, and a frequency agile receiver radio system of another node (v1), called receiver node, and a frequency band over which said link is able to communicate, each node having also at least one control radio system for exchanging control messages with said at least another node (v1) of said wireless network over a control frequency band different from the frequency band used by said at least one data radio system,
said method also comprising the steps of :

- dividing a set of generalized links in at least high priority generalized links, called HP generalized link, and low priority generalized links, called LP generalized link,
- making said generalized links contend for a channel corresponding to their frequency band by executing a CSMA based MAC scheduling protocol so that an HP generalized link loses channel access trough a contention resolution only to another HP generalized link.

15. A method according to claim 14 wherein the step of dividing also comprises dividing said set of generalized links in medium priority generalized links, called MP generalized links,
CSMA based MAC scheduling protocol being also configured to ensure that a MP generalized link loses channel access trough a contention resolution only to an HP generalized link or to another MP generalized link.

Samsung Ex. 1004, Page 470 of 563

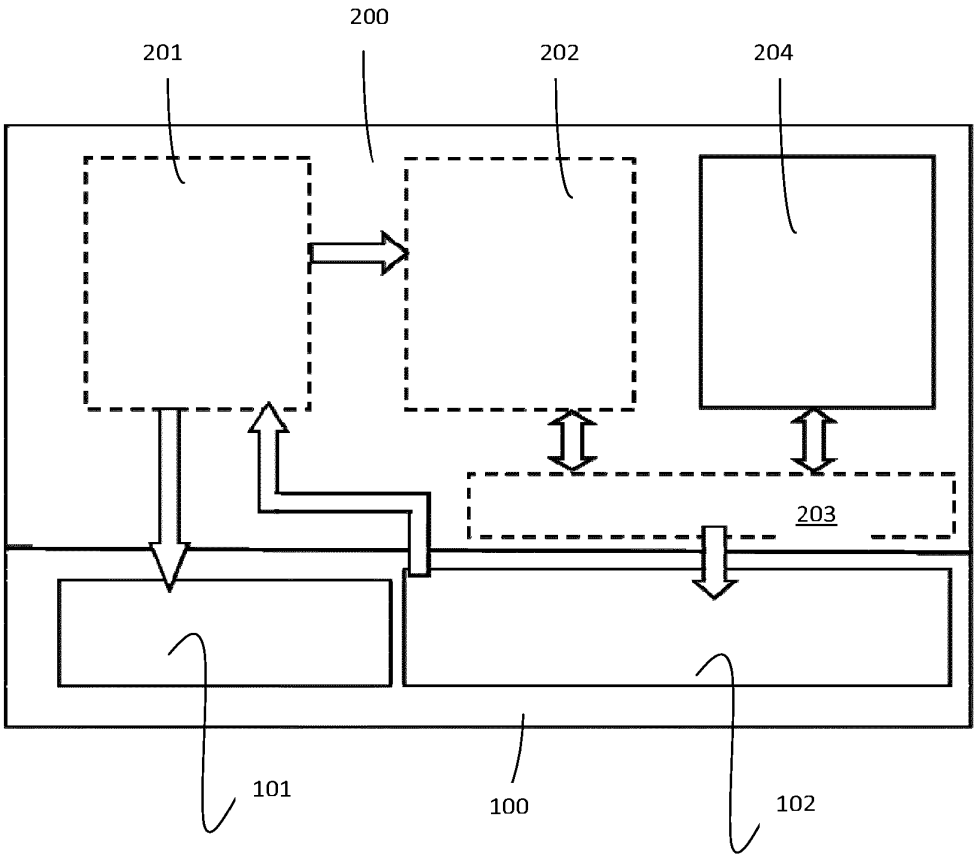


FIG.1

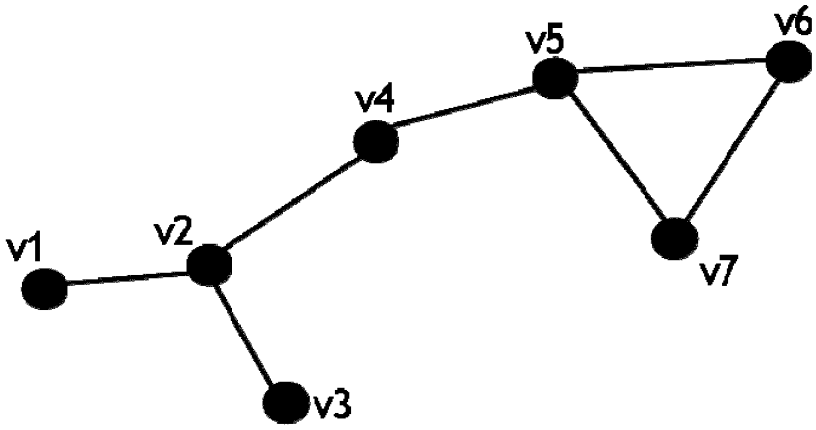


FIG.2

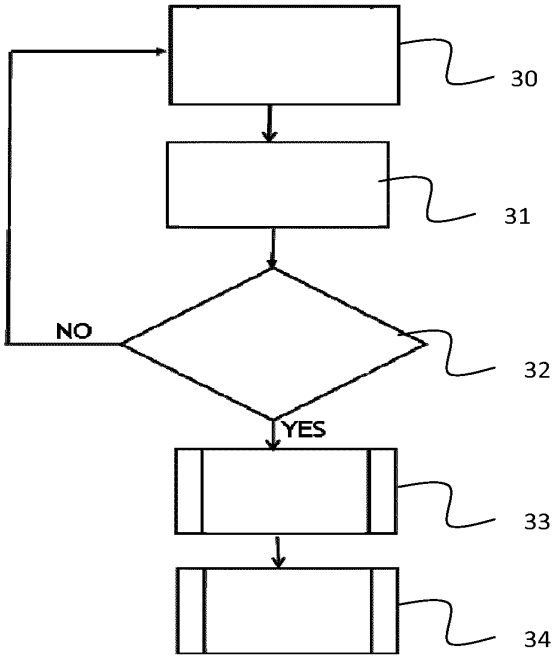


FIG.3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 11 30 6013

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	VEYSEH M ET AL: "OFDMA Based Multiparty Medium Access Control in Wireless Ad Hoc Networks", COMMUNICATIONS, 2009. ICC '09. IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 14 June 2009 (2009-06-14), pages 1-6, XP031506204, ISBN: 978-1-4244-3435-0	1-5,7, 9-12,14, 15	INV. H04W74/08
A	* abstract * * chapters I, III A B, V * * page 6, left-hand column, paragraph 1 *	6,8,13	
A	"IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Qua", IEEE STANDARD; [IEEE STANDARD], IEEE, PISCATAWAY, NJ, USA, 1 January 2005 (2005-01-01), pages _1-189, XP017603828, ISBN: 978-0-7381-4772-7 * chapters 3, 6, 7, 9, 9.1, 9.1.3, 9.1.3.1, 9.9.1 *	1-15	

-/--

TECHNICAL FIELDS SEARCHED (IPC)
H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Berlin	26 January 2012	Rosken, Wilfried

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C01)

Samsung Ex. 1004, Page 474 of 563

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 11 30 6013

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	HAMDAOUI B ET AL: "OS-MAC: An Efficient MAC Protocol for Spectrum-Agile Wireless Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 7, no. 8, 1 August 2008 (2008-08-01), pages 915-930, XP011335260, ISSN: 1536-1233, DOI: 10.1109/TMC.2007.70758 * abstract * * chapters 4.2.2, * -----	1-15	
A	MANSI THOPPIAN ET AL: "CSMA-Based MAC Protocol For Cognitive Radio Networks", WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS, 2007. WOWMOM 2007. IEEE INTERNATIONAL SYMPOSIUM ON A, IEEE, PI, 1 June 2007 (2007-06-01), pages 1-8, XP031149219, ISBN: 978-1-4244-0992-1 * chapter 5 * -----	1-15	TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Berlin	26 January 2012	Rosken, Wilfried

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1 EPO FORM 1503 03.82 (P04C01)

Samsung Ex. 1004, Page 475 of 563

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **R. GANDHI.** Distributed algorithms for coloring and domination in wireless ad hoc networks. *FSTTCS,* 2004 **[0076]**

Samsung Ex. 1004, Page 476 of 563

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 220 697 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.06.2018 Bulletin 2018/23

(51) Int Cl.:
H04W 52/02 *(2009.01)* ***H04W 4/00*** *(2018.01)*

(21) Application number: **17169607.3**

(22) Date of filing: **12.11.2013**

(54) **METHOD, APPARATUS, AND COMPUTER PROGRAM PRODUCT FOR POWER SAVE CONTROL FOR TETHERING CONNECTIONS**

VERFAHREN, VORRICHTUNG UND COMPUTERPROGRAMMPRODUKT ZUR ENERGIESPARSTEUERUNG FÜR TETHERING-VERBINDUNGEN

PROCÉDÉ, APPAREIL ET PRODUIT-PROGRAMME D'ORDINATEUR POUR UNE COMMANDE D'ÉCONOMIE D'ÉNERGIE DESTINÉE À DES CONNEXIONS D'ATTACHE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **22.01.2013 US 201313746717**

(43) Date of publication of application:
20.09.2017 Bulletin 2017/38

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
13192399.7 / 2 757 837

(73) Proprietor: **Nokia Technologies Oy**
02610 Espoo (FI)

(72) Inventors:
- **KIUKKONEN, Niko**
  02880 Veikkola (FI)
- **MARIN, Janne**
  02210 Espoo (FI)
- **REUNAMÄKI, Jukka**
  33820 Tampere (FI)

(74) Representative: **Nokia EPO representatives**
Nokia Technologies Oy
Karaportti 3
02610 Espoo (FI)

(56) References cited:
WO-A1-2011/019976
US-A1- 2008 076 411
US-A1- 2009 129 341
US-A1- 2011 263 242
US-A1- 2012 052 793
US-A1- 2012 115 471
US-A1- 2012 182 966

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 3 220 697 B1

Description

FIELD:

[0001] The field of the invention relates to wireless communication, and more particularly to configuring a mobile wireless hotspot in a wireless network.

BACKGROUND:

[0002] Modem society has adopted, and is becoming reliant upon, wireless communication devices for various purposes, such as connecting users of the wireless communication devices with other users. Wireless communication devices can vary from battery powered handheld devices to stationary household and/or commercial devices utilizing an electrical network as a power source. Due to rapid development of the wireless communication devices, a number of areas capable of enabling entirely new types of communication applications have emerged.

[0003] Cellular networks facilitate communication over large geographic areas. These network technologies have commonly been divided by generations, starting in the late 1970s to early 1980s with first generation (1G) analog cellular telephones that provided baseline voice communications, to modern digital cellular telephones. GSM is an example of a widely employed 2G digital cellular network communicating in the 900 MHZ/1.8 GHZ bands in Europe and at 850 MHz and 1.9 GHZ in the United States. While long-range communication networks, like GSM, are a well-accepted means for transmitting and receiving data, due to cost, traffic and legislative concerns, these networks may not be appropriate for all data applications.

[0004] Short-range communication technologies provide communication solutions that avoid some of the problems seen in large cellular networks. Bluetooth™ is an example of a short-range wireless technology quickly gaining acceptance in the marketplace. In addition to Bluetooth™ other short-range communication technologies include Bluetooth™ Low Energy, IEEE 802.11 wireless local area network (WLAN), Wireless USB, ZigBee (IEEE 802.15.4, IEEE 802.15.4a), and ultra high frequency radio frequency identification (UHF RFID) technologies. All of these wireless communication technologies have features and advantages that make them appropriate for various applications.

[0005] Near field communication technologies, such as radio frequency identification (RFID) technologies, comprise a range of RF transmission systems, for example standardized and proprietary systems for a large number of different purposes, such as product tagging for inventory handling and logistics, theft prevention purposes at the point of sale, and product recycling at the end of the life-cycle of the tagged product. In addition to RFID technologies, Near Field Communication (NFC) technology has recently evolved from a combination of existing contactless identification and interconnection technologies. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within close proximity of each other: A simple wave or touch can establish an NFC connection that may be used to exchange specific information for another communications protocol, which may then be used to create an actual connection in the other communications protocol, such as Bluetooth™ or wireless local area network (WLAN).

[0006] US2012/115471 discloses systems, methods, devices, and computer program products are described for discontinuous transmissions in a wireless communications system. In one example, a femtocell uses out-of-band (OOB) signals to detect the presence of user equipment (UEs) in a femtocell coverage area. In response to the detection, the femtocell may transmit in-band signals to facilitate communication with and registration of the detected UE. The femtocell may then perform discontinuous in-band transmissions to the registered UE.

SUMMARY:

[0007] Example method, apparatus, and computer program product embodiments are disclosed for configuring a mobile wireless hotspot in a wireless network.

[0008] Example embodiments of the invention include a method comprising:

establishing, by an apparatus operating as a mobile hotspot device, a control channel over a wireless out-of-band communications medium with a wireless device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

exchanging, by the apparatus operating as the mobile hotspot device, over the established control channel, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network and/or a wireless local area network provided by the apparatus operating as the mobile hotspot device.

[0009] Example embodiments of the invention include the method further comprising:

receiving, by the apparatus operating as the mobile hotspot device, over the control channel, a request from the wireless device for the in-band communi-

cations tethering connection for relaying, by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of the wide area communications network and/or the wireless local area network provided by the apparatus operating as the mobile hotspot device;

performing, by the apparatus operating as the mobile hotspot device, said exchanging over the control channel, with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and

transitioning, by the apparatus operating as the mobile hotspot device, from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection, in response to receiving the request.

[0010] Example embodiments of the invention include the method further comprising:
exchanging, by the apparatus operating as the mobile hotspot device, over the control channel, with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection with the wireless device.

[0011] Example embodiments of the invention include the method further comprising:
transitioning, by the apparatus operating as the mobile hotspot device, from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection, when no requests are received from any wireless device for the in-band communications tethering connection.

[0012] Example embodiments of the invention include the method further comprising:

wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol. Example embodiments of the invention include a method comprising:

establishing, by a wireless device, a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

exchanging, by the wireless device over the control channel, with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the apparatus operating as the mobile hotspot device in an in-band communications medium.

[0013] Example embodiments of the invention include the method further comprising:

transmitting, by the wireless device, over the control channel, a request to the apparatus operating as the mobile hotspot device for the in-band communications tethering connection;

performing, by the wireless device, said exchanging over the control channel, with the apparatus operating as the mobile hotspot device, of the in-band communications connectivity configuration information; and

establishing, by the wireless device, the in-band communications tethering connection with the apparatus operating as the mobile hotspot device, using the power saving features and optimized activity times for the in-band communications tethering connection.

[0014] Example embodiments of the invention include a computer program comprising computer readable program code configured to cause performing any of the preceding methods when said program is run on a computer.

[0015] Example embodiments of the invention include an apparatus operable as a mobile hotspot device, comprising:

means for establishing a control channel over a wireless out-of-band communications medium with a wireless device, wherein said means for establishing the control channel with the wireless device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

means for exchanging over the control channel, with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, for relaying by the apparatus, communications between the wireless device and one or more entities

Samsung Ex. 1004, Page 479 of 563

in at least one of a wide area communications network and/or a wireless local area network provided by the apparatus.

[0016] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:

means for receiving over the control channel, a request from the wireless device for the in-band communications tethering connection for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of the wide area communications network and/or the wireless local area network provided by the apparatus;

means for performing said exchanging over the control channel, with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and

means for transitioning from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection, in response to receiving the request.

[0017] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:
means for exchanging over the control channel, with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection with the wireless device.

[0018] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:
means for transitioning from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection, when no requests are received from any wireless device, for an in-band communications tethering connection

[0019] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.

[0020] Example embodiments of the invention include an apparatus comprising:

means for establishing a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said means for establishing the control channel with the apparatus operating as the mobile hotspot device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and
means for exchanging over the control channel, with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the apparatus operating as the mobile hotspot device in an in-band communications medium.

[0021] The resulting embodiments configure a mobile wireless hotspot in a wireless network.

DESCRIPTION OF THE FIGURES:

[0022]

Figure 1 is an example network diagram of a mobile wireless hotspot device A and the other wireless device B, exchanging the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, in accordance with example embodiments of the invention.

Figure 1A is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1, establishing the Bluetooth control channel, in accordance with example embodiments of the invention.

Figure 1B is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1A, receiving, by the mobile hotspot device, over the control channel, a request from the wireless device for a WLAN tethering connection for relaying by the mobile hotspot device, communications between the wireless device and the cellular telephone network, in accordance with example embodiments of the invention.

Figure 1C is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1B, exchanging over the control channel, by at least one of transmitting or receiving WLAN connectivity configuration information to enable power saving features and optimize activity times in A WLAN tethering connection with the wireless device, for relaying by the mobile hotspot device, communications between the wireless device and a cellular telephone network, in accordance with

Samsung Ex. 1004, Page 480 of 563

example embodiments of the invention.

Figure 1D is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1C, transitioning, by the mobile hotspot device, from a WLAN idle state to a WLAN active state using the power saving features and optimized activity times for the WLAN tethering connection, in response to receiving the request, in accordance with example embodiments of the invention.

Figure 1E is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure ID, exchanging adjustments in the WLAN connectivity configuration information to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 1F is an example network diagram of the mobile wireless hotspot device A of Figure 1E, transitioning, by the mobile hotspot device, from the WLAN active state to the WLAN idle state of the WLAN tethering connection, when no requests are received from any wireless device, for a WLAN tethering connection for relaying by the mobile hotspot device, communications between the any wireless device and a cellular telephone network, in accordance with example embodiments of the invention.

Figure 1G is an example flow diagram of the operation of the mobile hot spot device, wherein tethering is active until there are no active clients and then it goes into the idle state and may check that its control radio is turned on and that all connected clients support the power save feature. After receiving a tethering request from a client, it turns on mobile tethering and may also inform the client that it is up and running, in accordance with example embodiments of the invention.

Figure 2A is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging adjustments in the WLAN connectivity configuration information over the Bluetooth control channel, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 2B is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 2A, exchanging adjustments in the WLAN connectivity configuration information over the Near Field Communications (NFC) control channel or another local connectivity channel having low power, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 3A is an example flow diagram of the process performed by mobile hotspot device, in accordance with example embodiments of the invention.

Figure 3B is an example flow diagram of the process performed by the other wireless device, in accordance with example embodiments of the invention.

Figure 4 illustrates an example embodiment of the invention, wherein examples of removable storage media are shown, based on magnetic, electronic and/or optical technologies, such as magnetic disks, optical disks, semiconductor memory circuit devices and micro-SD memory cards (SD refers to the Secure Digital standard) for storing data and/or computer program code as an example computer program product, in accordance with at least one embodiment of the present invention.

DISCUSSION OF EXAMPLE EMBODIMENTS OF THE INVENTION:

[0023] This section is organized into the following topics:

A. Wireless Short-Range Communication Networks

B. Connection Formation Between Bluetooth™ Devices

C. WLAN Communication Technology

1, IEEE 802.11 WLAN

2. Wi-Fi Protected Setup / Wi-Fi Simple Configuration (WSC)

3. Authentication in Wi-Fi Protected Setup / Wi-Fi Simple Configuration

4. Wi-Fi Direct - Software Access Points

D. Near-Field Communication (NFC) Technology

E. Power Save Control For Tethering Connections

A. Wireless Short-Range Communication Networks

[0024] Short-range communication technologies provide communication solutions appropriate for many data applications, without the cost, traffic and legislative concerns of longer-range communication technologies.

Samsung Ex. 1004, Page 481 of 563

Short-range communication technologies include Bluetooth basic rate/enhanced data rate (BR/EDR), Bluetooth Low Energy (LE), IEEE 802.11 wireless local area network (WLAN), Wireless Universal Serial Bus (WUSB), ZigBee (IEEE 802.15.4, IEEE 802.15.4a), and near field communication technologies, such as radio frequency identification (RFID) and near field communication (NFC) technology that enable contactless identification and interconnection of wireless devices.

B. Connection Formation Between Bluetooth™ Devices

[0025] A procedure for forming connections between Bluetooth™ devices is described in the Bluetooth™ Specification, Version 4, June 30, 2010. The Bluetooth™ Baseband is the part of the Bluetooth™ system that implements the Media Access Control (MAC) and physical layer procedures to support the connection formation, exchange of data information streams, and ad hoc networking between Bluetooth™ devices. Connection formation may include inquiry, inquiry scanning, inquiry response, in addition to paging, page scanning, and page response procedures.

1. Inquiry

[0026] Inquiry is a procedure where a Bluetooth™ device transmits inquiry messages and listens for responses in order to discover the other Bluetooth™ devices that are within the coverage area and set discoverable. Bluetooth™ devices use the inquiry procedure to discover nearby devices, or to be discovered by devices in their locality. A Bluetooth™ device that tries to find other nearby devices is known as an inquiring device and actively sends inquiry requests. Bluetooth™ devices that are available to be found are known as discoverable devices, listen or scan for these inquiry requests, and send responses. The inquiry procedure uses dedicated physical channels for the inquiry requests and responses. The inquiry procedure does not make use of any of the architectural layers above the physical channel, although a transient physical link may be considered to be present during the exchange of inquiry and inquiry response information.

[0027] Bluetooth™ devices communicate with one another over a total bandwidth of 80 MHz divided into 79 physical channels of 1MHz each. An inquiring device wanting to discover other devices repetitively probes a first set of 16 frequencies, probing two frequencies every 625 microseconds. It repeats this at least 256 times. Then, it repetitively probes a second set of 16 frequencies. The inquiring device will repeat entire cycle at least two times. Of the 79 radio carriers, 32 are considered wake-up carriers and the inquiring device Broadcasts inquiry packets on these 32 carrier frequencies.

[0028] During the inquiry procedure, the master transmits inquiry messages with the general or dedicated inquiry access code. The timing for inquiry is the same as for paging. The identity or ID packet consists of the inquiry access code (IAC). It has a fixed length of 68 bits. The receiver uses a bit correlator to match the received packet to the known bit sequence of the ID packet. In order to discover other devices a device may enter inquiry substate. In this substate, it may repeatedly transmit the inquiry message (ID packet) at different hop frequencies. The inquiry hop sequence is derived from the Lower Address Part (LAP) of the General Inquiry Access Code (GIAC). Thus, even when dedicated inquiry access codes (DIACs) are used, the applied hopping sequence is generated from the GIAC LAP. A device that allows itself to be discovered, should regularly enter the inquiry scan substate to respond to inquiry messages. During the inquiry substate, the discovering device may collect the Bluetooth™ device Addresses of all devices that respond to the inquiry message. In addition, the discovering device also collects extended information (e.g. local name and supported services) from devices that respond with an extended inquiry response packet. It may then, if desired, make a connection to any one of the discovered devices by means of the page procedure described below. The inquiry message broadcast by the source does not contain any information about the source. However, it may indicate which class of devices should respond. There is one general inquiry access code (GIAC) to inquire for any device, and a number of dedicated inquiry access codes (DIAC) that only inquire for a certain type of device. The inquiry access codes are derived from reserved Bluetooth™ device addresses. There is only one DIAC defined in the Bluetooth™ Specification, and it is called the Limited Inquiry Access Code (LIAC). The LIAC is only intended to be used for limited time periods in scenarios where both devices have been explicitly caused to enter this state, usually by user action.

[0029] Inquiry scan is a procedure where a Bluetooth™ device listens for inquiry messages received on its inquiry scan physical channel. A device using one of its inquiry scan channels remains passive for duration of the inquiry scan window on that channel until it receives an inquiry message on this channel from another Bluetooth™ device. This is identified by the appropriate inquiry access code. If the inquiry scanning device receives an inquiry message during scan window it will then follow the inquiry response procedure to return a response to the inquiring device. The inquiry scan substate is very similar to the page scan substate. However, instead of scanning for the device's device Access code, the receiver should scan for the inquiry access code long enough to completely scan for 16 inquiry packets. The inquiry procedure uses 32 dedicated inquiry hop frequencies according to the inquiry hopping sequence. These frequencies are determined by the general inquiry address. The phase is determined by the native clock of the device carrying out the inquiry scan. Instead of, or in addition to, the general inquiry access code, the device may scan for one or more dedicated inquiry access codes. However, the scanning

Samsung Ex. 1004, Page 482 of 563

may follow the inquiry scan hopping sequence determined by the general inquiry address. The inquiry scan interval may be less than or equal to 2.56 s.

2. Inquiry Response

[0030] An inquiry response packet (FHS) is transmitted from the slave to the master after the slave has received an inquiry message. This packet contains information necessary for the inquiring master to page the slave and follows 625 microseconds after the receipt of the inquiry message. The inquiry response packet is received by the master at the hop frequency when the inquiry message received by the slave was first in the master-to-slave slot. The slave response substate for inquiries differs completely from the slave response substate applied for pages. When the inquiry message is received in the inquiry scan substate, the recipient shall return an inquiry response (FHS) packet containing the recipient's device Address (BD_ADDR) and other parameters. If the recipient has non-zero extended inquiry response data to send, it may return an extended inquiry response packet after the FHS packet. On the first inquiry message received in the inquiry scan substate the slave may enter the inquiry response substate. If the slave has non-zero extended inquiry response data to send it may return an FHS packet, with the extended inquiry response bit set to one, to the master 625 microseconds after the inquiry message was received. It may then return an extended inquiry response packet 1250 microseconds after the start of the FHS packet. If the slave's extended inquiry response data is all zeroes the slave may only return an FHS packet with the extended inquiry response bit set to zero.

[0031] A contention problem could arise when several devices are in close proximity to the inquiring device or master and all respond to an inquiry message at the same time. However, because every device has a free running clock it is highly unlikely that they all use the same phase of the inquiry hopping sequence. In order to avoid repeated collisions between devices that wake up in the same inquiry hop channel simultaneously, a device will backoff for a random period of time. Thus, if the device receives an inquiry message and returns an FHS packet, it will generate a random number, RAND, between 0 and MAX_RAND. For scanning intervals greater than or equal to 1.28 seconds MAX_RAND will be 1023, however, for scanning intervals less than 1.28s MAX_RAND may be as small as 127. A profile that uses a DIAC may choose to use a smaller MAX_RAND than 1023 even when the scanning interval is greater than or equal to 1.28s. The slave will return to the CONNECTION or STANDBY state for the duration of at least RAND time slots. Before returning to the CONNECTION and STANDBY state, the device may go through the page scan substate. After at least RAND slots, the device will add an offset of 1 to the phase in the inquiry hop sequence (the phase has a 1.28 second resolution) and return to the inquiry scan substate again. If the slave is triggered again, it will repeat the procedure using a new RAND. The offset to the clock accumulates each time an FHS packet is returned. During a period when the inquiry device is broadcasting inquiry packets, a slave may respond multiple times, but on different frequencies and at different times. Reserved synchronous slots should have priority over response packets; that is, if a response packet overlaps with a reserved synchronous slot, it will not be sent, but the next inquiry message is awaited. If a device has extended inquiry response data to send, but the extended inquiry response packet overlaps with a reserved synchronous slot, the FHS packet may be sent with the EIR bit set to zero.

[0032] The messaging during the inquiry routines is summarized as follows:

In step 1, the master transmits an inquiry message using the inquiry access code and its own clock.

In step 2, the slave responds with the FHS packet containing the slave's Bluetooth™ device Address, native clock and other slave information. This FHS packet is returned at times that tend to be random. The FHS packet is not acknowledged in the inquiry routine, but it is retransmitted at other times and frequencies as long as the master is probing with inquiry messages.

In step 3, if the slave has non-zero extended inquiry response data, it sends an extended inquiry response packet to the master.

3. Extended Inquiry Response

[0033] An Extended Inquiry Response may be used to provide miscellaneous information during the inquiry response procedure. Data types are defined for such things as local name and supported services, information that otherwise would have to be obtained by establishing a connection. A device that receives a local name and a list of supported services in an extended inquiry response does not have to connect to do a remote name request and a service discovery protocol (SDP) service search, thereby shortening the time to useful information. If the slave transmits an extended inquiry response packet, it is transmitted 1250 microseconds after the start of the inquiry response packet. The extended inquiry response packet is received by the master at the hop frequency when the inquiry message received by the slave was first in the master-to-slave slot. The extended inquiry response packet is an Asynchronous Connection-oriented Logical transport (ACL) data medium rate (DM) packet with type DM1, DM3, DM5, DH1, DH3 or DH5. To minimize interference it is recommended to use the shortest packet that is capable of containing the data. The packet is sent on the same frequency as the (frequency hop synchronization) FHS packet, 1250 microseconds after

Samsung Ex. 1004, Page 483 of 563

the start of the FHS packet. In the packet header, the logical transport address (LT_ADDR) may be set to zero. TYPE may be one of DM1, DM3, DM5, DH1, DH3 or DH5. FLOW, ARQN and SEQN may all be set to zero and ignored during receipt. (ARQN is automatic repeat address acknowledgement indication and SEQN is sequential numbering scheme.) The header error check (HEC) linear feedback shift register (LFSR) may be initialized with the same default check initialization (DCI) as for the FHS packet. In the payload header, logical link identifier (LLID) may contain the value 10 (start of a logical link control and adaptation control (L2CAP) message or no fragmentation). FLOW may be set to zero and ignored upon receipt. The length of the payload body (LENGTH) may be smaller than or equal to 240 bytes. The cyclic redundancy check (CRC) linear feedback shift register (LFSR) may be initialized with the same DCI as for the FHS packet. The data whitening LFSR may be initialized with the same value as for the FHS packet. The length of the payload body (LENGTH) may be smaller than or equal to 240 bytes. The CRC LFSR may be initialized with the same DCI as for the FHS packet. The data whitening LFSR may be initialized with the same value as for the FHS packet. The payload data has two parts, a significant part followed by a non-significant part. The significant part contains a sequence of data structures. The non-significant part contains all zero octets. The baseband may not change any octets in the significant part. When transmitting data, the non-significant part octets may be omitted from the payload. A device may store a single extended inquiry response packet. This packet may be used with all inquiry access codes (IACs).

4. Page

[0034] Page is the initial phase of the connection procedure where a device transmits a train of page messages until a response is received from the target device, is stopped by host or a timeout occurs. Page scan is a procedure where a device listens for page messages received on its page scan physical channel. In forming a connection, the paging device will become the master and the page scan device will become the slave in a piconet. Initially, after the slave has received an inquiry message, an inquiry response packet is transmitted from the slave to the master. The inquiry response packet sent from the slave contains information necessary for the inquiring master to page the slave, such as Bluetooth™ device Address of the slave device. The necessary information may be received by other means, such as Out-Of-Band pairing. Also the page is not away always preceded with inquiry, because the address may be known beforehand (for example saved from previous connections). In the paging procedure, the Bluetooth™ device that will become the master carries out a page procedure by transmitting page messages in connection request packets to the specified Bluetooth™ slave device that carries out a page scanning procedure to listen for connection request packets from the paging device. A connectable Bluetooth™ device listens for a page request on its page scan channel and, once received, enters into a sequence of exchanges with the paging device. In order for a device to connect to another device, it performs frequency hopping all page scan channel frequencies, sending a page request on each frequency and listening for a response. The page scan channel uses an access code derived from the scanning device's Bluetooth™ device Address BD_ADDR to identify communications on the channel. The page scan channel uses a slower hopping rate than the hop rate of the paging device, using the Bluetooth™ device clock of the scanning device as an input. A device listening on its page scan channel remains passive until it receives a page request from another Bluetooth™ device, identified by the page scan channel access code. The two devices will then follow the page procedure to form a connection where the paging device is the master and the page scan device is the slave in a piconet. In order for a paging device to connect to another Bluetooth™ device, it uses the page scan channel of the target device in order to send page requests. If the paging device does not know the phase of the target device's page scan channel, it does not know the current hop frequency of the target device. Therefore, the paging device transmits page requests on each of the page scan hop frequencies and listens for a page response. This is done at a faster hop rate, allowing the paging device to cover all page scan frequencies in a short period of time. The paging device may have some knowledge of the target device's Bluetooth™ clock, such as indicated during a previous inquiry transaction between the two devices, and may be able to predict the phase of the target device's page scan channel. It may use this information to optimize the synchronization of the paging and page scanning process and speed up the formation of the connection.

5. Service Discovery Protocol (SDP)

[0035] Bluetooth devices are designed to find other Bluetooth devices within their radio communications range and to discover what services they offer, using a service discovery protocol (SDP). The SDP searching function relies on links being established between the requesting Bluetooth device in a client role and the responding Bluetooth device in a server role. Once a link has been established, it can be used to find out about services in the responding Bluetooth device and how to connect to them.

[0036] Service Discovery Protocol (SDP) is used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (headset profile, hands free profile, advanced audio distribution profile, etc.) and the protocol multiplexor settings needed to con-

nect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

C. WLAN Communication Technology

1. IEEE 802.11 WLAN

[0037] The IEEE 802.11 standard specifies methods and techniques of an exemplary wireless local area network (WLAN) operation, examples include the IEEE 802.11b and 802.11g wireless local area network specifications, which have been a staple technology for traditional WLAN applications in the 2.4 GHz ISM band. The various amendments to the IEEE 802.11 standard were consolidated for IEEE 802.11a, b, d, e, g, h, i, j, k, n, r, s, u, v, and z protocols, into the base standard IEEE 802.11-2012, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, February 2012 (incorporated herein by reference). Since then, emerging broadband applications have stimulated interest in developing very high-speed wireless networks for short range communication, for example, the planned IEEE 802.11ac, and the planned IEEE 802.11ad WLAN specifications that are to provide a very high throughput in higher frequency bands. Applications of these IEEE 802.11 standards include products such as consumer electronics, telephones, personal computers, and access points for both for home and office.

[0038] An IEEE 802.11 WLAN may be organized as an independent basic service set (IBSS) or an infrastructure basic service set (BSS). The access point (AP) in an infrastructure basic service set (BSS) IEEE 802.11 WLAN network, is a central hub that must relay all communication between the mobile wireless devices (STAs) in an infrastructure BSS. If a STA in an infrastructure BSS wishes to communicate a frame of data to a second STA, the communication must take two hops. First, the originating STA transfers the frame to the AP. Second, the AP transfers the frame to the second STA. In an infrastructure BSS, the AP either transmits Beacons or responds to probes received from STAs for discover purposes. After a possible authentication of a STA that is conducted by the AP, an association occurs between the AP and a STA enabling data traffic to be exchanged with the AP. The Access Point (AP) in an Infrastructure BSS may bridge traffic out of the BSS onto a distribution network.

[0039] The IEEE 802.11 WLAN uses two types of transmission: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF employs Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Every packet sent is positively acknowledged by the receiver. A transmission begins with a Request to Send (RTS) and the receiver responds with a Clear to Send (CTS). The channel is cleared by these two messages, since all STAs that hear the CTS will suppress their own start of a transmission. Then when data packets are transmitted, each has a Network Allocation Vector (NAV) containing a duration value to reserve the channel for the sender and receiver for an interval after the current packet, equal to the NAV duration. The value of the NAV decrements with the passage of time. Once the sender and receiver have reserved the channel, they may hold it for the remaining duration of the NAV value. The last acknowledgement packet (ACK) contains a NAV value of zero, to immediately release the channel. The Point Coordination Function (PCF) is a polling method among the STAs of the BSS, which is coordinated by the access point.

[0040] IEEE 802.11 authentication operates at the link level between IEEE 802.11 STAs. IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is a station service that may be used by all STAs to establish their identity to STAs with which they communicate in both infrastructure and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, then an association is not established. IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the distribution system. Shared Key authentication relies on wired equivalent privacy to demonstrate knowledge of an encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods. A robust security network association (RSNA) supports authentication based on IEEE 802.1X-2004, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the Extensible Authentication Protocol (EAP) (IETF RFC 3748-2004) to authenticate STAs and an authentication server (AS) with one another. In IEEE 802.1X, a STA being authenticated and the authenticator device exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

[0041] The access point (AP) in an infrastructure BSS assists those mobile wireless devices (STAs) attempting to save power. The legacy IEEE 802.11e Wireless LAN standards provides for support of low power operation in handheld and battery operated STAs, called automatic power save delivery (APSD). A STA capable of APSD and currently in the power saving mode, will wake up at predetermined beacons received from the AP to listen to a Traffic Indication Map (TIM). If existence of buffered traffic waiting to be sent to the STA is signaled through the TIM, the STA will remain awake until AP sends out all the data. The STA does not need to send a polling signal to the AP to retrieve data, which is the reason for the term "automatic" in the acronym APSD.

[0042] A Traffic Indication Map (TIM) is a field transmitted in beacon frames, used to inform associated wireless client devices that the access point has buffered

Samsung Ex. 1004, Page 485 of 563

data waiting to be transmitted to them. Access points buffer frames of data for wireless client devices while they are sleeping in a low-power state. The access point transmits beacons at a regular interval, the target beacon transmission time (TBTT). The Traffic Indication Map (TIM) information element in the periodically transmitted beacon frame, indicates which wireless client devices have buffered data waiting to be accessed in the access point. Each frame of buffered data is identified by an association identifier (AID) associated with a specific wireless client device. The AID is used to logically identify the wireless client device to which buffered frames of data are to be delivered. The traffic indication map (TIM) contains a bitmap, with each bit relating to a specific association identifier (AID). When data is buffered in the access point for a particular association identifier (AID), the bit is "1". If no data is buffered, the bit for the association identifier (AID) is "0". Wireless client devices must wake up and listen for the periodic beacon frames to receive the Traffic Indication Map (TIM). By examining the TIM, a wireless client device may determine if the access point has buffered data waiting for it. To retrieve the buffered data, the wireless client device may use a power-save poll (PS-Poll) frame. After transmitting the PS-Poll frame, the client mobile station may stay awake until it receives the buffered data or until the bit for its association identifier (AID) in the Traffic Indication Map (TIM) is no longer set to "1", indicating that the access point has discarded the buffered data.

[0043] Two variations of the APSD feature are unscheduled automatic power save delivery (U-APSD) and scheduled automatic power save delivery (S-APSD). In U-APSD, the access point (AP) is always awake and hence a mobile wireless device (STA) in the power save mode may send a trigger frame to the AP when the STA wakes up, to retrieve any queued data at the AP.. In S-APSD, the AP assigns a schedule to a STA and the STA wakes up, sends a power save poll packet to the AP in order to retrieve from the AP any data queued. An AP may maintain multiple schedules either with the same STA or with different STAs in the infrastructure BSS network. Since the AP is never in sleep mode, an AP will maintain different scheduled periods of transmission with different STAs in the infrastructure BSS network to ensure that the STAs get the maximum power savings.

2. Wi-Fi Protected Setup / Wi-Fi Simple Configuration (WSC)

[0044] Network setup for IEEE 801.11 WLANs has been simplified by the Wi-Fi Protected Setup™ system that is included in most access points. The Wi-Fi Alliance published the Wi-Fi Protected Setup (WPS) specification 1.0, Wi-Fi Protected Setup Specification, Version 1.0h, December 2006 (incorporated herein by reference). The Wi-Fi Simple Configuration (WSC) Specification, Version 2.0, December 20, 2010, (incorporated herein by reference), updates the Wi-Fi Protected Setup Specification, Version 1.0h. The acronym WSC, for Wi-Fi Simple Configuration Specification, may be used interchangeably with the_acronym WPS, for Wi-Fi Protected Setup. Wi-Fi Protected Setup facilitates the initial setting up of IEEE 802.11 devices in a Wi-Fi infrastructure network so that they may be more easily configured with security features and so that that new Wi-Fi devices may be added to the network. Wi-Fi Protected Setup allows access points to be set up by entering a PIN. The Protected Setup system uses this information to send data to a computer connected to the access point, to complete the network setup. Wi-Fi Protected Setup defines new IEEE 802.11 information elements (IE) that are included in beacons, probe requests and probe responses. The purpose of these IEs is to advertise the presence of devices that are capable of performing Wi-Fi Protected Setup operations.

[0045] Initial discovery of Wi-Fi Simple Configuration devices is accomplished using IEEE 802.11 Information Elements in management frames (Beacon, Probe Request, and Probe Response). If the Enrollee decides to pursue a connection to the network, it initiates an IEEE 802.1X/EAP connection for the Extensible Authentication Protocol (EAP)-based Registration Protocol. The Wi-Fi Simple Configuration Information Element complies with the IEEE 802.11 Information Element format and indicates specific data necessary for network information, capabilities and modes, to configure an Enrollee for the wireless network and to report problems with the Enrollee associating with a specified wireless network with the supplied settings.

[0046] The Wi-Fi Protected Setup 1.0 standard defines three types of components in a network: a Registrar, an Enrollee, and an Access Point (AP). A Registrar is a component with the authority to issue and revoke credentials to a network. A Registrar may be integrated into an AP or it may be separate from the AP. An Enrollee is a component seeking to join a wireless LAN network. An Authenticator is an AP functioning as a proxy between a Registrar and an Enrollee. A Registrar wireless device configures the Enrollee wireless device, and the AP acts as an Authenticator to proxy the relevant messages between the Registrar and the Enrollee. The messages exchanged in the session are a series of Extensible Authentication Protocol (EAP) request/response messages, ending with the Enrollee reconnecting to the network with its new configuration. EAP is an authentication framework defined in RFC 5247, for providing the transport and usage of keying material and parameters needed to establish a secure Wi-Fi network. The Wi-Fi Simple Configuration Specification, Version 2.0, December 20, 2010, (incorporated herein by reference), updates the Wi-Fi Protected Setup Specification, Version 1.0h.

[0047] A standalone AP that supports Wi-Fi Protected Setup, includes a built-in Registrar and does not use an external Registrar. In initial WLAN setup with Wi-Fi Protected Setup, when initializing in a standalone mode, a Wi-Fi Protected Setup AP automatically chooses a random SSID and channel. A standalone AP that includes

Samsung Ex. 1004, Page 486 of 563

a Wi-Fi Protected Setup Registrar, issues keys to Enrollees via the Registration Protocol.

[0048] When an Enrollee is initialized, it looks for Beacons from APs and sends probe requests with the WSC information element (IE), into either selected networks or into each network sequentially. It may also send probe requests to each IEEE 802.11 channel with the WSC IE included. It looks for the WSC IE in probe-responses that it receives and can engage with one or more Registrars to further discover Registrar capabilities and to see if the user has selected a Registrar. The Enrollee may continue looking for selected Registrar flags in Beacons, probe-responses and any M2 messages and may cease scanning when it finds a Registrar indicating that it is prepared to configure the Enrollee.

[0049] The following example describes an example in-band setup procedure using Wi-Fi Protected Setup for adding Member devices using a Standalone AP/Registrar. The user may convey the Enrollee's device password to the AP/Registrar using keyboard entry or an out -of-band channel with Near-Field Communication (NFC) Connection Handover. This example does not show the exchange of preliminary M1 and M2D messages that may take place after the probe message exchange, because the Enrollee may be waiting for the user to configure the AP/Registrar with the Enrollee's device password.

1. The Enrollee sends its Discovery data in a probe request to a Wi-Fi Protected Setup AP or ad hoc wireless Registrar. The AP or wireless Registrar responds with its own Discovery data in the probe response.

2. The user may be prompted to enter the Enrollee's device password into the AP/Registrar using a keypad interface or an out-of-band channel.

3. The Enrollee connects and initiates the IEEE 802.1X port-based Network Access Control procedure for port-based authentication.

4. The Enrollee and Registrar exchange messages M1 -M8 to provision the Enrollee.

5. The Enrollee disassociates and reconnects, using its new WLAN authentication Credential. The Enrollee is now connected to the network with its new configuration.

3. Authentication in Wi-Fi Protected Setup/Wi-Fi Simple

Configuration

[0050] The Wi-Fi Simple Configuration Specification, Version 2.0 (renamed from the original name "Wi-Fi Protected Setup"), uses the IEEE 802.1X Port-Based Authentication and Extensible Authentication Protocol (EAP) to transport in-band Registration Protocol messages. This protocol is mapped onto a custom EAP method described below. Wi-Fi Simple Configuration does not require the AP to support remote authentication dial-in user service (RADIUS) (IETF RFC 2865-2000), and the network need not include an authentication server. In fact, many Wi-Fi Simple Configuration APs may support IEEE 802.1X only to configure Wi-Fi Protected Access 2 (WPA2)-Personal Credentials using Wi-Fi Simple Configuration. Enrollees using Wi-Fi Simple Configuration are not granted direct access to the WLAN through the Wi-Fi Simple Configuration custom EAP method. The EAP method is used to configure the Enrollee with a Credential that can be used subsequently with whatever access method is supported by that WLAN. For example, if the AP only supports WPA2-Personal with a network-wide shared Pre-Shared Key (PSK), then the Enrollee would run the 802.1X exchange to obtain the PSK, disassociate, and then reconnect and use WPA2-Personal to access the WLAN. Alternatively, if the AP supports 802.1X authentication, the Enrollee may first run the Wi-Fi Simple Configuration EAP method to obtain a shared secret Credential and then reconnect using that secret in conjunction with another EAP method to access the WLAN.

[0051] The Wi-Fi Simple Configuration EAP method (EAP-WSC) can be used for Registrar and Enrollee discovery and for Credential establishment. The first time the Enrollee encounters a new WLAN, it sends out its Discovery information and executes the EAP-WSC method. In both the Discovery message and in Registration Protocol Message M1, the Enrollee provides information about itself to the WLAN. The M2 and M2D messages sent to the Enrollee likewise provide information about the available Registrars. When the Enrollee first discovers and attempts to connect to the WLAN, the WLAN's Registrar(s) may not yet know the Enrollee's device password. Therefore, Registrars without the device password respond with M2D messages. Although these M2D messages are unauthenticated, they can help Enrollees with rich user interfaces, to guide the user through the enrollment process.

[0052] As the Enrollee scans over the M2D messages sent by the network, it may discover that none of them possesses its device password. At this point, the Enrollee has an opportunity to prompt the user to perform a trust bootstrapping operation such as connecting an available out-of-band channel or entering a device password into one of the available Registrars. If the user decides to enter the Enrollee's device password into the Registrar, the Enrollee can reconnect and run the EAP method once more to perform the complete Registration Protocol. If the Enrollee has no user interface to lead the user through the enrollment, it is likely that one or more of the WLAN's Registrars can do this. Both the Registrar and the Enrollee are given sufficient information about each others' capabilities through the EAP method to successfully lead

Samsung Ex. 1004, Page 487 of 563

the user through the enrollment. If the user decides to use an out-of-band channel for registration, then message M2 is implicitly authenticated by the channel and can carry the network configuration data.

[0053] The AP functions as the EAP authenticator on the WLAN. Thus, the AP generates EAP Request messages and Enrollees and Registrars generate EAP Responses. If the Registrar is external to the AP, then it uses universal plug and play (UPnP) to exchange Registration Protocol messages with the AP. A Registrar may also function in the role of an 802.1X authenticator, which is useful for networks with legacy APs.

[0054] The Wi-Fi Simple Configuration EAP method uses EAP, as specified in RFC 3748, and Extensible Authentication Protocol (EAP) over LAN (EAPoL), as specified in IEEE 802.1X-2001, but does not represent a network authentication protocol. Rather Wi-Fi Simple Configuration utilizes the 802.1X data connection for acquiring settings necessary for connecting to the network and the resulting EAP exchange must always terminate with EAP-Failure.

[0055] When the Enrollee decides to connect to the network and run the Wi-Fi Simple Configuration EAP method, it associates with the AP and sends an EAPoL-Start message. The AP responds with an EAP-Request/Identity. The Enrollee sends an EAP-Response/Identity containing the defined Wi-Fi Alliance name for a Simple Configuration Enrollee ("WFA-SimpleConfig-Enrollee-1-0"). This causes the AP to start running the Simple Configuration EAP method. The Registration Protocol messages are exchanged until M8 is received and validated by the Enrollee. If it successfully processes M8, the Enrollee sends an EAP-Response/Done message to the authenticator, which sends the WSC_Done message to any External Registrar and the authenticator returns an EAP-Failure message to the Enrollee. An Enrollee should assume that the received credentials are valid after successfully processing message M8 and sending the WSC_Done message. The Enrollee then disassociates and reconnects with the Credential obtained from M8's ConfigData. If M2D is received by the Enrollee, it should respond with an ACK message so that the AP can continue to send it discovery messages from other Registrars. After the AP sends an EAP-failure to the Enrollee, the Enrollee can do one of two things (given that the AP did not de-authenticate the Enrollee after sending the EAP-Failure): it can disconnect from the AP and reconnect some time later to rerun the Wi-Fi Simple Configuration EAP method by sending an EAPoL-Start message or it can stay connected to the AP and rerun the Wi-Fi Simple Configuration EAP method by sending another EAPoL-Start message.

[0056] Once the Enrollee sends an M3 message, both the Registrar and the Enrollee must proceed in lock-step fashion until either a failure or until success occurs (indicated by the Done response message). If the Enrollee (IEEE 802.1X supplicant) detects any errors in these later phases, it responds by sending a NACK message and transitioning to the termination state to terminate the connection. At this point, the Enrollee computes a fresh device password for use in the next instance of the Registration Protocol. If the same password is reused with multiple instances of the protocol, it will be susceptible to active attack.

[0057] The Registration Protocol Messages M1 to M8 are described in the Wi-Fi Simple Configuration Specification, Version 2.0. They include an exchange of public keys, description of the sending device, including its MAC address and device capabilities, and various message authentication values, culminating in the Registrar sending to the Enrollee credentials for accessing the network.

[0058] A credential is a data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network. With out-of-band configuration, WLAN credentials are sent across the out-of-band channel to the Enrollee. The NFC interfaces operating in peer-to-peer mode between an AP or Group Owner (GO) having an integrated Registrar and an Enrollee device, have the strongest security properties supported by the Wi-Fi Simple Configuration Specification, because practical man-in-the-middle attacks against NFC are not feasible. In this mode, a 1536-bit Diffie-Hellman exchange is performed over the NFC interface, and WLAN settings are encrypted using 128-bit Advanced Encryption Standard (AES) and delivered over the same interface between an AP or Group Owner (GO) and an Enrollee device. The Diffie-Hellman public keys and WLAN settings are implicitly authenticated by both the Registrar and the Enrollee, because they are received over the NFC channel.

4. Wi-Fi Direct - Software Access Points

[0059] The Wi-Fi Alliance has developed a Wi-Fi Peer-to-Peer technology named Wi-Fi Direct™ that is specified in the Wi-Fi Alliance Peer-to-Peer Specification, October 2010 (incorporated herein by reference). Wi-Fi Direct, is also referred to herein as Peer-to-Peer or P2P. Wi-Fi Direct enables IEEE 802.11a, g, or n devices to connect to one another, peer-to-peer, without prior setup or the need for wireless access points. Wi-Fi Direct embeds a software access point into any device, which provides a version of Wi-Fi Protected Setup. When a device enters the range of a STA supporting Wi-Fi Direct (a Wi-Fi Direct device), it can connect to it and then gather setup information using a Wi-Fi Protected Setup transfer. Devices that support Wi-Fi Direct may discover one another and advertise available services. Wi-Fi Direct devices support typical Wi-Fi ranges and the same data rates as can be achieved with an 802.11a, g, or n infrastructure connection. When a device enters the range of the Wi-Fi Direct device, it may connect to it using the existing protocol, and then gather setup information using a Wi-Fi Protected Setup 2.0 transfer.

[0060] Wi-Fi Direct enables IEEE 802.11 devices that support Wi-Fi Direct, to connect to one another, point-to-point. The specification may be implemented in any Wi-

Fi device. Devices that support the specification will be able to discover one another and advertise available services. Wi-Fi Direct devices will support typical Wi-Fi ranges and the same data rates as can be achieved with an infrastructure connection. Wi-Fi Direct provides point-to-point connections for networks by embedding a software access point into any device that wishes to support Wi-Fi Direct. The soft AP provides a version of Wi-Fi Protected Setup 2.0. When a device enters the range of the Wi-Fi Direct device, it may connect to it using the existing protocol, and then gather setup information using a Wi-Fi Protected Setup 2.0 transfer.

[0061] Wi-Fi Direct-certified devices may create direct connections between Wi-Fi client devices without requiring the presence of a traditional Wi-Fi infrastructure network of an access point or router. Wi-Fi Direct-certified devices support connection with existing legacy Wi-Fi devices using the IEEE 802.11 a/g/n protocols. Wi-Fi Direct Device Discovery and Service Discovery features allow users to identify available devices and services before establishing a connection, for example, discovering which Wi-Fi device is a printer.

[0062] A Wi-Fi Direct device may support an infrastructure network of an access point or router in addition to a peer-to-peer (P2P) connection. Wi-Fi Direct devices may join infrastructure networks as stations (STAs) and may support Wi-Fi Protected Setup enrollee functionality. Wi-Fi Direct devices may connect by forming Groups in a one-to-one or one-to-many topology. The Groups functions in a manner similar to an infrastructure basic service set (BSS). A single Wi-Fi Direct device will be the Group Owner (GO) that manages the Group, including controlling which devices are allowed to join and when the Group is started or terminated. The Group Owner (GO) will appear as an access point to legacy client's devices.

[0063] Wi-Fi Direct devices include a Wi-Fi Protected Setup Internal Registrar functionality and communication between Clients in the Group. Wi-Fi Direct devices may be a Group Owner (GO) of a Group and may be able to negotiate which device adopts this role when forming a Group with another Wi-Fi Direct device. A Group may include both Wi-Fi Direct devices and legacy devices (i.e., that are not compliant with the Wi-Fi Alliance Peer-to-Peer Specification). Legacy Devices can only function as Clients within a Group.

[0064] Wi-Fi Direct devices support Discovery mechanisms. Device Discovery is used to identify other Wi-Fi Direct devices and establish a connection by using a scan similar to that used to discover infrastructure access points. If the target is not already part of a Group, a new Group may be formed. If the target is already part of a Group, the searching Wi-Fi Direct device may attempt to join the existing Group. Wi-Fi Protected Setup may be used to obtain credentials from the Group Owner (GO) and authenticate the searching Wi-Fi Direct device. Wi-Fi Direct devices may include Service Discovery that enables the advertisement of services supported by higher layer applications to other Wi-Fi Direct devices. Service Discovery may be performed at any time (e.g. even before a connection is formed) with any other discovered Wi-Fi Direct device.

[0065] A Group may be created by a single Wi-Fi Direct device, such as when connecting a legacy device. When forming a connection between two Wi-Fi Direct devices, a Group may be formed automatically and the devices may negotiate to determine which device is the Group Owner. The Group Owner may decide if this is a temporary (single instance) or persistent (multiple, recurring use) Group. After a Group is formed, a Wi-Fi Direct device may invite another Wi-Fi Direct device to join the Group. The decision of whether or not to accept an invitation may be left to the invited Wi-Fi Direct device.

[0066] Wi-Fi Direct Devices may participate in multiple Groups. A Wi-Fi Direct Device that may be in a Group while maintaining a WLAN infrastructure connection at the same time is considered a Concurrent Device or a dual stack device. For example, a laptop connected directly to a printer while simultaneously using a WLAN connection is operating as a Concurrent Device. Concurrent connections may be supported by a single radio and may support connections on different channels. Concurrent operation may be supported by multiple protocol stacks, for example, one for operation as a WLAN-STA and one for operating as a Wi-Fi Direct device. For example, two separate physical MAC entities may be maintained, each associated with its own PHY entity, or they may use a single PHY entity supporting two virtual MAC entities.

[0067] The Wi-Fi Peer-to-Peer Technical Specification v1.1, 2010 published by the Wi-Fi Alliance, provides for provisioning in Wi-Fi Direct networks. Provisioning is a phase of peer-to-peer group formation in which credentials for the peer-to-peer group are exchanged based on the use of Wi-Fi Simple Configuration. Credentials are information that is required to join a peer-to-peer group as defined in the Wi-Fi Simple Configuration Specification.

[0068] To allow for peer-to-peer device configuration, peer-to-peer devices may delay starting the provisioning phase until the expiration of the larger of the peer-to-peer group owner's (GO) configuration time and the peer-to-peer client's client configuration time, based on respective configuration timeout attributes exchanged during a preceding group owner negotiation.

[0069] The peer-to-peer device selected as peer-to-peer group owner (GO) during group owner negotiation may start a peer-to-peer group session using the credentials it intends to use for that group. The peer-to-peer group owner (GO) may use the operating channel indicated during group owner negotiation, if available. The peer-to-peer client may connect to the peer-to-peer group owner to obtain credentials. If the operating channel is not available the peer-to-peer group owner may use another channel from a channel list attribute sent in the group owner negotiation confirmation frame. The peer-to-peer client may have to scan to find the peer-to-

Samsung Ex. 1004, Page 489 of 563

peer group owner if the intended operating channel is not available. A group formation bit in a peer-to-peer group capability bitmap of the peer-to-peer capability attribute may be set to one until provisioning succeeds.

[0070] Provisioning may be executed in Wi-Fi Direct networks, as described, for example, in the Wi-Fi Simple Configuration (WSC) Specification, Version 2.0, December 20, 2010. The peer-to-peer group owner (GO) may serve the role as the access point with an internal registrar. It will only allow association by the peer-to-peer device that it is currently with in a group formation. Since the user has entered the WSC PIN or triggered the WSC pushbutton functionality on both devices, the registrar may send an M2 message in response to an M1 message. The peer-to-peer client may serve the role as the STA enrollee. It may associate to the peer-to-peer device that it is currently with in the group formation.

[0071] If provisioning fails, then group formation ends and the peer-to-peer group owner (GO) may end the peer-to-peer group session. If provisioning fails, the peer-to-peer device may retry group formation or return to device discovery. On successful completion of provisioning in Wi-Fi Direct networks, the peer-to-peer group owner (GO) may set the group formation bit in the peer-to-peer group capability bitmap of the peer-to-peer capability attribute to zero. At this point the peer-to-peer client may join the peer-to-peer group in the Wi-Fi Direct network, using the credentials supplied during provisioning.

D. Near-Field Communication (NFC) Technology

[0072] One of the methods provided by the Wi-Fi Simple Configuration Specification, Version 2.0, is the Near-Field Communication (NFC) method, in which the user brings a new wireless client device (STA) close to an access point (AP) or Registrar of the Network to allow near field communication between the devices.

[0073] Near field communication technologies, such as radio frequency identification (RFID) technologies, comprise a range of RF transmission systems, for example standardized and proprietary systems for a large number of different purposes, such as product tagging for inventory handling and logistics, theft prevention purposes at the point of sale, and product recycling at the end of the life-cycle of the tagged product. In addition to RFID technologies, Near Field Communication (NFC) technology has recently evolved from a combination of existing contactless identification and interconnection technologies. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within close proximity of each other: A simple wave or touch can establish an NFC connection, which is then compatible with other known wireless technologies, such as Bluetooth™ or wireless local area network (WLAN).

[0074] Near-field communication (NFC) technology used in the Wi-Fi Protected Setup (WPS) standard, communicates between two NFC Devices or between an NFC device And an NFC Tag via magnetic field induction, where two loop antennas are located within each other's near field, effectively energizing a wireless contact by forming an air-core transformer. An example NFC radio operates within the unlicensed radio frequency ISM band of 13.56 MHz, with a bandwidth of approximately 2 MHz over a typical distance of a few centimeters. The NFC radio may be affixed to a new wireless client device (STA) and the user brings the NFC radio on the device close to an access point (AP) or Registrar of the Network to allow near field communication between the devices.

[0075] NFC technology is an extension of the ISO/IEC 14443 proximity-card standard (incorporated herein by reference) for contactless smartcards and radio frequency ID (RFID) devices, which combines the interface of a contactless smartcard and a reader into a single device, and uses the ISO/IEC 18092 NFC communication standard (incorporated herein by reference) to enable two-way communication. An NFC radio may communicate with both existing ISO/IEC 14443 contactless smartcards and readers, as well as with other NFC devices by using ISO/IEC 18092. The NFC Forum™, a non-profit industry association, has released specifications that enable different operation modes called: tag emulation, read/write mode, and peer to peer communication. Furthermore, NFC Forum has defined specifications for NFC Data Exchange Format (NDEF), NFC Tag Types, NFC Record Type Definition, and Connection Handover Specification. See, for example, Connection Handover Technical Specification, NFC Forum™, Connection Handover 1.2, NFCForum_1.2, 2010-07-07 (incorporated herein by reference). The ISO/IEC 18092 standard defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductively coupled devices operating at the center frequency of 13,56 MHz for interconnection of computer peripherals. The ISO/IEC 18092 standard specifies modulation schemes, codings, transfer speeds and frame format of the RF interface, initialization schemes, conditions required for data collision control during initialization, and a transport protocol including protocol activation and data exchange methods.

[0076] The basic handover to a WLAN carrier stores WLAN parameters and credentials on NFC Forum Tags as part of Wi-Fi Protected Setup (WPS). The information is stored in the payload of an NFC Data Exchange Format (NDEF) record identified by the mime-type "application/vnd.wfa.wsc", known as the "WPS Record". The wireless LAN parameters and credentials information provided inside a WPS Record includes the IEEE 802.11 Service Set Identifier (SSID), authentication and encryption type deployed by the wireless network, the secret network key that a wireless station needs to authenticate with the network, and the MAC address of the device receiving the configuration (if unknown, this address is set to all-zeros). The Wi-Fi Protected Setup specification 1.0 uses the term "Registrar" for a device that is able to provide WLAN credentials and "Enrollee" for a device

Samsung Ex. 1004, Page 490 of 563

that wants to join a wireless network.

[0077] In the Wi-Fi Simple Configuration Specification, Version 2.0, December 20, 2010, a Handover Requester with Wi-Fi capability may format an NFC Handover Request Message in the NFC Data Exchange Format (NDEF), which indicates that the requester is an IEEE 802.11 device, but which does not include any configuration information. A Handover Request may be sent via the NFC link in at least two scenarios: [1] the requester may not have yet joined a wireless domain or [2] even if the requester is already member of a WLAN network, a peer device may be in a different network and thus a Connection Handover is required to obtain the peer device's credentials. In the Wi-Fi Protected Setup specification 2.0, the Handover Selector would deduce from this message that the Handover Requester supports a Wi-Fi certified IEEE 802.11 radio. In the Wi-Fi Protected Setup specification 2.0, if the Handover Selector is a Wi-Fi device with wireless connectivity, it should respond with an NFC Handover Select Message in the NFC Data Exchange Format (NDEF), with a configuration record that includes credentials, such as network index, SSID, authentication type, encryption type, network key, and MAC address.

[0078] The NFC Data Exchange Format (NDEF) specification, NFC Forum Data Exchange Format (NDEF) Specification, NFC Forum™, 2006 (incorporated herein by reference), defines a common data format for NFC devices to exchange application or service specific data. An NDEF message is constructed of a number of NDEF records, with the first and the last record providing message begin and end markers. Between two NFC Devices, NDEF messages may be exchanged over the NFC Logical Link Control Protocol (LLCP) protocol, specified in NFC Forum Logical Link Control Protocol Specification, NFC Forum™, 2009 (incorporated herein by reference). The NFC Connection Handover specification, NFC Forum Connection Handover Specification, NFC Forum™, 2010-07-07 (incorporated herein by reference), defines the exchange of NDEF messages between two NFC Devices in a negotiated handover to discover and negotiate alternative wireless communication technologies.

[0079] The Handover Requester in the Wi-Fi Protected Setup specification 2.0, would then typically use the SSID and Network Key to enroll on the same Wi-Fi network to which the Handover Selector is connected. Further actions depend on the provision of an IP address identifying the Handover Selector, the available services, and the Handover Requester's intended activity.

E. Power Save Control For Tethering Connections

[0080] A hotspot may be a location that offers Internet access via one or more WLAN access points installed at the location. For example, stationary hotspots in coffee shops and other public places may offer free access to the Internet, up to a maximum number of users. A mobile hotspot may be a mobile telephone or smartphone that has WLAN communication capability and serves as a WLAN gateway to the cellular telephone network. The mobile hotspot enables other WLAN-capable devices that are tethered to the mobile hotspot, to relay their traffic via the WLAN connection and the cellular telephone network, to the Internet. The mobile hotspot may also relay traffic between tethered devices.

[0081] Setting up the WLAN tethering option in a smartphone may require assigning an SSID network name and passkey for the smartphone and the smartphone may automatically issue an IP address. Then, to connect another WLAN-capable device as a tethered device via a WLAN connection to the smartphone, the SSID, passkey, and IP address may need to be entered into the tethered device.

[0082] In accordance with an example embodiment of the invention, the configuration of the WLAN tethering connections with the SSID and passkeys may be automatically set up in a user friendly manner, so that that the user does not need to enter set up data into any other of the WLAN-capable devices.

[0083] WLAN tethering may consume significant power in a mobile hotspot device, since the device may need to stay active as a gateway device for other client devices, even if there is no ongoing data traffic or other client devices. Further, the mobile hotspot device may need to transmit beacons regularly to maintain connections, wasting the device's battery power.

[0084] In accordance with an example embodiment of the invention, to minimize power consumption in the mobile hotspot device, a control connection is initially established between the mobile hotspot device and the client wireless device using an out-of-band communications connection in an out-of-band communications medium, such as Bluetooth, Bluetooth Low Energy, or Near Field Communications. The mobile hotspot device and the client wireless device may then exchange over the control channel, in-band communications connectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and passkeys. The mobile hotspot device and the client wireless device may further exchange over the control channel, in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN. In this manner the mobile hotspot device A may relay communications between the wireless device B and a wide area communications network, such as a cellular telephone network, and enable WLAN power save features of the WLAN tethering connection. The mobile hotspot device A may also relay communications between devices connected to the mobile hotspot device.

[0085] Figure 1 is an example network diagram of a mobile wireless hotspot device A with its Bluetooth circuit 14A and the other wireless device B with its Bluetooth circuit 14B, exchanging information 50 that may be re-

Samsung Ex. 1004, Page 491 of 563

quired to create a Bluetooth control channel connection between the mobile hotspot device A and the wireless device B. The devices may exchange the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, in accordance with example embodiments of the invention. If the Bluetooth control channel connection setup requires authentication, link keys may be initially exchanged using a Near Field Communications link, for example, with an NFC Data Exchange Format (NDEF) configuration record that includes the link keys. As a result, setting up the WLAN tethering option in a smartphone and in tethered wireless devices may be performed as a part of the initial device set-up, requiring minimal user involvement.

[0086] The figure shows two stationary hotspot access points AP1 and AP2 at fixed locations, connected to the Internet 46. When the other wireless device B is within communication range of at least one of the stationary hotspot access points AP1 or AP2, it may use that stationary access point within range to access the Internet 46. If the other wireless device B moves beyond the communication range of any of the stationary hotspot access points AP1 and AP2, the other wireless device B may still be able to access the internet 46 by becoming tethered over a WLAN connection to the mobile hotspot device A. The mobile hotspot device A may serve as a WLAN gateway to the cellular base station 18, cellular telephone network 39, internet gateway 44, and Internet 46. The mobile hotspot device A may then relay the communications traffic of the other wireless device B, via the WLAN tethering connection between the devices A and B, and via the cellular telephone network 39 and internet gateway 44, to the Internet 39.

[0087] In another example embodiment of the invention, the devices may exchange the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, via the cellular telephone network connected to a server that provides this information.

[0088] Figure 1A is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1, establishing the Bluetooth control channel 52 between the Bluetooth circuit 14A and the Bluetooth circuit 14B, in accordance with example embodiments of the invention.

[0089] Figure 1B is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1A,

[0090] In accordance with an example embodiment of the invention, request message 54 may request a tethering connection requesting the mobile hotspot device A to relay communications between wireless device B, via cellular base station 18 and Internet 46, to either the social network server 36 or the other network server 37. Request message 54 may request a tethering connection requesting the mobile hotspot device A to relay communications between wireless device B, via cellular base station 18 and over one or more cellular wireless connections 19 to one or more wireless devices C. Request message 54 may request a tethering connection requesting the mobile hotspot device A to relay communications between wireless device B and over one or more WLAN connections 13 to one or more wireless devices D connected to the hotspot device A. The figure shows a second WLAN circuit 12' on the mobile hotspot device A, shown to clarify the description of the WLAN connection 13 to the wireless device D, however, the mobile hotspot device A may accomplish its WLAN communications with the single WLAN circuit 12.

[0091] In another example embodiment of the invention, the mobile hotspot device A may receive a request from the client wireless device D over a Bluetooth control channel between Bluetooth circuits 14D and 14A, for a WLAN tethering connection for relaying by the mobile hotspot device A, communications between the wireless device D and one or more entities in at least one of the cellular telephone network 18 and a wireless local area network provided by the mobile hotspot device A, in accordance with example embodiments of the invention.

[0092] Figure 1C is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1B, exchanging over the Bluetooth control channel 52, WLAN connectivity configuration information 56. The mobile hotspot device A and the client wireless device B may exchange over the control channel 52, by at least one of transmitting or receiving in-band communications connectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and passkeys, a required authentication procedure, the public key of the mobile hotspot device A, available data rates, available data throughput, a required site blacklist for virus protection, and the like.

[0093] In accordance with an example embodiment of the invention, the mobile hotspot device A and the wireless device B may further exchange over the Bluetooth control channel 52, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in the in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN. Example power saving features may include scheduled sleep and awake periods wherein both the mobile hotspot device A and the wireless device B observe substantially the same sleep and awake periods. Control information may also be exchanged to optimize the timing of the sleep and awake periods in the WLAN tethering connection, in accordance with example embodiments of the invention.

[0094] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may exchange over a Bluetooth control channel between Bluetooth circuits 14D and 14A, by at least one of transmitting or receiving in-band communications con-

nectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and passkeys, a required authentication procedure, the public key of the mobile hotspot device A, available data rates, available data throughput, a required site blacklist for virus protection, and the like. The mobile hotspot device A and the wireless device D may further exchange over the Bluetooth control channel between Bluetooth circuits 14D and 14A, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in the in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN, in accordance with example embodiments of the invention.

[0095] Figure 1D is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1C, establishing the WLAN tethering connection 58 between the WLAN circuit 12A of the mobile wireless hotspot A and the WLAN circuit 12B of the wireless device B. The figure shows the transitioning, by the mobile hotspot device A, from a WLAN idle state to a WLAN active state, using the power saving features and optimized activity times for the WLAN tethering connection 58, in response to receiving the request 54 over the Bluetooth control channel 52, in accordance with example embodiments of the invention.

[0096] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may establish a WLAN tethering connection between the WLAN circuit 12A' of the mobile wireless hotspot A and the WLAN circuit 12D of the wireless device B , in response to receiving the request over the Bluetooth control channel between Bluetooth circuits 14D and 14A, in accordance with example embodiments of the invention.

[0097] Figure 1E is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure ID, exchanging messages for adjustments 59 in the WLAN connectivity configuration information to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention. WLAN traffic 75 from the wireless device B is shown being relayed by the mobile hotspot device A from its cell phone circuit 18A as the relayed traffic 75' to the antenna 17 of the cellular base station 18. The cellular base station 18 passes the traffic on to the telephone network 39, and internet gateway 44 to the Internet 46, towards a destination server 36, in accordance with example embodiments of the invention. The destination server 36 may be a social network server connected to the Internet 46.

[0098] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may exchange over a Bluetooth control channel between Bluetooth circuits 14D and 14A, messages for adjustments in the WLAN connectivity configuration information to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection between the WLAN circuit 12A' of the mobile wireless hotspot A and the WLAN circuit 12D of the wireless device B, in accordance with example embodiments of the invention.

[0099] Figure 1F is an example network diagram of the mobile wireless hotspot device A of Figure 1E, transitioning from the WLAN active state to the WLAN idle state of the WLAN tethering connection, when no requests are received from any wireless device, for a WLAN tethering connection for relaying by the mobile hotspot device A, communications between the any wireless device and the cellular telephone network 18, in accordance with example embodiments of the invention.

[0100] Figure 1G is an example flow diagram 100 of the operation of the mobile hot spot device A, wherein tethering is active in step 102 until here are no active clients as determined in step 104. If there are no active clients, then the mobile hot spot A goes into the idle state in step 106 and may check that its Bluetooth control radio 14A is turned on and that all connected clients support the power save feature. After receiving a tethering request from a client in step 108, the mobile hot spot A turns on mobile tethering in s102 and may also inform the client that it is up and running, in accordance with example embodiments of the invention.

[0101] Figure 2A is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging adjustments 59 in the WLAN connectivity configuration information over the Bluetooth control channel 52, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention.

[0102] In accordance with an embodiment of the invention, mobile hotspot device A further includes an NFC reader/writer 16A, a Bluetooth transceiver 14A, a IEEE 802.11 WLAN transceiver 12A, and a cellular telephone transceiver 18A. The cellular telephone transceiver 18A may be based on Wide Area (WAN) communications protocols that include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0103] In an example embodiment of the invention, the mobile hotspot device A may be a device having an overall function as a PDA, cell phone, laptop or palmtop computer, or the like. The mobile hotspot device A includes a processor 20 that includes a single core, dual core or multi-core central processing unit (CPU_1 and CPU_2), a random access memory (RAM), a read only memory (ROM), and interface circuits to interface with circuits, such as a cell phone radio, a battery and other power sources, key pad, touch screen, display, microphone, speakers, ear pieces, camera or other imaging devices, etc. in the device A. The RAM and ROM may be remov-

able memory devices 126 such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, flash memory devices, etc., as shown in Figure 4. The IEEE 802.11 MAC and PHY 12A, provide the medium access control and radio for IEEE 802.11 WLAN communications. The mobile hotspot device A may include a user interface such as a key pad and a location detection device such as the global positioning system (GPS). Device A may measure its location by the GPS, by cellular telephone Cell-ID sensed by the wide area wireless transceiver 18A, or by WLAN signals sensed by the IEEE 801.11 transceiver 12A, for example. With reference to Figure 2B, the other wireless device B has similar components to mobile hotspot device A in Figure 2A.

[0104] In an example embodiment of the invention, the mobile hotspot device A may include the connectivity management system 28A, to read device capabilities of the mobile hotspot device A. The connectivity management system 28A may generate the user specific device connectivity configurations to enable the other wireless device B, to automatically connect to the mobile hotspot device A as a tethered wireless device, the connectivity configurations including a specification of a WLAN tethering connection having a network name (SSID) and passkey.

[0105] Figure 2B is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 2A, exchanging adjustments 59' in the WLAN connectivity configuration information over the Near Field Communications (NFC) control channel via the NFC reader/writer 16A and NFC reader/writer 16B, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention. In an example embodiment of the invention, the mobile wireless hotspot device A and the other wireless device B of Figure 2A, may exchange adjustments 59' in the WLAN connectivity configuration information over another local connectivity channel having low power.

[0106] In an example embodiment of the invention, the connectivity management system 28A in the mobile hotspot device A, may read device capabilities mobile hotspot device A. The connectivity management system 28A may generate user specific device connectivity configurations to enable a other wireless device B, to automatically connect to the mobile hotspot device A as a tethered wireless device, the connectivity configurations including specification of a WLAN tethering connection having a network name and passkey. The connectivity management system 28A may receive from the other wireless device B, a WLAN tethering connection request based on the user specific device connectivity configurations.

[0107] In an example embodiment of the invention, the other wireless device B may exchange information directly with the mobile hotspot device A via a short range communications link, such as the Bluetooth (or Bluetooth Low Energy) circuits 14A and 14B or the Near Field Communications (NFC) reader/writer circuits 16A and 16B.

[0108] Figure 3A is an example flow diagram 300 of the process performed by mobile hotspot device A, in accordance with example embodiments of the invention. The steps of the flow diagram represent computer code instructions stored in the RAM and/or ROM memory of the mobile hotspot device A, which when executed by the central processing units (CPU), carry out the functions of the example embodiments of the invention. The steps may be carried out in another order than shown and individual steps may be combined or separated into component steps. Additional steps may be included in this sequence. The steps of the example method are as follows.

[0109] Step 302: establishing, by a mobile hotspot device, a control channel with a wireless device, using an out-of-band communications connection in an out-of-band communications medium; and

[0110] Step 304: exchanging, by the mobile hotspot device over the control channel, with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, for relaying by the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network and a wireless local area network provided by the mobile hotspot device.

[0111] Figure 3B is an example flow diagram 350 of the process performed by the other wireless device B, in accordance with example embodiments of the invention. The steps of the flow diagram represent computer code instructions stored in the RAM and/or ROM memory of the other wireless device B, which when executed by the central processing units (CPU), carry out the functions of the example embodiments of the invention. The steps may be carried out in another order than shown and individual steps may be combined or separated into component steps. Additional steps may be included in this sequence. The steps of the example method are as follows.

[0112] Step 352: establishing, by a wireless device, a control channel with a mobile hotspot device, using an out-of-band communications connection in an out-of-band communications medium; and

[0113] Step 354: exchanging, by the wireless device over the control channel, with the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the mobile hotspot device in an in-band communications medium, for relaying by the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications

Samsung Ex. 1004, Page 494 of 563

network and a wireless local area network provided by the mobile hotspot device.

[0114] Figure 4 illustrates an example embodiment of the invention, wherein examples of removable storage media 126 are shown, based on magnetic, electronic and/or optical technologies, such as magnetic disks, optical disks, semiconductor memory circuit devices and micro-SD memory cards (SD refers to the Secure Digital standard) for storing data and/or computer program code as an example computer program product, in accordance with at least one embodiment of the present invention.

[0115] In an alternate example embodiment of the invention, RFID transponders may be used in devices A and B, which may be the passive type or the active type, instead of the NFC transponders. A passive RFID transponder requires no internal power source to communicate with an RFID reader, and is only active when it is near an RFID reader that energizes the transponder with a continuous radio frequency signal at a resonant frequency of the antenna. The small electrical current induced in the antenna by the continuous radio frequency signal provides enough power for an integrated circuit in the transponder to power up and transmit a modulated response, typically by backscattering the continuous carrier wave from the RFID reader. A passive RFID transponder may include writable electrically erasable, programmable, read-only memory (EEPROM) for storing data received from the RFID reader, which modulates the continuous carrier wave sent by the RFID reader. Reading distances for passive RFID transponders typically range from a few centimeters to a few meters, depending on the radio frequency and antenna design. By contrast, active RFID transponders require a power source to receive and transmit information with an RFID reader. The RFID transponder may be affixed to or integrated with the wireless device A and device B and the user brings the RFID transponder on the device A close to an RFID reader circuit in device B to allow near field communication between the devices. In example embodiments, both devices A and B may have RFID reader circuits to read RFID signals from the other device.

[0116] In an example embodiment, the wireless transceiver carrier in device A and device B may be a suitable short-range communications protocol, such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Infrared Data Association (IrDA), or Ultra Wide Band (UWB), for example.

[0117] An example of the Radio Frequency Identification (RFID) out-of-band short-range carrier is described, for example, ISO 11785 (air interface protocol), ISO 14443 (air interface protocol), and ISO 15693, incorporated herein by reference.

[0118] An example of the Near Field Communication (NFC) out-of-band short-range carrier is described, for example, in ISO/IEC 14443 and ISO/IEC 18092, incorporated herein by reference.

[0119] An example of the Infrared Data Association (IrDA) out-of-band short-range carrier is described, for example, in IrDA Link Access Protocol, v1.1 (1996), incorporated herein by reference.

[0120] An example of the Ultra Wide Band (UWB) out-of-band short-range carrier is described, for example, in WiMedia Common Radio Platform Specification, Version 1.5 (2010), incorporated herein by reference.

[0121] In example embodiments, the wireless transceiver carrier in device A and device B may be a suitable communications protocol, such as a Vehicle Area (WVAN) communications protocol, Wireless Video Networks (WVAN-TV) communications protocol, Personal Area (WPAN) communications protocol, Local Area (WLAN) communications protocol, or Wide Area (WAN) communications protocol, using the standard procedures and primitives defined by the respective standards. Personal Area (WPAN) communications protocols include Bluetooth BR/EDR, Bluetooth Low Energy, Wireless USB (WUSB), Ultra Wide-band (UWB), ZigBee (IEEE 802.15.4, or IEEE 802.15.4a) for short range communication between devices. Local Area (WLAN) communications protocols include IEEE 802.11, digital enhanced cordless telecommunications (DECT) and HIPERLAN. Wide Area (WAN) communications protocols include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0122] Using the description provided herein, the embodiments may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0123] Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media such as resident memory devices, smart cards or other removable memory devices, or transmitting devices, thereby making a computer program product or article of manufacture according to the embodiments. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program.

[0124] As indicated above, memory/storage devices include, but are not limited to, disks, optical disks, removable memory devices such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, etc. Transmitting mediums include, but are not limited to, transmissions via wireless communication networks, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links.

[0125] Although specific example embodiments have been disclosed, a person skilled in the art will understand

Samsung Ex. 1004, Page 495 of 563

that changes can be made to the specific example embodiments without departing from the scope of the invention.

[0126] An example of the Infrared Data Association (IrDA) out-of-band short-range carrier is described, for example, in IrDA Link Access Protocol, v1.1 (1996), incorporated herein by reference.

[0127] An example of the Ultra Wide Band (UWB) out-of-band short-range carrier is described, for example, in WiMedia Common Radio Platform Specification, Version 1.5 (2010), incorporated herein by reference.

[0128] In example embodiments, the wireless transceiver carrier in device A and device B may be a suitable communications protocol, such as a Vehicle Area (WVAN) communications protocol, Wireless Video Networks (WVAN-TV) communications protocol, Personal Area (WPAN) communications protocol, Local Area (WLAN) communications protocol, or Wide Area (WAN) communications protocol, using the standard procedures and primitives defined by the respective standards. Personal Area (WPAN) communications protocols include Bluetooth BR/EDR, Bluetooth Low Energy, Wireless USB (WUSB), Ultra Wide-band (UWB), ZigBee (IEEE 802.15.4, or IEEE 802.15.4a) for short range communication between devices. Local Area (WLAN) communications protocols include IEEE 802.11, digital enhanced cordless telecommunications (DECT) and HIPERLAN. Wide Area (WAN) communications protocols include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0129] Using the description provided herein, the embodiments may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0130] Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media such as resident memory devices, smart cards or other removable memory devices, or transmitting devices, thereby making a computer program product or article of manufacture according to the embodiments. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program.

[0131] As indicated above, memory/storage devices include, but are not limited to, disks, optical disks, removable memory devices such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, etc. Transmitting mediums include, but are not limited to, transmissions via wireless communication networks, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links.

[0132] Although specific example embodiments have been disclosed, a person skilled in the art will understand that changes can be made to the specific example embodiments without departing from the scope of the invention.

Claims

1. A method, comprising:

establishing (302), by an apparatus operating as a mobile hotspot device, a control channel (52) over a wireless out-of-band communications medium with a wireless device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

exchanging (304), by the apparatus operating as the mobile hotspot device, over the established control channel (52), by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network (39,46) and/or a wireless local area network provided by the apparatus operating as the mobile hotspot device.

2. The method of claim 1, further comprising:

receiving, by the apparatus operating as the mobile hotspot device, over the control channel (52), a request from the wireless device for the in-band communications tethering connection (58) for relaying, by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of the wide area communications network (39,46) and/or the wireless local area network provided by the apparatus operating as the mobile hotspot device;

performing, by the apparatus operating as the mobile hotspot device, said exchanging over the control channel (52), with the wireless device, of the in-band communications connectivity configuration information, in response to receiving

Samsung Ex. 1004, Page 496 of 563

the request; and
transitioning, by the apparatus operating as the mobile hotspot device, from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection (58), in response to receiving the request.

3. The method of claim 1 or claim 2, further comprising:
exchanging, by the apparatus operating as the mobile hotspot device, over the control channel, with the wireless device, adjustments (59,59') in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection (58) with the wireless device.

4. The method of any of the preceding claims, further comprising:
transitioning, by the apparatus operating as the mobile hotspot device, from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection (58), when no requests are received from any wireless device for the in-band communications tethering connection.

5. The method of any of the preceding claims, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.

6. A method, comprising:

establishing (352), by a wireless device, a control channel (52) over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and
exchanging (354), by the wireless device over the control channel (52), with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device in an in-band communications medium.

7. The method of claim 6, further comprising:

transmitting, by the wireless device, over the control channel (52), a request to the apparatus operating as the mobile hotspot device for the in-band communications tethering connection (58);
performing, by the wireless device, said exchanging over the control channel (52), with the apparatus operating as the mobile hotspot device, of the in-band communications connectivity configuration information; and
establishing, by the wireless device, the in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device, using the power saving features and optimized activity times for the in-band communications tethering connection.

8. A computer program comprising computer readable program code configured to cause performing of the method of any of the preceding claims when said program is run on a computer.

9. The computer program product of claim 8, wherein the computer program is a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

10. An apparatus operable as a mobile hotspot device, comprising:

means (14A) for establishing a control channel (52) over a wireless out-of-band communications medium with a wireless device, wherein said means for establishing the control channel with the wireless device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and
means (14A) for exchanging over the control channel (52), with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of a wide area communications network (39,46) and/or a wireless local area network provided by the apparatus.

11. The apparatus of claim 10, further comprising:

Samsung Ex. 1004, Page 497 of 563

means (14A) for receiving over the control channel (52), a request from the wireless device for the in-band communications tethering connection (58) for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of the wide area communications network (39,46) and/or the wireless local area network provided by the apparatus;

means (14A) for performing said exchanging over the control channel (52), with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and

means (12A,20) for transitioning from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection (58), in response to receiving the request.

12. The apparatus of claim 10 or claim 11, further comprising:
means (14A) for exchanging over the control channel (52), with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection (58) with the wireless device.

13. The apparatus of any of the claims 10-12, further comprising:
means (12A,20) for transitioning from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection (58), when no requests are received from any wireless device, for an in-band communications tethering connection.

14. The apparatus of any of the claims 10-13, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.

15. An apparatus, comprising:

means (14B) for establishing a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said means for establishing the control channel with the apparatus operating as the mobile hotspot device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

means (14B) for exchanging over the control channel (52), with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device in an in-band communications medium.

Patentansprüche

1. Verfahren, umfassend:

Einrichten (302), durch ein Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einer drahtlosen Vorrichtung, wobei das Einrichten des Steuerkanals mit dem drahtlosen Medium umfasst, über das drahtlose Außerbandkommunikationsmedium, zumindest Außerband-Paarungsinformationen oder geteilte geheime Informationen auszutauschen; und

Austauschen (304), durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den eingerichteten Steuerkanal (52) durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung in einem Inbandkommunikationsmedium zu optimieren, um Kommunikationen durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem eines Weitbereichskommunikationsnetzwerks (39, 46) und/oder eines drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, weiterzuleiten.

2. Verfahren nach Anspruch 1, ferner umfassend:

Empfangen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den Steuerkanal (52), einer Anforderung, von der drahtlosen Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) zum Weiterleiten, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von Kommunikationen zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens ei-

Samsung Ex. 1004, Page 498 of 563

nem des Weitbereichskommunikationsnetzwerks (39, 46) und/oder des drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird;
Durchführen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, des Austauschens, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen als Reaktion auf Empfangen der Anforderung; und
Übergehen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von einem Inbandkommunikation-Ruhezustand zu einem Inbandkommunikation-Aktivzustand unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung (58) als Reaktion auf Empfangen der Anforderung.

3. Verfahren nach Anspruch 1 oder Anspruch 2, ferner umfassend:
Austauschen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den Steuerkanal mit der drahtlosen Vorrichtung, von Anpassungen (59, 59') in den Inbandkommunikation-Konnektivitätskonfiguration-Informationen zum Modifizieren mindestens eines der Leistungssparmerkmale und der optimierten Aktivitätszeiten in der Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung.

4. Verfahren nach einem der vorhergehenden Ansprüche, ferner umfassend:
Übergehen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von dem Inbandkommunikation-Aktivzustand zu dem Inbandkommunikation-Ruhezustand der Inbandkommunikation-Anbindungsverbindung (58), wenn keine Anforderungen, von einer drahtlosen Vorrichtung, für die Inbandkommunikation-Anbindungsverbindung empfangen werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Außerbandkommunikationsmedium ein Bluetooth-Kommunikationsprotokoll oder ein Bluetooth-Low-Energy-Kommunikationsprotokoll umfasst und das Inbandkommunikationsmedium ein IEEE 802.11-Kommunikationsprotokoll umfasst.

6. Verfahren, umfassend:

Einrichten (352), durch eine drahtlose Vorrichtung, eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einem Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, wobei das Einrichten des Steuerkanals mit der drahtlosen Vorrichtung umfasst, über das drahtlose Außerbandkommunikationsmedium, zumindest Außerband-Paarungsinformationen oder geteilte geheime Informationen auszutauschen; und
Austauschen (354), durch die drahtlose Vorrichtung, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, in einem Inbandkommunikationsmedium zu optimieren.

7. Verfahren nach Anspruch 6, ferner umfassend:

Übertragen, durch die drahtlose Vorrichtung, über den Steuerkanal (52), einer Anforderung, an das Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, für die Inbandkommunikation-Anbindungsverbindung (58);
Durchführen, durch die drahtlose Vorrichtung, des Austauschens, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen; und
Einrichten, durch die drahtlose Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung.

8. Computerprogramm, umfassend computerlesbaren Programmcode, konfiguriert zum Bewirken, dass das Verfahren nach einem der vorstehenden Ansprüche durchgeführt wird, wenn das Programm auf einem Computer ausgeführt wird.

9. Computerprogrammprodukt nach Anspruch 8, wobei das Computerprogramm ein Computerprogrammprodukt ist, umfassend ein computerlesbares Medium, das Computerprogrammcode trägt, der darin für Verwendung mit einem Computer verkörpert ist.

10. Gerät, betreibbar als eine mobile Hotspot-Vorrichtung, umfassend:

Mittel (14A) zum Einrichten eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einer drahtlosen Vorrich-

Samsung Ex. 1004, Page 499 of 563

tung, wobei das Mittel zum Einrichten des Steuerkanals mit dem drahtlosen Medium Mittel zum Austauschen, über das drahtlose Außerbandkommunikationsmedium, von zumindest Außerband-Paarungsinformationen oder geteilten geheimen Informationen umfasst; und
Mittel (14A) zum Austauschen, über den Steuerkanal (52) mit der drahtlosen Vorrichtung durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung in einem Inbandkommunikationsmedium zu optimieren, um Kommunikationen durch das Gerät zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem eines Weitbereichskommunikationsnetzwerks (39, 46) und/oder eines drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, weiterzuleiten.

11. Gerät nach Anspruch 10, ferner umfassend:

Mittel (14A) zum Empfangen, über den Steuerkanal (52), einer Anforderung, von der drahtlosen Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) zum Weiterleiten, durch das Gerät, von Kommunikationen zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem des Weitbereichskommunikationsnetzwerks (39, 46) und/oder des drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät;
Mittel (14A) zum Durchführen des Austauschens, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen als Reaktion auf Empfangen der Anforderung; und
Mittel (12A, 20) zum Übergehen von einem Inbandkommunikation-Ruhezustand zu einem Inbandkommunikation-Aktivzustand unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung (58) als Reaktion auf Empfangen der Anforderung.

12. Gerät nach Anspruch 10 oder Anspruch 11, ferner umfassend:
Mittel (14A) zum Austauschen, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, von Anpassungen in den Inbandkommunikation-Konnektivitätskonfiguration-Informationen zum Modifizieren mindestens eines der Leistungssparmerkmale und der optimierten Aktivitätszeiten in der Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung.

13. Gerät nach einem der Ansprüche 10-12, ferner umfassend:
Mittel (12A, 20) zum Übergehen von dem Inbandkommunikation-Aktivzustand zu dem Inbandkommunikation-Ruhezustand der Inbandkommunikation-Anbindungsverbindung (58), wenn keine Anforderungen, von einer drahtlosen Vorrichtung, einer Inbandkommunikation-Anbindungsverbindung empfangen werden.

14. Gerät nach einem der Ansprüche 10-13, wobei das Außerbandkommunikationsmedium ein Bluetooth-Kommunikationsprotokoll oder ein Bluetooth-Low-Energy-Kommunikationsprotokoll umfasst und das Inbandkommunikationsmedium ein IEEE 802.11-Kommunikationsprotokoll umfasst.

15. Gerät, umfassend:

Mittel (14B) zum Einrichten eines Steuerkanals über ein drahtloses Außerbandkommunikationsmedium mit einem Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, wobei das Mittel zum Einrichten des Steuerkanals mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, Mittel zum Austauschen, über das drahtlose Außerbandkommunikationsmedium, von zumindest Außerband-Paarungsinformationen oder geteilten geheimen Informationen umfasst; und
Mittel (14B) zum Austauschen, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, in einem Inbandkommunikationsmedium zu optimieren.

Revendications

1. Procédé, comprenant les étapes suivantes :

établir (302), par un appareil fonctionnant comme dispositif de point d'accès mobile, un canal de commande (52) sur un support de communication hors bande sans fil avec un dispositif sans fil, où ledit établissement du canal de commande avec le dispositif sans fil comprend le fait d'échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et
échanger (304), par l'appareil fonctionnant com-

Samsung Ex. 1004, Page 500 of 563

me dispositif de point d'accès mobile sur le canal de commande établi (52), par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec le dispositif sans fil dans un support de communication dans la bande, pour relayer par l'appareil fonctionnant comme dispositif de point d'accès mobile, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi un réseau de communication étendu (39, 46) et un réseau local sans fil fourni par l'appareil fonctionnant comme dispositif de point d'accès mobile.

2. Procédé selon la revendication 1, comprenant en outre les étapes suivantes :

recevoir, par l'appareil fonctionnant comme dispositif de point d'accès mobile, sur le canal de commande (52), une demande provenant du dispositif sans fil pour la connexion de type modem de communication dans la bande (58) pour relayer, par l'appareil fonctionnant comme dispositif de point d'accès mobile, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi le réseau de communication étendu (39, 46) et le réseau local sans fil fourni par l'appareil fonctionnant comme dispositif de point d'accès mobile ;
procéder, par l'appareil fonctionnant comme dispositif de point d'accès mobile, audit échange sur le canal de commande (52), avec le dispositif sans fil, des informations de configuration de connectivité de communication dans la bande, en réponse à la réception de la demande ; et
effectuer une transition, par l'appareil fonctionnant comme dispositif de point d'accès mobile, d'un état de repos de communication dans la bande à un état actif de communication dans la bande utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande (58), en réponse à la réception de la demande.

3. Procédé selon la revendication 1 ou la revendication 2, comprenant en outre l'étape suivante :
échanger, par l'appareil fonctionnant comme dispositif de point d'accès mobile, sur le canal de commande, avec le dispositif sans fil, des ajustements (59, 59') dans les informations de configuration de connectivité de communication dans la bande pour modifier au moins un des éléments parmi les fonctionnalités d'économie d'énergie et les temps d'activité optimisés dans la connexion de type modem de communication dans la bande (58) avec le dispositif sans fil.

4. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre les étapes suivantes : effectuer une transition, par l'appareil fonctionnant comme dispositif de point d'accès mobile, de l'état actif de communication dans la bande à l'état de repos de communication dans la bande de la connexion de type modem de communication dans la bande (58), lorsqu'aucune demande n'est reçue d'un quelconque dispositif sans fil, pour la connexion de type modem de communication dans la bande.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le support de communication hors bande comprend un protocole de communication Bluetooth ou un protocole de communication Bluetooth à faible énergie, et le support de communication dans la bande comprend un protocole de communication IEEE 802.11.

6. Procédé, comprenant les étapes suivantes :

établir (352), par un dispositif sans fil, un canal de commande (52) sur un support de communication hors bande sans fil avec un appareil fonctionnant comme dispositif de point d'accès mobile, où ledit établissement du canal de commande avec le dispositif sans fil comprend le fait d'échanger, par l'intermédiaire du support de communication hors bande sans fil au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et
échanger (354), par le dispositif sans fil sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile dans un support de communication dans la bande.

7. Procédé selon la revendication 6, comprenant en outre les étapes suivantes :

transmettre, par le dispositif sans fil, sur le canal de commande (52), une demande à l'appareil fonctionnant comme dispositif de point d'accès mobile pour la connexion de type modem de

Samsung Ex. 1004, Page 501 of 563

communication dans la bande (58) ;
procéder, par le dispositif sans fil, audit échange sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, des informations de configuration de connectivité de communication dans la bande ; et
établir, par le dispositif sans fil, la connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile, en utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande.

8. Programme informatique comprenant un code de programme lisible par ordinateur configuré pour amener l'exécution du procédé selon l'une quelconque des revendications précédentes lorsque ledit programme est exécuté sur un ordinateur.

9. Produit programme informatique selon la revendication 8, dans lequel le programme informatique est un produit programme informatique comprenant un support lisible par ordinateur intégrant un code de programme informatique destiné à être utilisé avec un ordinateur.

10. Appareil pouvant fonctionner comme dispositif de point d'accès mobile, comprenant :

des moyens (14A) pour établir un canal de commande (52) sur un support de communication hors bande sans fil avec un dispositif sans fil, où lesdits moyens pour établir le canal de commande avec le dispositif sans fil comprennent des moyens pour échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et
des moyens (14A) pour échanger sur le canal de commande (52), avec le dispositif sans fil, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec le dispositif sans fil dans un support de communication dans la bande, pour relayer par l'appareil des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi un réseau de communication étendu (39, 46) et un réseau local sans fil fourni par l'appareil.

11. Appareil selon la revendication 10, comprenant en outre :

des moyens (14A) pour recevoir sur le canal de commande (52) une demande provenant du dispositif sans fil pour la connexion de type modem de communication dans la bande (58) pour relayer, par l'appareil, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi le réseau de communication étendu (39, 46) et le réseau local sans fil fourni par l'appareil ;
des moyens (14A) pour procéder audit échange sur le canal de commande (52), avec le dispositif sans fil, des informations de configuration de connectivité de communication dans la bande, en réponse à la réception de la demande ; et
des moyens (12A, 20) pour effectuer une transition d'un état de repos de communication dans la bande à un état actif de communication dans la bande en utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande (58), en réponse à la réception de la demande.

12. Appareil selon la revendication 10 ou la revendication 11, comprenant en outre :
des moyens (14A) pour échanger sur le canal de commande (52), avec le dispositif sans fil, des ajustements dans les informations de configuration de connectivité de communication dans la bande pour modifier au moins un des éléments parmi les fonctionnalités d'économie d'énergie et les temps d'activité optimisés dans la connexion de type modem de communication dans la bande (58) avec le dispositif sans fil.

13. Appareil selon l'une quelconque des revendications 10 à 12, comprenant en outre :
des moyens (12A, 20) pour effectuer une transition de l'état actif de communication dans la bande à l'état de repos de communication dans la bande de la connexion de type modem de communication dans la bande (58), lorsqu'aucune demande n'est reçue d'un quelconque dispositif sans fil, pour une connexion de type modem de communication dans la bande.

14. Appareil selon l'une quelconque des revendications 10 à 13, dans lequel le support de communication hors bande comprend un protocole de communication Bluetooth ou un protocole de communication Bluetooth à faible énergie, et le support de communication dans la bande comprend un protocole de communication IEEE 802.11.

15. Appareil comprenant :

Samsung Ex. 1004, Page 502 of 563

des moyens (14B) pour établir un canal de commande sur un support de communication hors bande sans fil avec un appareil fonctionnant comme dispositif de point d'accès mobile, où lesdits moyens pour établir le canal de commande avec l'appareil fonctionnant comme dispositif de point d'accès mobile comprennent des moyens pour échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et

des moyens (14B) pour échanger sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile dans un support de communication dans la bande.

Samsung Ex. 1004, Page 503 of 563

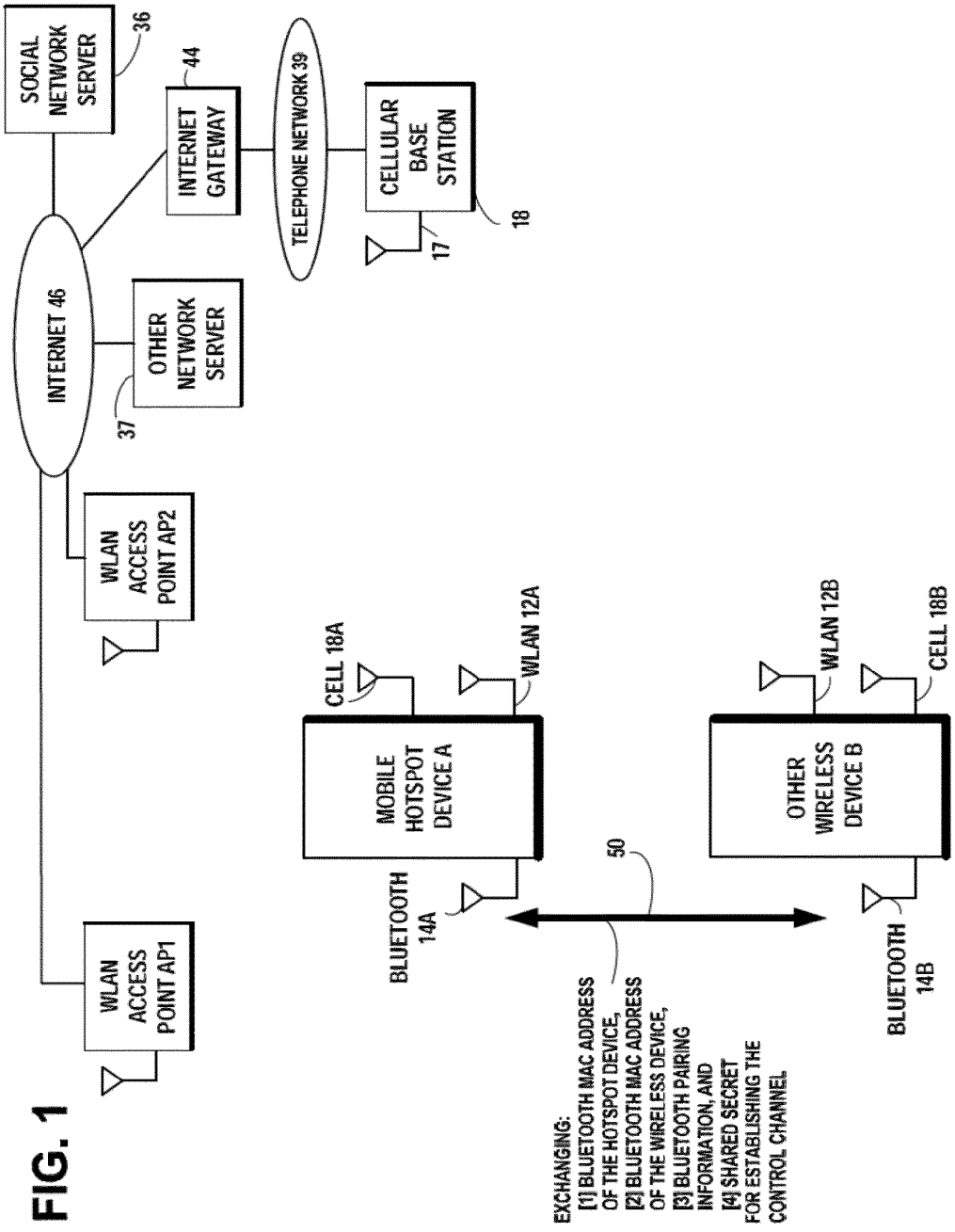

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
17
INTERNET 46
OTHER NETWORK SERVER
37
WLAN ACCESS POINT AP2
WLAN ACCESS POINT AP1
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
BLUETOOTH 14A
50
OTHER WIRELESS DEVICE B
WLAN 12B
CELL 18B
BLUETOOTH 14B
EXCHANGING:
[1] BLUETOOTH MAC ADDRESS OF THE HOTSPOT DEVICE,
[2] BLUETOOTH MAC ADDRESS OF THE WIRELESS DEVICE,
[3] BLUETOOTH PAIRING INFORMATION, AND
[4] SHARED SECRET
FOR ESTABLISHING THE CONTROL CHANNEL

FIG. 1

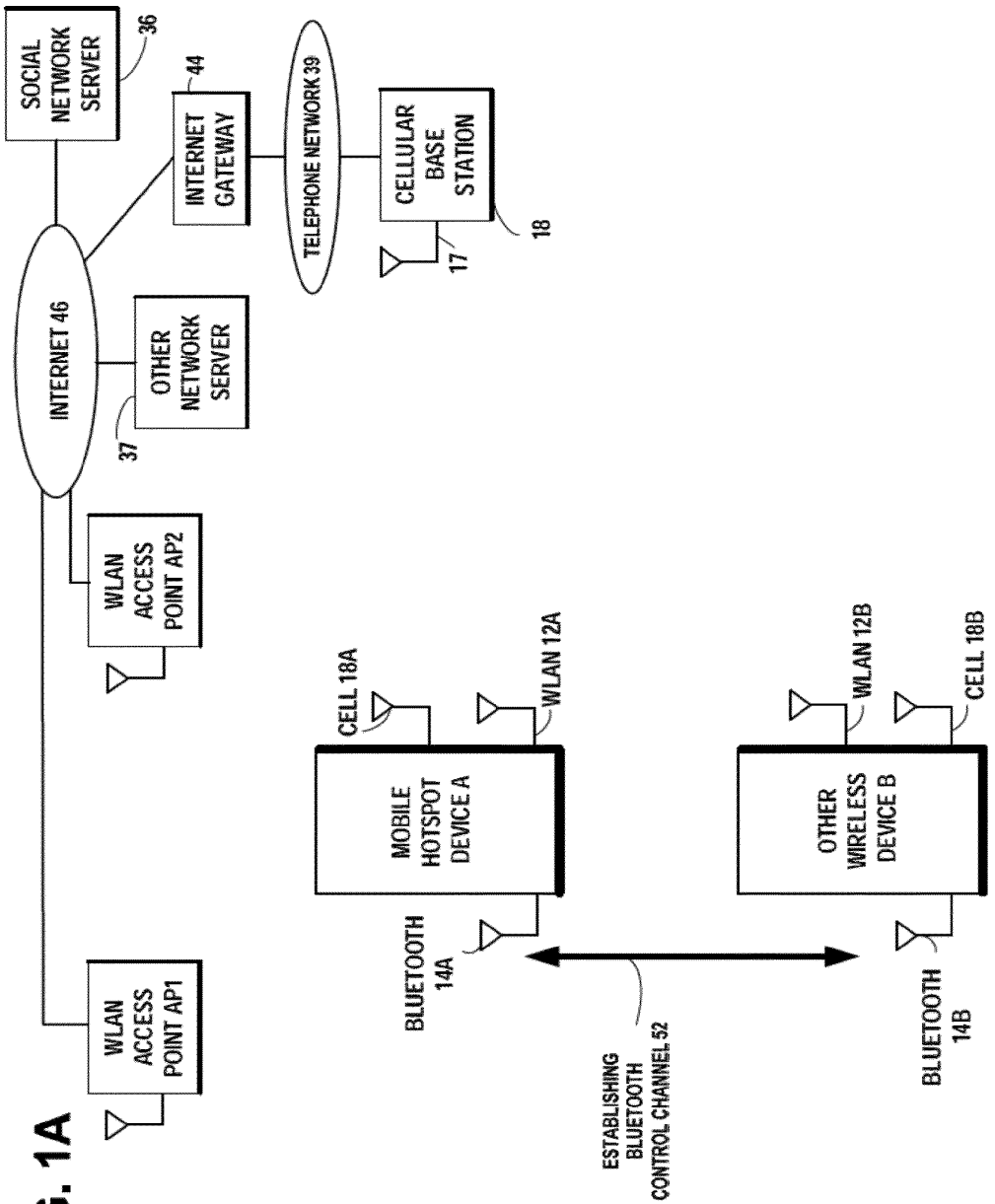

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
17
INTERNET 46
OTHER NETWORK SERVER
37
WLAN ACCESS POINT AP2
WLAN ACCESS POINT AP1
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
BLUETOOTH 14A
ESTABLISHING BLUETOOTH CONTROL CHANNEL 52
WLAN 12B
CELL 18B
OTHER WIRELESS DEVICE B
BLUETOOTH 14B

FIG. 1A

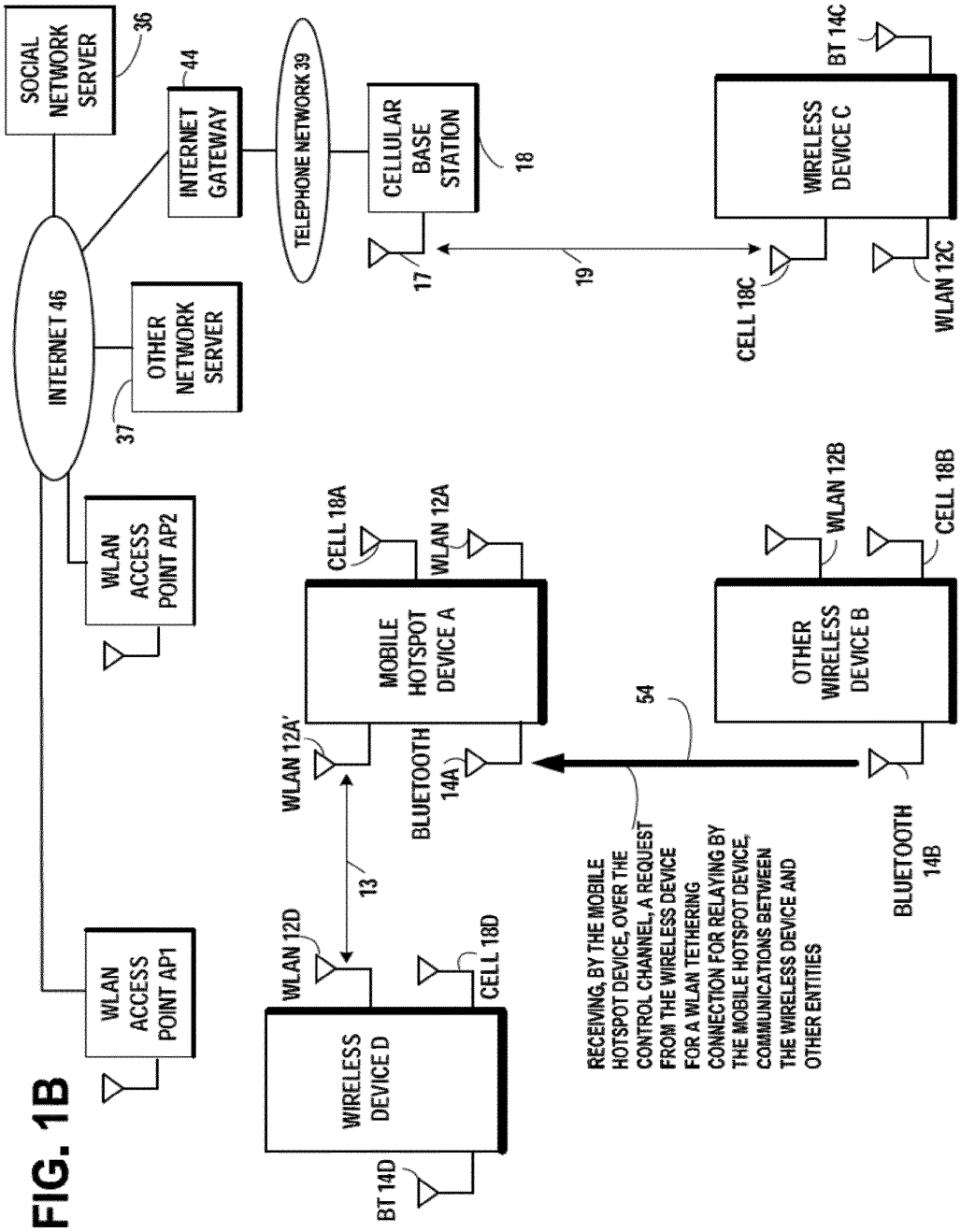

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
INTERNET 46
OTHER NETWORK SERVER
37
17
19
WIRELESS DEVICE C
BT 14C
CELL 18C
WLAN 12C
WLAN ACCESS POINT AP2
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
WLAN 12A'
BLUETOOTH 14A
54
OTHER WIRELESS DEVICE B
WLAN 12B
CELL 18B
BLUETOOTH 14B
WLAN ACCESS POINT AP1
WLAN 12D
13
CELL 18D
WIRELESS DEVICE D
BT 14D
RECEIVING, BY THE MOBILE HOTSPOT DEVICE, OVER THE CONTROL CHANNEL, A REQUEST FROM THE WIRELESS DEVICE FOR A WLAN TETHERING CONNECTION FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND OTHER ENTITIES

FIG. 1B

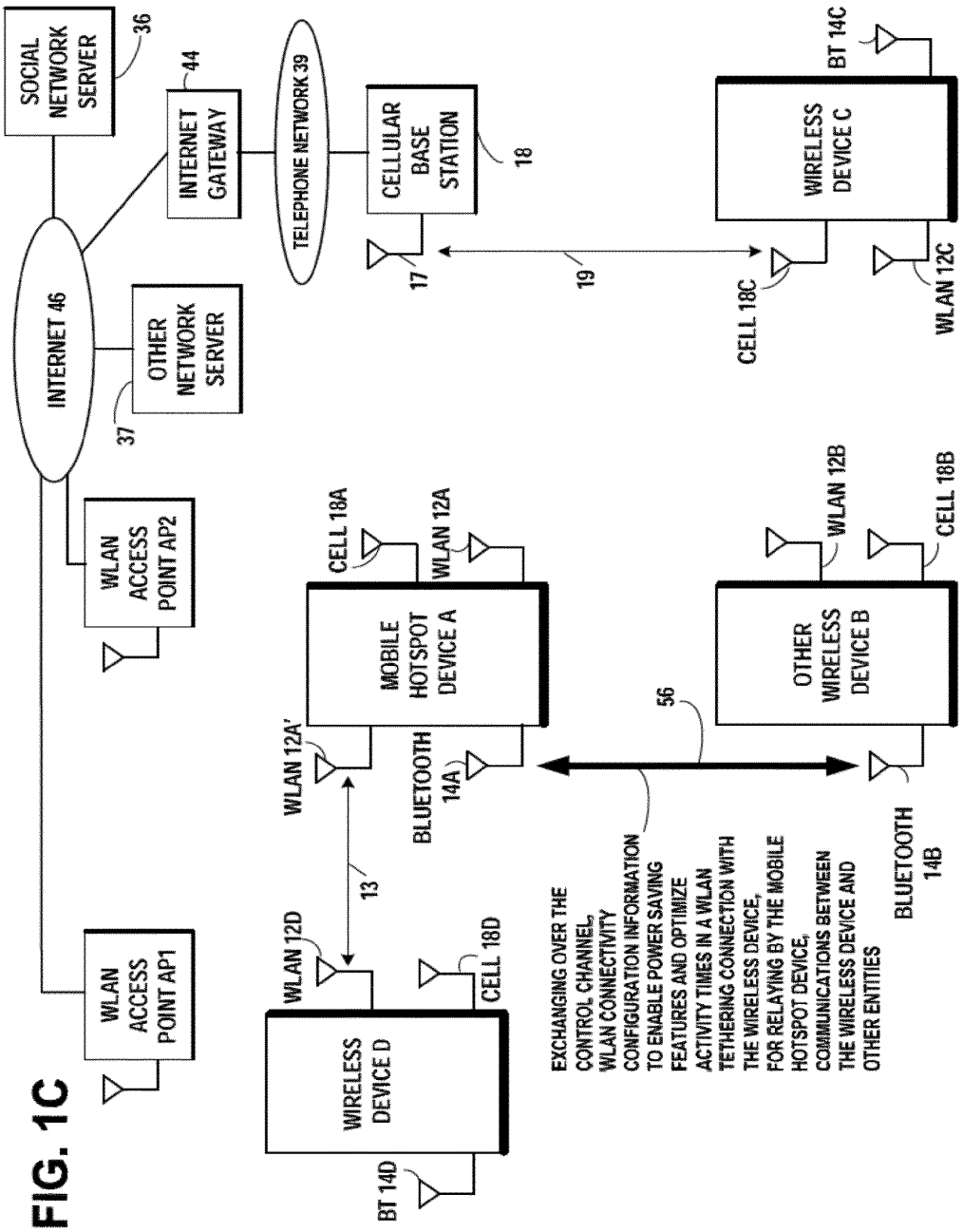

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
BT 14C
WIRELESS DEVICE C
INTERNET 46
OTHER NETWORK SERVER
37
17
19
CELL 18C
WLAN 12C
WLAN ACCESS POINT AP2
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
WLAN 12B
CELL 18B
OTHER WIRELESS DEVICE B
WLAN 12A'
BLUETOOTH 14A
56
WLAN ACCESS POINT AP1
WLAN 12D
13
CELL 18D
WIRELESS DEVICE D
BT 14D
BLUETOOTH 14B
EXCHANGING OVER THE CONTROL CHANNEL, WLAN CONNECTIVITY CONFIGURATION INFORMATION TO ENABLE POWER SAVING FEATURES AND OPTIMIZE ACTIVITY TIMES IN A WLAN TETHERING CONNECTION WITH THE WIRELESS DEVICE, FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND OTHER ENTITIES

FIG. 1C

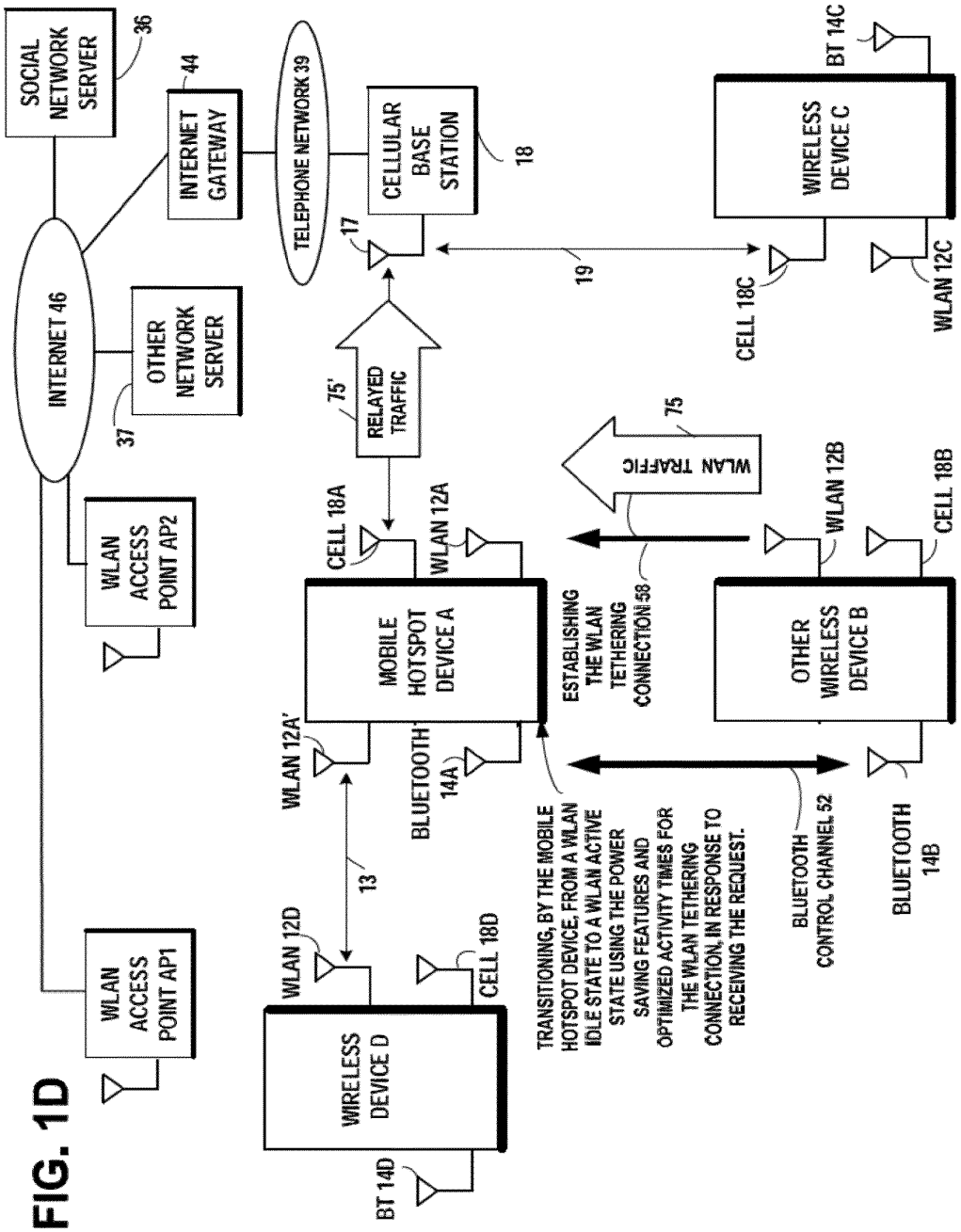

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
17
INTERNET 46
OTHER NETWORK SERVER
37
WLAN ACCESS POINT AP2
WLAN ACCESS POINT AP1
75'
RELAYED TRAFFIC
19
WIRELESS DEVICE C
BT 14C
CELL 18C
WLAN 12C
75
WLAN TRAFFIC
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
ESTABLISHING THE WLAN TETHERING CONNECTION 58
WLAN 12B
CELL 18B
OTHER WIRELESS DEVICE B
WLAN 12A'
BLUETOOTH 14A
13
WLAN 12D
CELL 18D
WIRELESS DEVICE D
BT 14D
TRANSITIONING, BY THE MOBILE HOTSPOT DEVICE, FROM A WLAN IDLE STATE TO A WLAN ACTIVE STATE USING THE POWER SAVING FEATURES AND OPTIMIZED ACTIVITY TIMES FOR THE WLAN TETHERING CONNECTION, IN RESPONSE TO RECEIVING THE REQUEST.
BLUETOOTH CONTROL CHANNEL 52
BLUETOOTH 14B

FIG. 1D

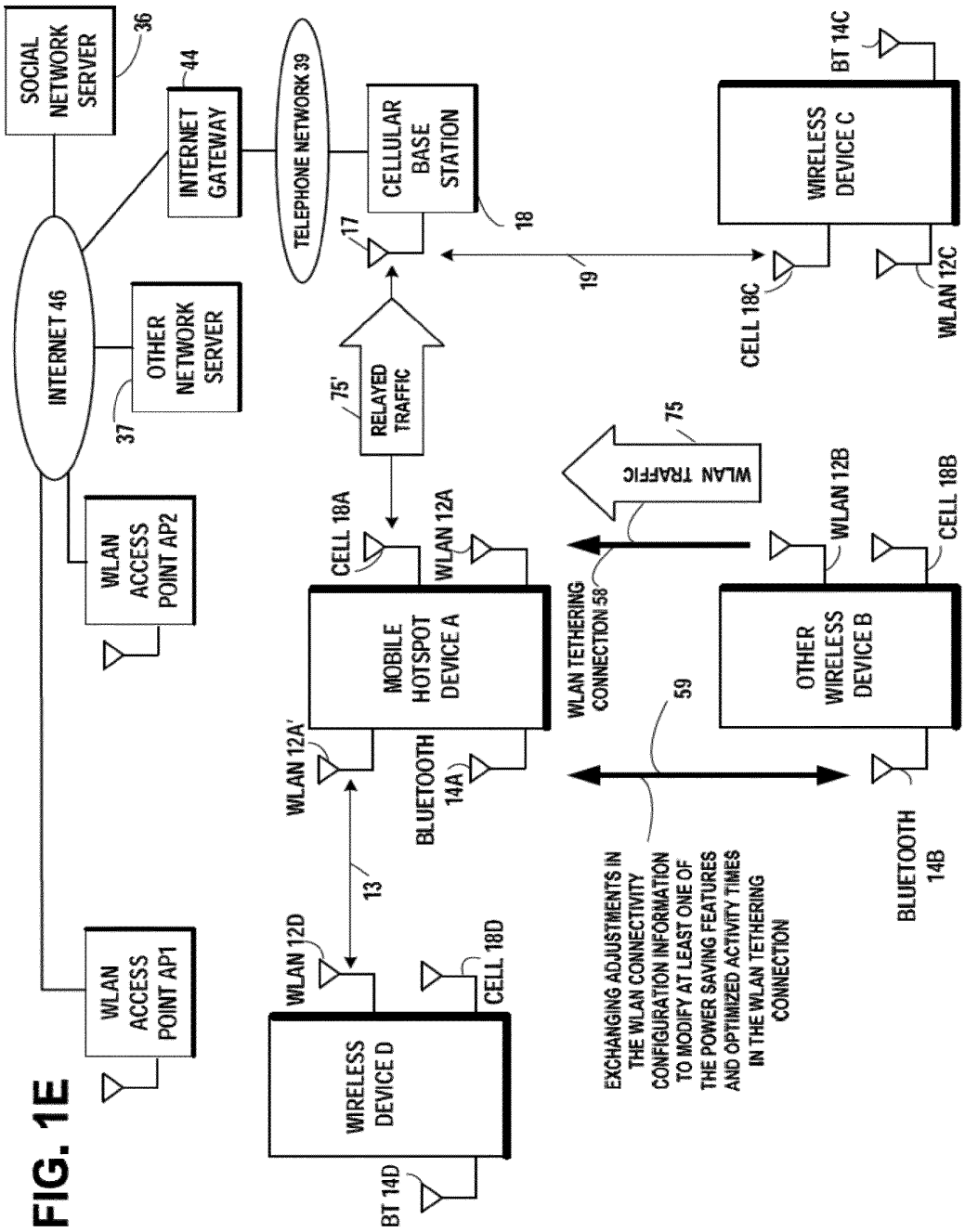

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
17
INTERNET 46
OTHER NETWORK SERVER
37
WLAN ACCESS POINT AP2
WLAN ACCESS POINT AP1
75'
RELAYED TRAFFIC
19
WIRELESS DEVICE C
BT 14C
CELL 18C
WLAN 12C
75
WLAN TRAFFIC
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
WLAN TETHERING CONNECTION 58
WLAN 12B
CELL 18B
OTHER WIRELESS DEVICE B
WLAN 12A'
BLUETOOTH 14A
59
13
WLAN 12D
CELL 18D
WIRELESS DEVICE D
BT 14D
BLUETOOTH 14B
EXCHANGING ADJUSTMENTS IN THE WLAN CONNECTIVITY CONFIGURATION INFORMATION TO MODIFY AT LEAST ONE OF THE POWER SAVING FEATURES AND OPTIMIZED ACTIVITY TIMES IN THE WLAN TETHERING CONNECTION

FIG. 1E

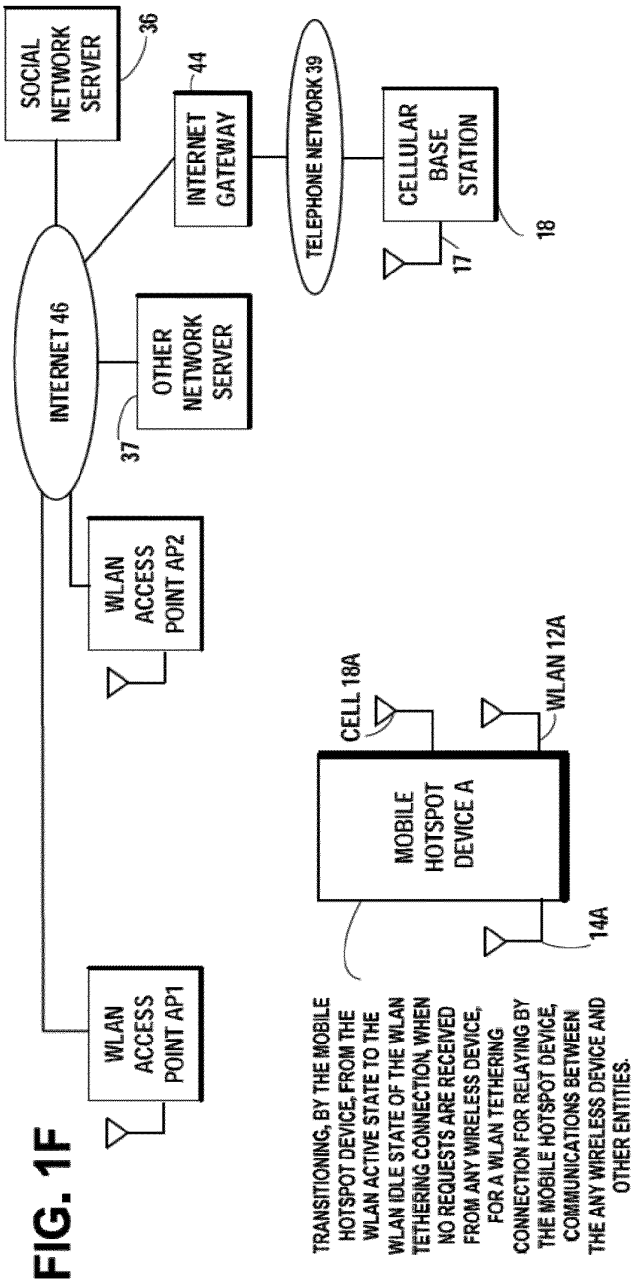

SOCIAL NETWORK SERVER
36
INTERNET GATEWAY
44
TELEPHONE NETWORK 39
CELLULAR BASE STATION
18
17
INTERNET 46
OTHER NETWORK SERVER
37
WLAN ACCESS POINT AP2
WLAN ACCESS POINT AP1
CELL 18A
WLAN 12A
MOBILE HOTSPOT DEVICE A
14A
TRANSITIONING, BY THE MOBILE HOTSPOT DEVICE, FROM THE WLAN ACTIVE STATE TO THE WLAN IDLE STATE OF THE WLAN TETHERING CONNECTION, WHEN NO REQUESTS ARE RECEIVED FROM ANY WIRELESS DEVICE, FOR A WLAN TETHERING CONNECTION FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE ANY WIRELESS DEVICE AND OTHER ENTITIES.

FIG. 1F

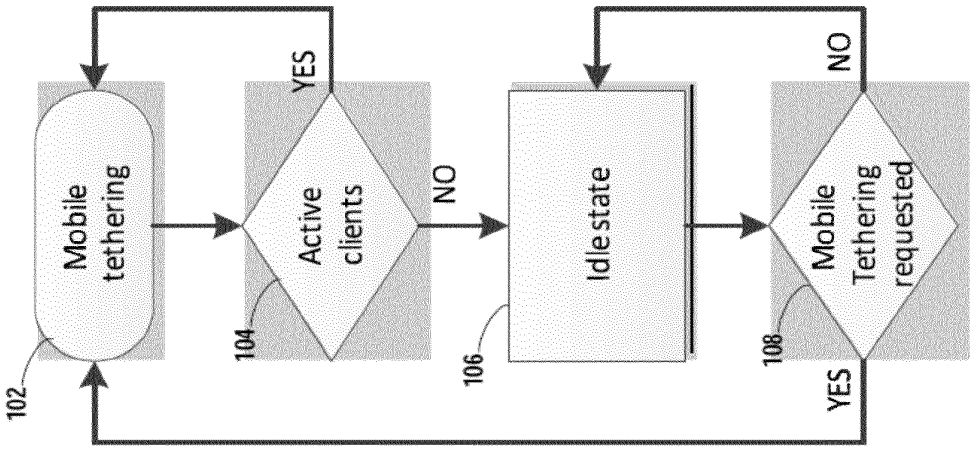

Mobile tethering
Active clients
YES
NO
Idle state
Mobile Tethering requested
NO
YES
102
104
106
108

FIG. 1G

100

FIG. 2A

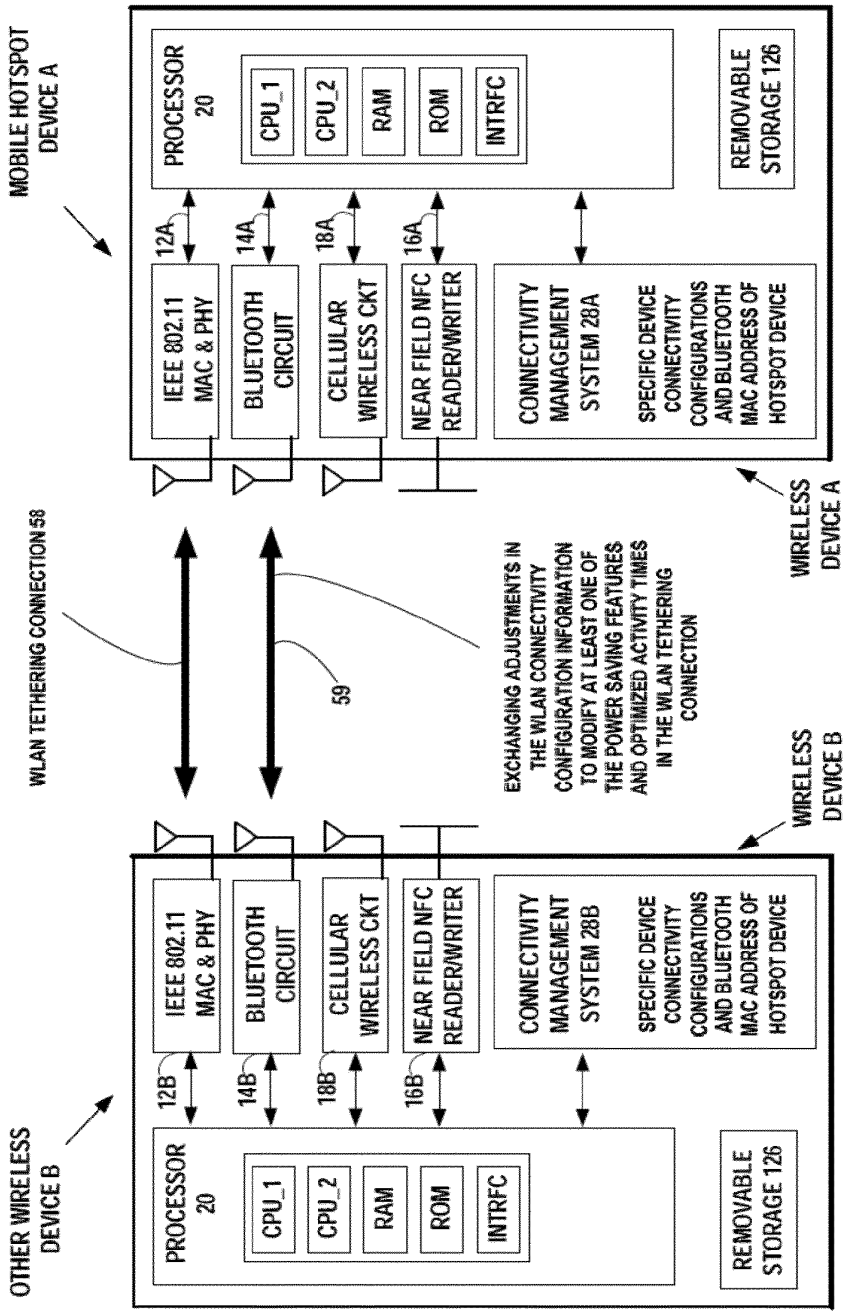

MOBILE HOTSPOT DEVICE A
PROCESSOR 20
CPU_1
CPU_2
RAM
ROM
INTRFC
REMOVABLE STORAGE 126
12A
14A
18A
16A
IEEE 802.11 MAC & PHY
BLUETOOTH CIRCUIT
CELLULAR WIRELESS CKT
NEAR FIELD NFC READER/WRITER
CONNECTIVITY MANAGEMENT SYSTEM 28A
SPECIFIC DEVICE CONNECTIVITY CONFIGURATIONS AND BLUETOOTH MAC ADDRESS OF HOTSPOT DEVICE
WIRELESS DEVICE A
WLAN TETHERING CONNECTION 58
59
EXCHANGING ADJUSTMENTS IN THE WLAN CONNECTIVITY CONFIGURATION INFORMATION TO MODIFY AT LEAST ONE OF THE POWER SAVING FEATURES AND OPTIMIZED ACTIVITY TIMES IN THE WLAN TETHERING CONNECTION
WIRELESS DEVICE B
OTHER WIRELESS DEVICE B
PROCESSOR 20
CPU_1
CPU_2
RAM
ROM
INTRFC
REMOVABLE STORAGE 126
12B
14B
18B
16B
IEEE 802.11 MAC & PHY
BLUETOOTH CIRCUIT
CELLULAR WIRELESS CKT
NEAR FIELD NFC READER/WRITER
CONNECTIVITY MANAGEMENT SYSTEM 28B
SPECIFIC DEVICE CONNECTIVITY CONFIGURATIONS AND BLUETOOTH MAC ADDRESS OF HOTSPOT DEVICE

FIG. 2B

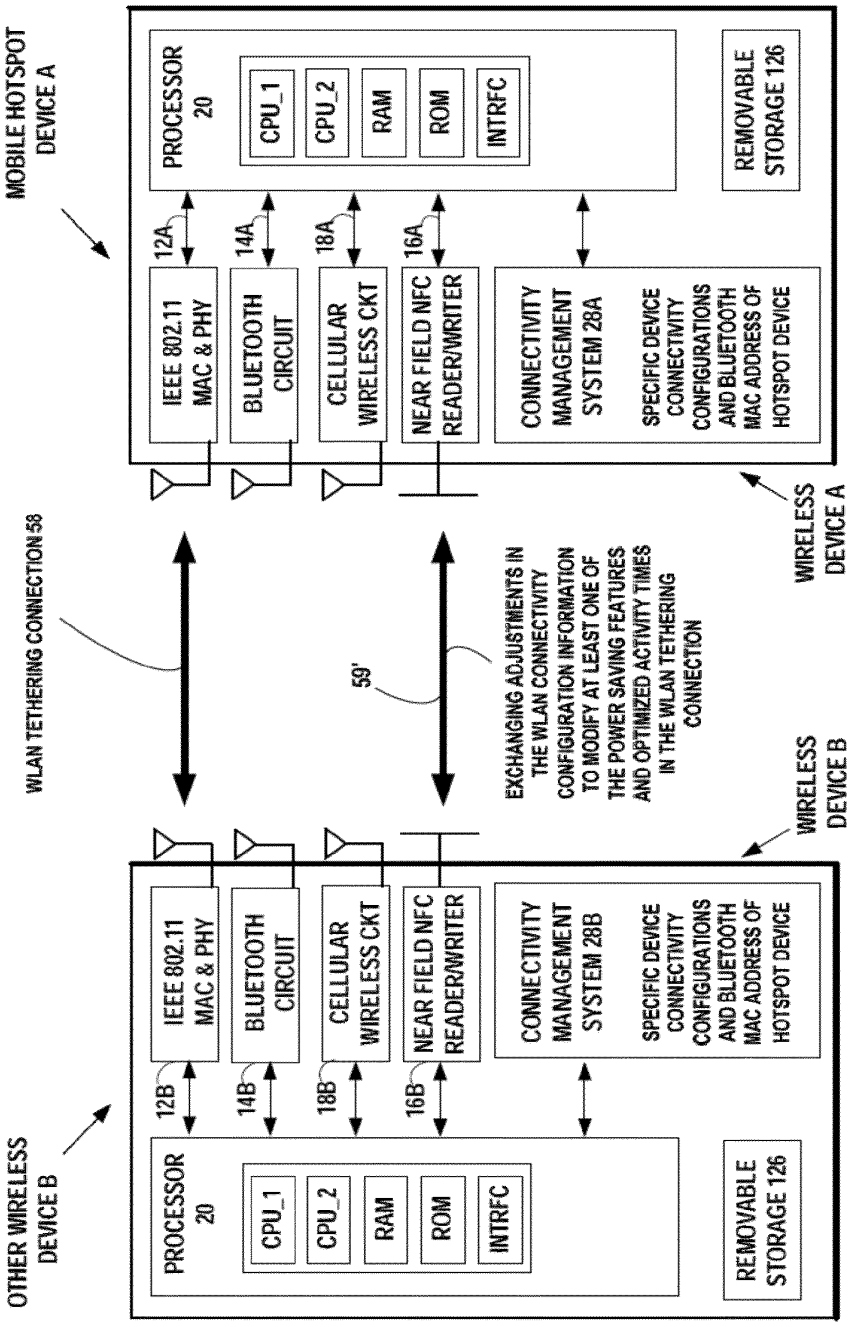

MOBILE HOTSPOT DEVICE A
PROCESSOR 20
CPU_1
CPU_2
RAM
ROM
INTRFC
REMOVABLE STORAGE 126
12A
14A
18A
16A
IEEE 802.11 MAC & PHY
BLUETOOTH CIRCUIT
CELLULAR WIRELESS CKT
NEAR FIELD NFC READER/WRITER
CONNECTIVITY MANAGEMENT SYSTEM 28A
SPECIFIC DEVICE CONNECTIVITY CONFIGURATIONS AND BLUETOOTH MAC ADDRESS OF HOTSPOT DEVICE
WLAN TETHERING CONNECTION 58
59'
EXCHANGING ADJUSTMENTS IN THE WLAN CONNECTIVITY CONFIGURATION INFORMATION TO MODIFY AT LEAST ONE OF THE POWER SAVING FEATURES AND OPTIMIZED ACTIVITY TIMES IN THE WLAN TETHERING CONNECTION
WIRELESS DEVICE A
WIRELESS DEVICE B
OTHER WIRELESS DEVICE B
PROCESSOR 20
CPU_1
CPU_2
RAM
ROM
INTRFC
REMOVABLE STORAGE 126
12B
14B
18B
16B
IEEE 802.11 MAC & PHY
BLUETOOTH CIRCUIT
CELLULAR WIRELESS CKT
NEAR FIELD NFC READER/WRITER
CONNECTIVITY MANAGEMENT SYSTEM 28B
SPECIFIC DEVICE CONNECTIVITY CONFIGURATIONS AND BLUETOOTH MAC ADDRESS OF HOTSPOT DEVICE

FIG. 3A

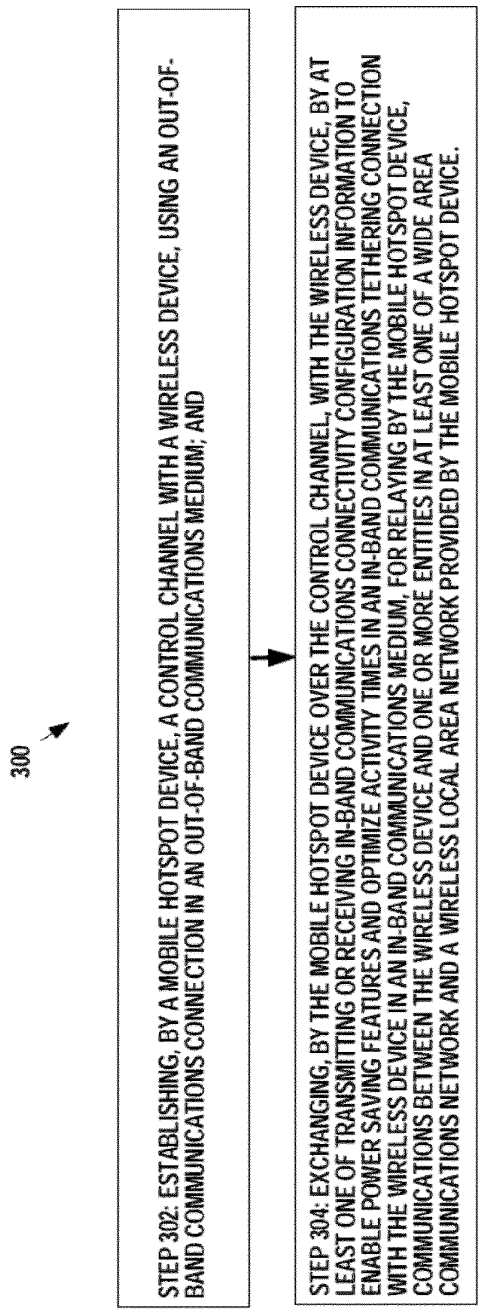
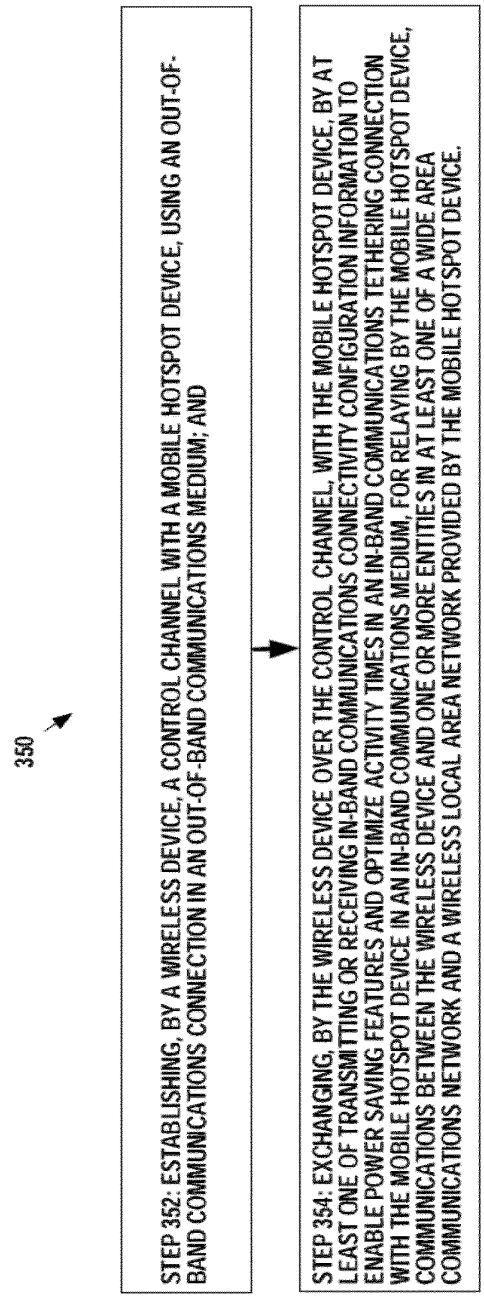

300
STEP 302: ESTABLISHING, BY A MOBILE HOTSPOT DEVICE, A CONTROL CHANNEL WITH A WIRELESS DEVICE, USING AN OUT-OF-BAND COMMUNICATIONS CONNECTION IN AN OUT-OF-BAND COMMUNICATIONS MEDIUM; AND
STEP 304: EXCHANGING, BY THE MOBILE HOTSPOT DEVICE OVER THE CONTROL CHANNEL, WITH THE WIRELESS DEVICE, BY AT LEAST ONE OF TRANSMITTING OR RECEIVING IN-BAND COMMUNICATIONS CONNECTIVITY CONFIGURATION INFORMATION TO ENABLE POWER SAVING FEATURES AND OPTIMIZE ACTIVITY TIMES IN AN IN-BAND COMMUNICATIONS TETHERING CONNECTION WITH THE WIRELESS DEVICE IN AN IN-BAND COMMUNICATIONS MEDIUM, FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND ONE OR MORE ENTITIES IN AT LEAST ONE OF A WIDE AREA COMMUNICATIONS NETWORK AND A WIRELESS LOCAL AREA NETWORK PROVIDED BY THE MOBILE HOTSPOT DEVICE.

FIG. 3B


350
STEP 352: ESTABLISHING, BY A WIRELESS DEVICE, A CONTROL CHANNEL WITH A MOBILE HOTSPOT DEVICE, USING AN OUT-OF-BAND COMMUNICATIONS CONNECTION IN AN OUT-OF-BAND COMMUNICATIONS MEDIUM; AND
STEP 354: EXCHANGING, BY THE WIRELESS DEVICE OVER THE CONTROL CHANNEL, WITH THE MOBILE HOTSPOT DEVICE, BY AT LEAST ONE OF TRANSMITTING OR RECEIVING IN-BAND COMMUNICATIONS CONNECTIVITY CONFIGURATION INFORMATION TO ENABLE POWER SAVING FEATURES AND OPTIMIZE ACTIVITY TIMES IN AN IN-BAND COMMUNICATIONS TETHERING CONNECTION WITH THE MOBILE HOTSPOT DEVICE IN AN IN-BAND COMMUNICATIONS MEDIUM, FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND ONE OR MORE ENTITIES IN AT LEAST ONE OF A WIDE AREA COMMUNICATIONS NETWORK AND A WIRELESS LOCAL AREA NETWORK PROVIDED BY THE MOBILE HOTSPOT DEVICE.

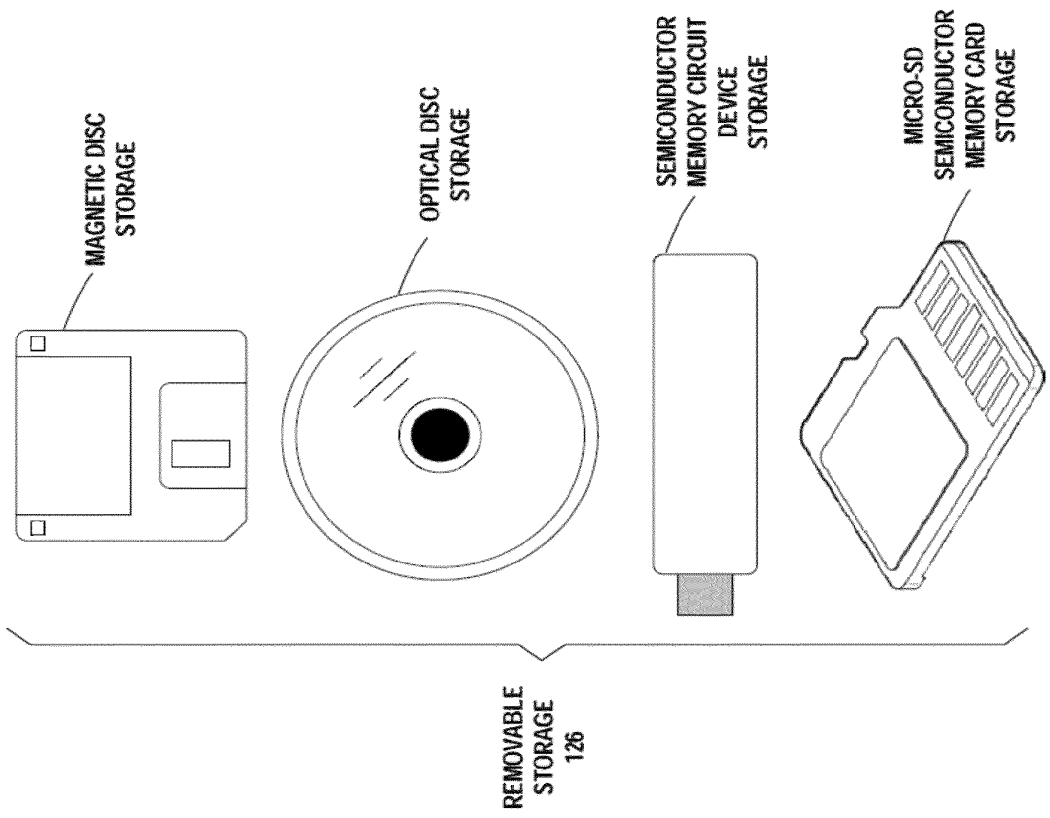

MAGNETIC DISC STORAGE
OPTICAL DISC STORAGE
SEMICONDUCTOR MEMORY CIRCUIT DEVICE STORAGE
MICRO-SD SEMICONDUCTOR MEMORY CARD STORAGE
REMOVABLE STORAGE 126

FIG. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2012115471 A **[0006]**

Samsung Ex. 1004, Page 517 of 563

I500350

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I500350 B**

(45)公告日： 中華民國 104 (2015) 年 09 月 11 日

(21)申請案號：102135927 (22)申請日： 中華民國 102 (2013) 年 10 月 04 日

(51)Int. Cl.： ***H04W76/04 (2009.01)*** ***H04L29/06 (2006.01)***

(71)申請人：瑞昱半導體股份有限公司 (中華民國) REALTEK SEMICONDUCTOR CORPORATION (TW)
新竹市新竹科學園區創新二路 2 號

(72)發明人：顏光裕 YEN, KUANG YU (TW) ；劉又誠 LIU, YU CHEN (TW) ；程崇嘉 CHEN, CHUNG CHIA (TW)

(74)代理人：林昱礽；鄭慶鴻

(56)參考文獻：

US 2013/0016708A1 WO 03/028313A2

審查人員：陳奕昌

申請專利範圍項數：15 項 圖式數：3 共 22 頁

(54)名稱

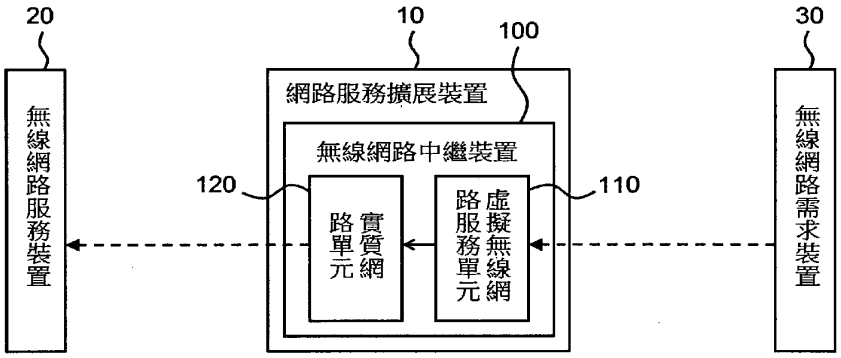
網路服務擴展方法與裝置

NETWORK SERVICE EXTENSION METHOD AND DEVICE

(57)摘要

本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

The present invention discloses a network service extension method which is capable of increasing the range of a network service and carried out by a network service extension device. The method comprises: establishing the link between a real network unit of a wireless network relay device and a wireless network serving device; configuring a virtual wireless network serving unit according to the link setting of the wireless network serving device in which the link settings of the serving device and the serving unit are the same; establishing the link between the virtual wireless network serving unit and a wireless network demand device; and establishing the connection between the wireless network serving device and the wireless network demand device via the virtual wireless network serving unit and the real network unit.



10・・・網路服務擴展裝置

20・・・無線網路服務裝置

30・・・無線網路需求裝置

100・・・無線網路中繼裝置

110・・・虛擬無線網路服務單元

120・・・實質網路單元

【圖1】

I500350 專利案號：102135927

申請日：102. 10. -4

公告本

IPC分類：

H04W 76/04 (2009.01)

H04L 29/02 (2006.01)

【發明摘要】

【中文發明名稱】 網路服務擴展方法與裝置

【英文發明名稱】 Network service extension method and device

【中文】

本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【英文】

The present invention discloses a network service extension method which is capable of increasing the range of a network service and carried out by a network service extension device. The method comprises: establishing the link between a real network unit of a wireless network relay device and a wireless network serving device; configuring a virtual wireless network serving unit according to the link setting of the wireless network serving device in which the link settings of the serving device and the serving unit are the same; establishing the link between the virtual wireless network serving unit and a wireless network demand device; and establishing the connection between the wireless network

serving device and the wireless network demand device via the virtual wireless network serving unit and the real network unit.

【指定代表圖】　　圖1

【代表圖之符號簡單說明】

10 網路服務擴展裝置

20 無線網路服務裝置

30 無線網路需求裝置

100 無線網路中繼裝置

110 虛擬無線網路服務單元

120 實質網路單元

【發明說明書】

【中文發明名稱】 網路服務擴展方法與裝置

【英文發明名稱】 Network service extension method and device

【技術領域】

【0001】 本發明是關於網路方法與裝置，尤其是關於網路服務擴展方法與裝置。

【先前技術】

【0002】 無線網路基於其便利性已廣泛地應用於日常生活中。一般無線網路之架構包含一基礎服務裝置（Basic Service Set, BSS。例如一無線網路接取點（Access Point, AP）），該基礎服務裝置連線至一可靠網路（例如一有線網路），於一服務範圍內提供一基礎無線網路服務，並允許該服務範圍內的其它無線網路裝置經由它連線至該可靠網路。然而根據目前技術，若一第一無線網路裝置擁有該基礎無線網路服務之連線設定且位於前述服務範圍內，而一第二無線網路裝置擁有該基礎無線網路服務之連線設定但位於該服務範圍外或無法穩定地連線至該基礎服務裝置，此第二無線網路需透過該第一無線網路裝置所提供之一有別於前述基礎無線網路服務之連線服務方能穩定地連線至該基礎服務裝置，舉例來說，該基礎無線網路服務係一第一無線區域網路（Wireless Local Area Network, WLAN）服務，該連線服務係一第二無線區域網路服務，該第一與第二無線區域網路服務之連線設定（例如一服務設定識別碼（Service Set Identifier, SSID）、一保密類型（Security Type）、一金鑰）不同，因此該第二無

線網路裝置需同時具備該第一與第二無線區域網路服務之連線設定才能借道該第一無線網路裝置連線至該基礎服務裝置，換言之，倘若該第二無線網路裝置不具有該第一無線網路裝置之連線設定，即無法經由該第一無線網路裝置連線至該基礎服務裝置，此一限制減少了該第二無線網路裝置之連線機會。

【發明內容】

【0003】 鑑於先前技術之不足，本發明之一目的在於提供一種網路服務擴展方法與一種網路服務擴展裝置，以擴展一網路服務之範圍。

【0004】 本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由本發明之網路服務擴展裝置或其等效裝置來執行。依據本發明之一實施例，該方法包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【0005】 本發明另揭露了一種網路服務擴展裝置，能夠擴展一無線網路服務裝置之網路服務之範圍。依據本發明之一實施例，該裝置包含：一無線網路中繼裝置，用來與該無線網路服務裝置建立連線，包含：一虛擬無線網路服務單元，係依據該無線網路服務裝置之連線設定而形成，用來與一無線網路需求裝置建立連線，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；以及一實質網路單元，用來與該虛擬無線網路服務單元以及該無線網路服務裝置建立連線，因此該無線網路中繼裝置藉由該虛擬無線網

路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【0006】 有關本發明的特徵、實作與功效，茲配合圖式作較佳實施例詳細說明如下。

【圖式簡單說明】

【0007】

〔圖1〕為本發明之網路服務擴展裝置之一實施例的示意圖；

〔圖2a〕為圖1之無線網路中繼裝置之運作的一實施例的示意圖；

〔圖2b〕為圖1之無線網路中繼裝置之運作的另一實施例的示意圖；以及

〔圖3〕為本發明之網路服務擴展方法之一實施例的流程圖。

【實施方式】

【0008】 以下說明內容之技術用語係參照本技術領域之習慣用語，如本說明書對部分用語有加以說明或定義，該部分用語之解釋係以本說明書之說明或定義為準。

【0009】 本發明之揭露內容包含網路服務擴展裝置與方法，能夠擴展一網路服務之範圍。該裝置與方法可應用於一積體電路或一系統裝置，在實施為可能的前提下，本技術領域具有通常知識者能夠依本說明書之揭露內容來選擇等效之元件或步驟來實現本發明，亦即本發明之實施並不限於後敘之實施例。由於本發明之網路服務擴展裝置所包含之部分元件單獨而言可能為已知元件，因此在不影響該裝置發明之充分揭露及可實施性的前提下，以下說明對於已知元

件的細節將予以節略。此外，本發明之網路服務擴展方法可藉由本發明之網路服務擴展裝置或其等效裝置來執行，在不影響該方法發明之充分揭露及可實施性的前提下，以下方法發明之說明將著重於步驟內容而非硬體。

【0010】 請參閱圖1，其係本發明之網路服務擴展裝置之一實施例的示意圖，於本實施例中，該擴展裝置10係一無線區域網路（Wireless Local Area Network, WLAN）裝置，例如一筆記型電腦、一手機、一平板電腦、一網路卡或一網路晶片，能夠無線連線至一無線網路服務裝置20（例如一無線網路接取點（Access Point, AP））並擴展其網路服務的範圍。如圖1所示，該網路服務擴展裝置10包含：一無線網路中繼裝置100，用來與該無線網路服務裝置20建立連線，包含一虛擬無線網路服務單元110以及一實質網路單元120，該無線網路中繼裝置100可以是一無線網路卡、一無線網路晶片或其等效裝置。所述虛擬無線網路服務單元110係依據前述無線網路服務裝置20之連線設定而形成（Configured），具有與該無線網路服務裝置20之連線設定相同之設定，用來與一無線網路需求裝置30（例如一筆記型電腦、一手機或一平板電腦）建立連線，換句話說，只要該無線網路需求裝置30擁有連線至該無線網路服務裝置20之設定，即可連線至該虛擬無線網路服務單元110，本實施例中，該虛擬無線網路服務單元110係藉由無線網路中繼裝置100模擬該無線網路服務裝置20所形成。另外，所述實質網路單元120用來與該虛擬無線網路服務單元110以及該無線網路服務裝置20建立連線，因此，該無線網路中繼裝置100可藉由該虛擬無線網路服務單元110以及該實質網路單元120建立起該無線網路服務裝置20與該無線網路需求裝置30間的連結，本實施例中，該實質網路單元120係該無線網路中繼裝置100之固有架構。

【0011】 承上所述，本實施例係假設：該無線網路需求裝置30無法直接或

穩定地連線至該無線網路服務裝置20，因此需透過該網路服務擴展裝置10來連線至該無線網路服務裝置20。換句話說，該無線網路需求裝置30所接收之該無線網路服務裝置20之訊號強度/穩定度會小於該無線網路需求裝置30所接收之該虛擬無線網路服務單元110之訊號強度/穩定度。由於該虛擬無線網路服務單元110與該無線網路服務裝置20之連線設定相同，因此無線網路需求裝置30會將該虛擬無線網路服務單元110視為該無線網路服務裝置20，且該無線網路需求裝置30只要擁有該無線網路服務裝置20之連線設定（例如一服務設定識別碼（Service Set Identifier, SSID）；一保密類型（Security Type）；以及一金鑰），即能連線至該虛擬無線網路服務單元110，再經由它連接該無線網路服務裝置20。詳言之，本實施例中，該虛擬無線網路服務單元110會發出一信標（Beacon）以供該無線網路需求裝置30得知該虛擬無線網路服務單元110之存在，之後該無線網路需求裝置30會發出一探詢要求（Probe Request）訊號，而該虛擬無線網路服務單元110會再針對該探詢要求訊號回應一探詢回應（Probe Response）訊號，進而建立兩者間的連線。

【0012】 請繼續參閱第1圖，於該無線網路需求裝置30與該虛擬無線網路服務單元110建立連線後，若該無線網路需求裝置欲經由該無線網路服務裝置20輸出資料，會發送一傳送封包至該虛擬無線網路服務單元110，接著該虛擬無線網路服務單元110再經由該實質網路單元120將該傳送封包傳輸至該無線網路服務裝置20；另一方面，若該無線網路服務裝置20欲發送一接收封包屬於該無線網路需求裝置30，會將該接收封包傳輸至該實質網路單元120，該實質網路單元120再經由該虛擬無線網路服務單元110將該接收封包傳輸至該無線網路需求裝置30。上述封包傳送可藉由多種方式來實現，舉例而言，請參閱圖2a，該虛

擬無線網路服務單元110包含一虛擬實體層（Physical Layer, PHY Layer）112、一虛擬媒體存取控制層（Media Access Control Layer, MAC Layer）114、一虛擬階層3協定層（Layer-3 Protocol Layer）116以及一虛擬應用層（Application Layer）118，該實質網路單元120則包含一實質應用層122、一實質階層3協定層124、一實質媒體存取控制層126以及一實質實體層128，該虛擬實體層112用來從該無線網路需求裝置30接收該傳送封包，並依序經由該虛擬媒體存取控制層114、該虛擬階層3協定層116、該實質階層3協定層124、該實質媒體存取控制層126以及該實質實體層128將該傳送封包傳輸至該無線網路服務裝置20，其中該虛擬階層3協定層116及/或該實質階層3協定層124會依據傳送封包之資訊（例如來源欄位、目的欄位或特定標籤）來判斷該傳送封包之接收者是否為該無線網路中繼裝置100，若否即將該傳送封包轉發至該無線網路服務裝置20；類似地，該實質實體層128用來從該無線網路服務裝置20接收該接收封包，並依序經由該實質媒體存取控制層126、該實質階層3協定層124、該虛擬階層3協定116、該虛擬媒體存取控制層114以及該虛擬實體層112將該接收封包傳輸至該無線網路需求裝置30，其中該實質階層3協定層124及/或該虛擬階層3協定層116會依據接收封包之資訊（例如來源欄位、目的欄位或特定標籤）來判斷該接收封包之接收者是否為該無線網路中繼裝置100，若否即將該接收封包轉發至該無線網路需求裝置30。另舉例而言，請參閱圖2b，本發明亦可不透過階層3協定層而直接轉發該傳送封包或接收封包，更精確地說，該傳送封包會依序經由該虛擬實體層112、該虛擬媒體存取控制層114、該實質媒體存取控制層126以及該實質實體層128而傳送至該無線網路服務裝置20，而該接收封包會依序經由該實質實體層128、該實質媒體存取控制層126、該虛擬媒體存取控制層114以及該虛擬實體層112而傳送至該無線網路需求裝置30。

【0013】 請注意，前述應用層118、122屬於網路分層之一環，並未用於圖2a與圖2b之實施例。另外，前述虛擬實體層112之運作原理與實質實體層128相同；虛擬媒體存取控制層114之運作原理與實質媒體存取控制層126相同；且虛擬階層3協定層116之運作原理與實質階層3協定層124之運作原理相同。再者，由於該些實質單元124、126、128個別而言屬於本領域之習知技術，且本技術領域人士可依據本發明之揭露及當前技術來實現該些實質單元124、126、128以及虛擬單元112、114、116，因此在不影響本發明之充分揭露及可實施性的前提下，不必要之說明在此予以節略。

【0014】 承前所述，本發明除可如圖1般模擬無線網路服務裝置20以延伸其網路服務之範圍，使無線網路需求裝置30得以經由本發明以相同的連線設定連線至該無線網路服務裝置20，亦可依循前揭方式來模擬更多不同的無線網路服務裝置，以支援更多的無線網路需求裝置，由於本技術領域具有通常知識者可依前揭內容瞭解相同/相似的模擬暨連線過程，並能自行採用現有或自設的規則來進行多連線操作（例如複數個虛擬裝置輪流進行連線或發送中斷要求（Interrupt Request）以要求連線等），故在不影響本發明之揭露與可實施性的要求下，冗餘之說明在此予以節略。

【0015】 除前述之裝置外，本發明亦相對應地揭露了一種網路服務擴展方法，能夠擴展一網路服務（例如一無線區域網路服務）之範圍，係由前揭網路服務擴展裝置10或其等效裝置來執行。如圖3所示，本發明之一實施例包含下列步驟：

步驟S310：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；

步驟S320：依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同。本實施例中，該連線設定例如是一服務設定識別碼；一保密類型；以及一金鑰；

步驟S330：建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線。本實施例中，步驟S330包含：令該虛擬無線網路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在；以及令該虛擬無線網路服務單元依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號；以及

步驟S340：經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。本實施例中，步驟S340包含：建立該虛擬無線網路服務單元與該實質網路單元間的連線；經由該虛擬無線網路服務單元與該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及經由該實質網路單元與該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【0016】承上所述，步驟S340之封包傳送可藉由多種方式來實現，舉例而言，將該傳送封包傳輸至該無線網路服務裝置之步驟包含：經由該虛擬無線網路服務單元之一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層3協定層與該實質網路單元之一實質階層3協定層、一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及將該接收封包傳輸至該無線網路需求裝置之步驟包含：經由該實質網路單元之該實質實體層、該實質媒體存取控制層以及該實質階層3協定層與該虛擬無線網路服務單元之該虛擬階層3協定層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。另舉例而言，步驟S340亦可不透過階層3協定層而直接轉發該

傳送封包或接收封包，亦即將該傳送封包傳輸至該無線網路服務裝置之步驟包含：經由該虛擬無線網路服務單元之虛擬實體層以及虛擬媒體存取控制層與該實質網路單元之實質媒體存取控制層以及實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及將該接收封包傳輸至該無線網路需求裝置之步驟包含：經由該實質網路單元之實質實體層以及實質媒體存取控制層與該虛擬無線網路服務單元之虛擬媒體存取控制層以及虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【0017】 由於本技術領域具有通常知識者可藉由圖1至圖2b之裝置發明的揭露內容來瞭解圖3之方法發明的實施細節與變化，因此，為避免贅文，在不影響該方法發明之揭露要求及可實施性的前提下，重複之說明在此予以節略。請注意，前揭圖示中，元件之形狀、尺寸、比例以及步驟之順序等僅為示意，係供本技術領域具有通常知識者瞭解本發明之用，非用以限制本發明。另外，本技術領域人士可依本發明之揭露內容及自身的需求選擇性地實施任一實施例之部分或全部技術特徵，或者選擇性地實施複數個實施例之部分或全部技術特徵之組合，藉此增加本發明實施時的彈性。再者，前揭實施例雖以無線區域網路為例，然此並非對本發明之限制，本技術領域人士可依本發明之揭露適當地將本發明應用於其它類型的網路系統中。

【0018】 綜上所述，本發明之網路服務擴展裝置與方法能夠模擬一無線網路服務裝置以延伸其網路服務之範圍，並能使一無線網路需求裝置經由本發明以相同的連線設定連線至該無線網路服務裝置，亦即只要該無線網路需求裝置擁有該無線網路服務裝置之連線設定，即能透過本發明之中繼來連接該無線網路服務裝置以上網，藉此解決該無線網路服務裝置之服務範圍不足或服務死角

等問題，並增加該無線網路需求裝置之連線機會。

【0019】 雖然本發明之實施例如上所述，然而該些實施例並非用來限定本發明，本技術領域具有通常知識者可依據本發明之明示或隱含之內容對本發明之技術特徵施以變化，凡此種種變化均可能屬於本發明所尋求之專利保護範疇，換言之，本發明之專利保護範圍須視本說明書之請求項所界定者為準。

【符號說明】

【0020】

10 網路服務擴展裝置

20 無線網路服務裝置

30 無線網路需求裝置

100 無線網路中繼裝置

110 虛擬無線網路服務單元

112 虛擬實體層

114 虛擬媒體存取控制層

116 虛擬階層3協定層

118 虛擬應用層

120 實質網路單元

122 實質應用層

124 實質階層3協定層

126 實質媒體存取控制層

128 實質實體層

S310 建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連

線

S320 依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同

S330 建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線

S340 經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結

104年 04月 27日 修正替換頁

【發明申請專利範圍】

【第 1 項】一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：

建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的無線連線；

依據該無線網路服務裝置之連線設定提供該無線網路中繼裝置之一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；

建立該虛擬無線網路服務單元與一無線網路需求裝置間的無線連線；以及

經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【第 2 項】如請求項第 1 項所述之網路服務擴展方法，其中建立該虛擬無線網路服務單元與該無線網路需求裝置間的連線之步驟進一步包含：

令該虛擬無線網路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在；以及

令該虛擬無線網路服務單元依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號。

【第 3 項】如請求項第 1 項所述之網路服務擴展方法，其中建立該無線網路服務裝置與該無線網路需求裝置間的連線之步驟進一步包含：

建立該虛擬無線網路服務單元與該實質網路單元間的連線；

經由該虛擬無線網路服務單元與該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及

經由該實質網路單元與該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【第 4 項】如請求項第 3 項所述之網路服務擴展方法，其中將該傳送封包傳輸至該無線網路服務裝置之步驟包含：

經由該虛擬無線網路服務單元之一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層 3 協定層與該實質網路單元之一實質階層 3 協定層、一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及

將該接收封包傳輸至該無線網路需求裝置之步驟包含：

經由該實質網路單元之該實質實體層、該實質媒體存取控制層以及該實質階層 3 協定層與該虛擬無線網路服務單元之該虛擬階層 3 協定層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【第 5 項】如請求項第 3 項所述之網路服務擴展方法，其中將該傳送封包傳輸至該無線網路服務裝置之步驟包含：

經由該虛擬無線網路服務單元之一虛擬實體層以及一虛擬媒體存取控制層與該實質網路單元之一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及

將該接收封包傳輸至該無線網路需求裝置之步驟包含：

經由該實質網路單元之該實質實體層以及該實質媒體存取控制層與該虛

擬無線網路服務單元之該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【第 6 項】如請求項第 1 項所述之網路服務擴展方法，其中該無線網路服務裝置之連線設定包含：一服務設定識別碼；一保密類型；以及一金鑰。

【第 7 項】如請求項第 1 項所述之網路服務擴展方法，其中該網路服務係一無線區域網路服務。

【第 8 項】一種網路服務擴展裝置，能夠擴展一無線網路服務裝置之網路服務之範圍，包含：

一無線網路中繼裝置，用來與該無線網路服務裝置建立無線連線，包含：

一虛擬無線網路服務單元，係依據該無線網路服務裝置之連線設定而形成，用來與一無線網路需求裝置建立無線連線，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；以及

一實質網路單元，用來與該虛擬無線網路服務單元建立連線以及與該無線網路服務裝置建立無線連線，

其中該無線網路中繼裝置藉由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【第 9 項】如請求項第 8 項所述之網路服務擴展裝置，其中該無線網路需求裝置所接收之該無線網路服務裝置之訊號強度小於該無線網路需求裝置所接收之該虛擬無線網路服務單元之訊號強度。

【第 10 項】如請求項第 8 項所述之網路服務擴展裝置，其中該虛擬無線網

路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在，並且依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號。

【第 11 項】如請求項第 8 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元經由該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及該實質網路單元經由該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【第 12 項】如請求項第 11 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元包含一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層 3 協定層；該實質網路單元包含一實質階層 3 協定層、一實質媒體存取控制層以及一實質實體層；該虛擬實體層接收該傳送封包，並依序經由該虛擬媒體存取控制層、該虛擬階層 3 協定層、該實質階層 3 協定層、該實質媒體存取控制層以及該實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及該實質實體層接收該接收封包，並依序經由該實質媒體存取控制層、該實質階層 3 協定層、該虛擬階層 3 協定、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

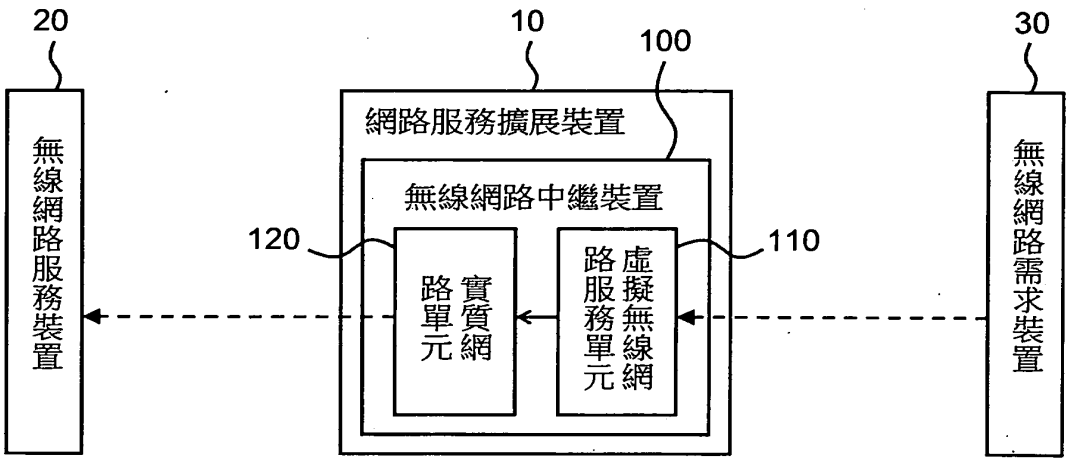
【第 13 項】如請求項第 11 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元包含一虛擬實體層以及一虛擬媒體存取控制層；該實質網路單元包含一實質媒體存取控制層以及一實質實體層；該虛擬實體層接收該傳送封包，並依序經由該虛擬媒體存取控制層、該實質媒體存取控

制層以及該實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及該實質實體層接收該接收封包，並依序經由該實質媒體存取控制層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

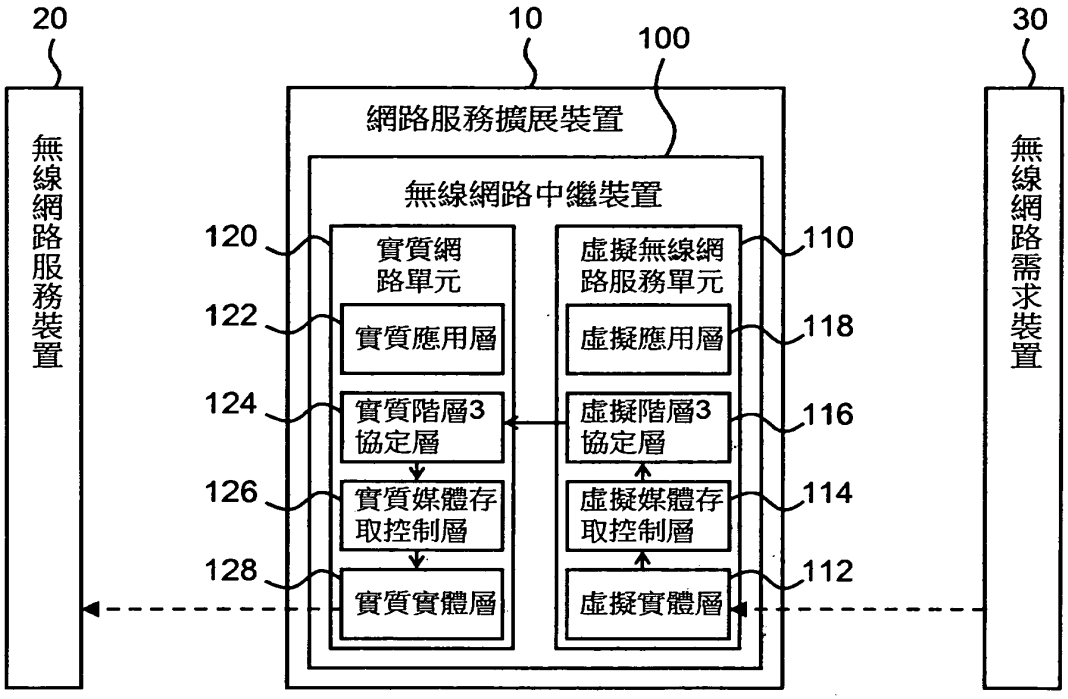
【第 14 項】如請求項第 8 項所述之網路服務擴展裝置，其中該無線網路服務裝置之連線設定包含：一服務設定識別碼；一保密類型；以及一金鑰。

【第 15 項】如請求項第 8 項所述之網路服務擴展裝置，其中該網路服務係一無線區域網路服務。

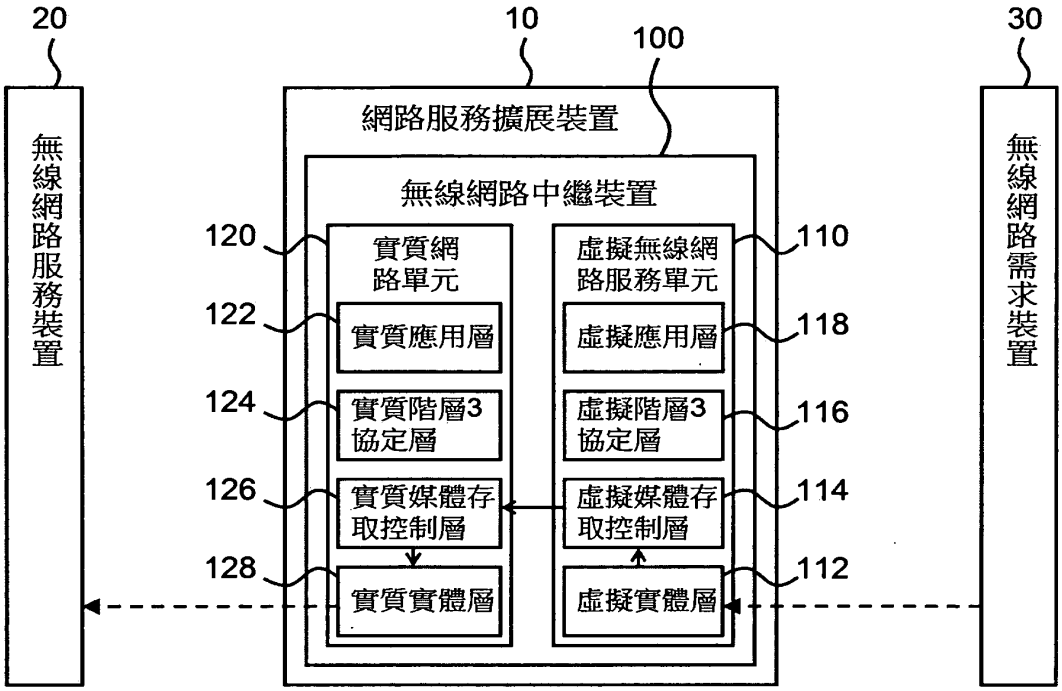
【發明圖式】


20
10
100
30
無線網路服務裝置
網路服務擴展裝置
無線網路中繼裝置
120
110
實質網路單元
虛擬無線網路服務單元
無線網路需求裝置

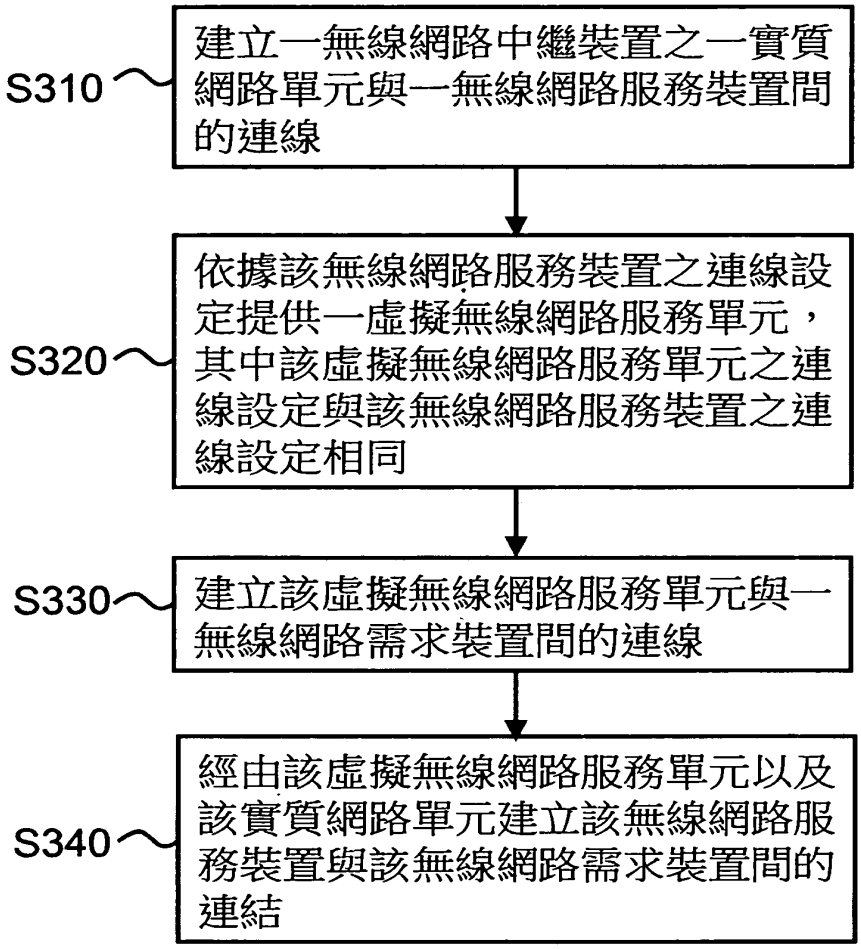
【圖1】


20
10
100
30
無線網路服務裝置
網路服務擴展裝置
無線網路中繼裝置
120
實質網路單元
110
虛擬無線網路服務單元
122
實質應用層
118
虛擬應用層
124
實質階層3協定層
116
虛擬階層3協定層
126
實質媒體存取控制層
114
虛擬媒體存取控制層
128
實質實體層
112
虛擬實體層
無線網路需求裝置

【圖2a】


20
10
100
30
無線網路服務裝置
網路服務擴展裝置
無線網路中繼裝置
無線網路需求裝置
120
實質網路單元
110
虛擬無線網路服務單元
122
實質應用層
118
虛擬應用層
124
實質階層3協定層
116
虛擬階層3協定層
126
實質媒體存取控制層
114
虛擬媒體存取控制層
128
實質實體層
112
虛擬實體層

【圖2b】


S310
建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線
S320
依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同
S330
建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線
S340
經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結

【圖3】

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 016 750 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.09.2017 Bulletin 2017/39

(21) Application number: **07781811.0**

(22) Date of filing: **18.04.2007**

(51) Int Cl.:
H04W 88/08 *(2009.01)* ***G06F 21/35*** *(2013.01)*
G06F 21/74 *(2013.01)*

(86) International application number:
PCT/US2007/066514

(87) International publication number:
WO 2007/124279 (01.11.2007 Gazette 2007/44)

(54) **SIMPLIFIED DUAL MODE WIRELESS DEVICE AUTHENTICATION APPARATUS AND METHOD**

VORRICHTUNG UND VERFAHREN FÜR VEREINFACHTE AUTHENTIFIZIERUNG DRAHTLOSER BIMODALER GERÄTE

PROCÉDÉ ET APPAREIL D'AUTHENTIFICATION D'UN DISPOSITIF SANS FIL BIMODE SIMPLIFIÉ

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

(30) Priority: **21.04.2006 US 408764**

(43) Date of publication of application:
21.01.2009 Bulletin 2009/04

(73) Proprietor: **Cisco Technology, Inc.**
San Jose, CA 95134-1706 (US)

(72) Inventors:
- **LEE, Shze Chew**
  Irvine, California 92618 (US)
- **GUTMAN, Andrew M.**
  Foothill Ranch, California 92610 (US)
- **WILLIS, Edward Dean**
  Plano, Texas 75075 (US)

(74) Representative: **Kazi, Ilya et al**
Mathys & Squire LLP
The Shard
32 London Bridge Street
London SE1 9SG (GB)

(56) References cited:
EP-A1- 1 424 810
WO-A2-2008/021547
US-A1- 2001 048 744
US-A1- 2001 048 744
US-A1- 2005 232 209
US-A1- 2005 232 209

- **"AT-WA7500 Dual Radio Wireless Access Point Next Generation Wireless Access Point Enterprise-class Features", , 14 October 2004 (2004-10-14), XP055164237, Retrieved from the Internet: URL:http://www.alliedtelesis.com/media/datasheets/wa7500_ds.pdf [retrieved on 2015-01-22]**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 2 016 750 B1

Description

TECHNICAL FIELD

[0001] The present invention relates to security apparatus and methods and, in particular, to apparatus and methods for authentication of a dual-mode wireless device.

BACKGROUND

[0002] With the confluence of electronic communications, data, and computing services, (collectively, services) there arises a need to bridge the disparate network infrastructures supporting these services and to address resulting new opportunities and challenges. A wireline network (WLN) employs a structured transmission medium, including copper wire, fiber optic cable, and other defined waveguides. By comparison, a wireless network can be any network with a physical layer that permits constituent devices to communicate using an unstructured transmission medium, such as the atmosphere, or space. Wireless networks have developed within two formerly distinct spheres: wireless wide area networks (WWAN), which were cast in the formal likeness of wireline telephony networks; and wireless local area networks (WLAN), which are often informally structured, if at all, having coverage zones of at least three of magnitude less than a WWAN. Currently popular WWAN networks can provide mobile wireless services, as specified by the AMPS, D-AMPS, PCS, GSM, and UMTS wireless mobile service standards. A growing diversity of WLAN standards describe the physical-to-network architectures of fixed wireless services, with devices operable with WLAN frequently being capable of being operable with more than one type of fixed wireless service. Dual-mode devices were developed to meet the diverse needs of those using both WWAN and WLAN systems.

[0003] Dual-mode services are becoming attractive to mobile operators and their subscribers because of three trends: a growing population of mobile subscribers, the prevalence of home broadband connections, and the availability of low-cost, home wireless access points that support local wireless networking. To satisfy this evolving need, technology manufacturers are developing and introducing into the marketplace, dual-mode devices, that is, devices capable of communicating over mobile radio networks, such as mobile phone networks, and wireless local area networks, such as those found in the increasingly popular "hotspots," or access zones for wireless networking, frequently providing the myriad of services available over the Internet.

[0004] A dual mode device can offer advantages over a single mode device. First, although mobile wireless systems may provide mobile wireless services to the high-mobility receiving stations of subscribers within a broad geographic area, they bear the disadvantages of poor indoor reception and uneven signal availability, particularly in dense urban environments hilly terrain. Second, fixed wireless systems can deliver a vast range of broadband services to stationary or low-mobility receivers located indoors, within a broadcast zone (e.g., hot spots or hot zones), but are disadvantaged by sharply-limited signal range, security and billing concerns, and the uncertainties arising from proprietary ownership and non-uniform product availability. Thus, a dual-mode device can enable a mobile service subscriber to switch from mobile wireless services to fixed wireless services, for example, in an area of poor mobile wireless service coverage. In addition, with a dual-mode device, using dual-mode services, mobile wireless service subscribers may make voice calls when outdoors in the ordinary manner, using the facilities of the subscribed mobile wireless service at the standard tariff rate. While indoors or in a remote geographic location where a signal compatible with the subscribed mobile wireless network is unavailable, a dual-mode device may permit customers to make and receive voice calls using a fixed wireless network. To reflect the offloading of the subscriber's call bandwidth from the mobile wireless service provider' s to a less-expensive fixed wireless network and the Internet, the mobile wireless provider may offer the mobile wireless subscriber lower tariff rates when using a fixed- wireless link. Also, a dual-mode device makes possible voice call handoff and transfer of communication links as a subscriber roams between mobile wireless and fixed wireless systems. Furthermore, dual-mode devices and services create an opportunity for subscribers or vendors who wish to assist a third party with obtaining provider-authorized allocations of mobile wireless voice or dual-mode services. Nevertheless, there is a substantial need to provide apparatus and methods rendering the desired degree of security to protect a mobile wireless provider infrastructure from Internet-based threats, as well as to safeguard provider network operator for their subscribers from interlopers and miscreants.

[0005] A wireless access point having encryption and authentication capabilities is disclosed in "AT-WA7500 Dual Radio Wireless Access Point", Datasheet, Allied Telesis (2006). EP 1424810 discloses a system in which a dual mode communication unit can connect to a WLAN and authenticate with a GPRS network via the WLAN. An access point device implementing an authentication method is disclosed in US 2001/048744.

[0006] Aspects of the invention are set out in the independent claims. Certain preferred features are set out in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] These and other features, aspects and advantages of the present invention will be more fully understood when considered with respect to the following detailed description, appended claims and accompanying drawings, wherein:

FIG. 1 is a graphical depiction of a dual-mode authentication system, as an embodiment of the invention herein;

FIG. 2 is a generalized flow diagram of a subscriber-provisioner dual-mode authentication operation, according to an embodiment of the present invention; and

FIG. 3 is a generalized flow diagram of a subscriber-passthrough dual-mode authentication operation, according to another embodiment of the present invention.

DETAILED DESCRIPTION

[0008] The inventive embodiments of the invention described herein include apparatus and methods for provisioning provisioned wireless services (PWS) to an authorized device by a provisioned service provider (PSP) in which a supplicant device may become an authorized device after successful authentication. A PWS can be any wireless service including, without limitation voice service, short message service (SMS), multimedia message service (MMS), video broadcasts, instant messaging, news and financial information, games and interactive gaming, Web-based services, and premium data services, to name a few.

[0009] A PSP can be a mobile wireless service provider, which also may operate a WWAN, also known as a radio area network, or RAN. A mobile telephone network is an exemplary RAN. Typically, WWAN provide service signals over a broad geographic region, using high-powered (more than 10W per channel) transmitters that are licensed to broadcast within defined frequency bands, which typically are allocated and regulated by a public authority. WWAN signals may be encoded or use sophisticated signaling techniques to provide privacy between communicating parties from potential eavesdroppers. Current WLAN transmit signals that are low-powered (under 0.1W per channel), limited-range (under about 300 m), and generated within prescribed frequency bands (e.g., 2.4 GHz, 5 GHz, 11 GHz, and 60 GHz). In general, such fixed wireless networks may be designated "unlicensed spectrum" wireless networks (USW), because by international consent, no operating license is required for wireless systems designed to operate within these constraints. USW can include networks employing the wireless protocols defined by the IEEE Std. 802.11 family of standards (including IEEE WLAN Stds. 802.11a, 802.11b, 802.11g, 802.11n, and 802.11j); IEEE Std. 802.15 (including wireless personal area networks - WPAN); IEEE Std. 802.16 (including wireless metropolitan area networks - WMAN); and by the ETSI Broadband Radio Access Network and Radio LAN Standards (e.g., HiperLAN2, HiperMAN, and HiperRAN), as well as, the TTR Korea WiBRO mobile network standard.

[0010] In large part, a wireline network (WLN) can be based on one of the family of standards, IEEE Std. 802.3 CSMA/CD Access Method, including 10 Mbps "Ethernet" (Stds. 802.3a, 802.3i, and 802.3j), 100 Mbps "Fast Ethernet" (Std. 802.3u), 1000 Mbps Gigabit Ethernet [GbE] (Stds. 802.3z, 802.3ab), and 10,000 Mbps GbE (Std. 802.3ae) Because IEEE Stds. 802.3 specify the lowermost networking layers (e.g., OSI Layers 1-3), the inventive embodiments herein are foreseeably operable with access technologies having bandwidth greater than 10 Gigabit Ethernet WLN. Each of the foregoing standards and specifications are incorporated herein, in their entirety. Also as used herein, the term generic access network (GAN) refers to both USW and WLN, when convenient to distinguish both from RAN-based networks. Furthermore, a WLN may include the Internet, where a person having ordinary skill in the art would recognize that inclusion is appropriate.

[0011] As used herein, the like terms "provision" and "provisioned" in verb form, and "provisioning" in gerund form, refer to a process including one or more of, without limitation: creating for an authorized user a service account for a subscribed service, the appropriate access to that account, the rights associated with that account, and the resources for managing the accounts; configuring one or both of authorized user hardware and software to activate the subscribed service; creating or modifying a record in an authorized user database and associating it with the service(s) and service level for which the authorized user has subscribed; providing the authorized user with subscribed provisioned wireless service resources, in accordance with the subscription agreement; and issuing preselected allocation units of PWS to the authorized user, upon request. Performing AAA services in conjunction with PWS requests and usage can be a provisioning activity as well. In general, AAA services include authentication, authorization and accounting, whereby prior to service, a PWS requester is authenticated and authorized to use the service offered by a MWSP or PSV in response to the PWS request; and while the PWS is delivered, PWS usage is metered and usage data is collected and can be associated with billing and collection.

[0012] PWS offered over a subscribed RAN (SRAN) typically are within the context of well-established and highly regulated access control, security, integrity, cost recovery, billing, enforcement, and Quality of Service mechanisms. GAN may lack one, more, or all of these features, simplifying the quest of unscrupulous users to purloin, misuse, or compromise valuable wireless services. To address the disparities in the regulatory and business structures between SRAN and GAN, and to encourage providers to offer valuable data and services regardless of the transmission medium used, a number of entities have put forth standards, provisional recommendations, and proposals for interoperative infrastructure management and policy enforcement. Pragmatic implementations tend to control access to services at a point close to service use, namely the customer premises, by remote management of customer premises equipment (CPE) through which such data and services are request-

Samsung Ex. 1004, Page 544 of 563

ed.

[0013] It is desirable to implement embodiments of the present invention in cooperation with remotely managed customer premises equipment (CPE) in accordance with a managed access architecture, premises network, and management, control, and interoperability principles and standards, articulated by the following exemplary DSL Forum Technical Reports, as amended: TR-044, Auto-Configuration for Basic Internet (IP-based) Services, December 2001; TR-046 Auto-Configuration Architecture & Framework, February 2002; TR-064, LAN-Side DSL CPE Configuration, May 2004; TR-069, CPE WAN Management Protocol, May 2004; TR-092, Broadband Remote Access Server (BRAS) Requirements Document, August 2004; TR-094, Multi-Service Delivery Framework for Home Networks, August 2004; TR-104, DSLHome™ Provisioning Parameters for VoIP CPE, September 2005; TR-110, DSLHome™ Reference Models for VoIP Configurations in the DSL Home, September 2005; and TR-111, Applying TR-069 to Remote Management of Home Networking Devices, December 2005. It is to be understood that other CPE-management models also may apply, including without limitation, those described in European Telecommunications Standards Institute document: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; OSS Architecture Release 1 (ETSI TS 188 001 V0.2.9 (2005-07)); and by IEEE Std. 802.21. The foregoing standards of the IEEE, ETSI, Korea TTR, and DSL Forum are incorporated herein by reference, in their entirety.

[0014] In general, the three fundamental security processes include access control, authentication, and audit. Of these constituent security processes, access control is a policy-based process that determines whether a supplicant is permitted to access a requested resource or service (i.e., "Are you permitted to access this resource?"). Authentication is a credential-based process by which a supplicant verifies its identity to the authenticator (i.e., "Are you who you say you are?"). Authentication also may include identification, and non-repudiation functions. Audit is an administrative process by which the appropriateness of policy-defined access to resources is monitored, and by which security enforcement mechanisms may be invoked upon identification of a policy violation. Audit also may include analysis of integrity (e.g., of link, data, or identity), intrusion detection, and containment. Finally, authorization can be an executive process that comprehends at least two of the constituent security processes, usually incorporating requirements of security policy, regulatory framework, and the like. For example, in an authorization process where a security policy implements authentication, a supplicant is required to prove its identity before access credentials are issued to the supplicant. In practice, security processes may vary in scope vertically and horizontally, and be almost as diverse in implementation as the applications needing security. A security process of vertical scope may operate at increasingly complex and abstract layers, e.g., authentication may be described within the context of a device level, a user level, an organization level, and an enterprise level. Similarly, horizontal security processes can include compartments that span communication occurring at one or more points along a communication path. For example, authentication may be compartmentalized with respect to a simple device-to-device exchange, to remote network links, or to a complete end-to-end secure communication exchange. End-to-end security also may result from cooperation of a sequence of cooperating authentication compartments which, in the whole, span the communication path. Frequently, contiguous subprocesses interact or overlap, although there may be no requirement for a given security process to be continuously operable over any portion of the communication path or over more than one physical or logical layer. Cryptographic processes may also be a constituent of authorization, and may include key creation, management, and distribution and encrypted communications. Thus, even if a supplicant is properly authenticated to the desired horizontal and vertical layers of security, the supplicant may not be able to participate in particular communications because the authorization process denied a requisite encryption key to the supplicant. The aforementioned security principles, as used herein are provided in National Institute of Standards and Technology (NIST) Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook; and NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, which documents are hereby incorporated herein in their entirety. Desirably, security processes exemplified in the present embodiments can implement or facilitate AAA processes of a provisioned service provider, and may further be enhanced by remote configuring of a local authenticator in an USW access point, in accordance with a foregoing remote configuration as a CPE.

[0015] Within the above context, FIG. 1 illustrates an embodiment of dual-mode authentication system 100 according to the present invention that includes a USW access point. Mobile wireless service provider (MWSP) 105, coupled to a RAN-based subscribed radio area network (SRAN) 108 and a wireline network (WLN) 110, can provision PWS, when requested, directly, or through an intermediary, which may be a Provisioned Services Vendor (PSV) 112. PSV 112, also coupled to the WLN 110, can provision PWS to an authorized device, and may provision PWS in cooperation with another provisioned service provider (PSP), which may include MWSP 105. The authorized device may be dual-mode access point (DMAP) 120 of unlicensed spectrum wireless network (USW) 117 operated by MWSP provisioned service subscriber (PSS) 115. DMAP 120 can be a USW access point adapted to couple USW 117 to wireline network (WLN) 110, and to be remotely configurable by a PSP. An authorized user also can be PSS Guest 123. Guest 123 can communicate using dual mode mobile station

(DMMS) 125. DMMS 125 can be configurable to communicate, in a first mode, with DMAP 120 over USW 117 and, in a second mode, with MWSP 105 over SRAN 108. DMSS 125 need not be configured to communicate in both modes simultaneously. DMMS 125 may be a supplicant wireless device, e.g., as it seeks to associate with DMAP 120, or may be an associated device, e.g., after association is completed. It is desirable to adapt DMAP 110 to be configurable as a remotely managed CPE using a remote CPE management technique, such as the aforementioned techniques for remotely managed CPE. Using DMMS 125 in communication with the DMAP 120, Guest 123 can request, and may be authorized to receive, a predefined PWS allocation unit, hereafter, a PWS token 127, requested from one of MWSP 105, PSV 112, and PSS 115. DMAP 120 can be configured to employ a first predefined authentication technique, in which DMAP 120 authenticate the identity of DMMS 125 and, upon DMMS 125 authentication by the predefined authentication technique, to provision PWS token 127 to DMMS 125. Alternatively, DMAP 120 can be configured to facilitate PWS provisioning by employing a second predefined authentication technique, in which DMAP 125 passes authentication credentials obtained from DMMS 125 through to a provisioned service provider (PSP), including one of MWSP 105 and PSV 112. Upon authentication of DMMS 125, the PWS provisioner can transmit PWS token 127 to DMAP 120, which can pass PWS token 127 to DMMS 125.

[0016] In general, DMAP 120 can implement link-layer and device-level authentication, as described by IEEE Std. 802.11 (1999) and by IEEE Std. 802.1X, including WEP, WPA, WPA2, MAd filtering, and the like. See, for example, the white paper entitled: "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite" (October 2003) at URL: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodli t/wswpf_wp.pdf (verified March 21, 2006), hereinafter referred to as "A Comprehensive Review." However, provisioned service providers may demand user-level authentication of supplicant guest 123 attempting to access provisioned services, so that the identity of guest 123 is verified. To this end, it may be convenient to implement selected embodiments of the present invention to provide user-level authentication. User-level authentication implementations are well-known in the converged arts art of computer and network security, as may be typified in "A Comprehensive Review", as well as in the Broadcom Corporation White Paper entitled "Securing Home Wi-Fi® Networks: A Simple Solution Can Save Your Identity," Wireless-WP200-x, (May 18, 2005) at URL http://www.54g.org/pdf/Wireless-WP200-RDS.pdf(verified March 21, 2006); and in the Cisco Systems, Inc. Application Note, entitled: "802.1x and EAP-Based Authentication Across Congested WAN Links," March 2002, at URL http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit /authp_an.pdf (verified March 16, 2006). The foregoing references are hereby incorporated by reference herein in their entirety, but are exemplary, are not to be considered inclusive or limiting examples.

[0017] Also, effective security implementations in a wireless/USW environment can include successive layers of constituent security processes, sequences of constituent security processes, and combinations thereof. In a fixed wireless environment/USW, one device-level authentication implementation, e.g., OSA, effects connectivity between devices in the physical link layer, but is susceptible to breach when viewed from the perspective of a logical, end-to-end implementation. Other device-level authentication methods, such as MAC filtering, can provide an appropriately greater degree of security than OSA, but are not intended to verify the identity of the entity using the device. In this instance, entity authentication techniques may be used to verify the identity of the entity by comparing identification information provided by the entity to the content of a known and trusted information repository. User-level authentication is a form of entity authentication capable of being adapted to the fixed wireless/USW environment, in which the user of a USW supplicant device can provide a credential verifiably asserting the user's identity.

[0018] Embodiments of the present invention can be adapted to implement horizontal and vertical constituent and executive security processes which cooperate to identify one of the authentication state, indicating whether guest 123 has proven its identity through DMMS 125, and the eligibility state, indicating whether DMMS 125 is a supplicant device eligible to receive provisioned wireless services. In selected exemplary embodiments, it is desirable to configure an authenticator, such as local authenticator 150 to implement link-layer, and device-to-device, authentication and identification. Relative to link layer and device-to-device authentication, local authenticator can determine whether supplicant device DMMS 125 is as mobile device, which may be allowed to associate with DMAP 110, and which potentially may be eligible to request provisioned services. The inventive embodiments herein desirably provide remote CPE configuration of local authenticator 150 by provisioned service providers MWSP 105 and PSV 112, by which local authenticator 150 can be configured to implement user-level authentication. In exemplary embodiments, guest 123 may be authenticated at a user level to receive provisioned wireless services using DMMS 125. Local authenticator 150 can challenge a supplicant, such as DMMS 125, to prove its identity, with the result of the challenge being represented by an authentication state. DMMS 125 can communicate to DMAP 110 a pass code entered by guest 123. Local authenticator 150 can evaluate the pass code to determine an authentication state with respect to guest 123. If the authentication state of DMMS 125 indicates that the identity of guest 123 using DMMS 125 is authenticated, then local authenticator 150 may use the identification information to further qualify supplicant device DMMS 125 for eligibility to received selected pro-

visioned services. The term eligibility can comprehend product capabilities as well as service or QoS features that may be available to guest 123 under term of a provisioned service subscription agreement, which agreement may be made between PSS 115 and PSV 112 or MWSP 105.

[0019] Embodiments of the present invention can effect one or both of authentication and provisioning, at least in part, by securely transmitted authentication, authorization, and provisioning information from upstream provisioned service providers including, without limitation, MWSP 105 and PSV 112. In contrast, authentication and other security mechanisms and methods that operate autonomously within the local communication range of an access point, typically have at least one non-secure broadcast, through which an interloper or miscreant may be able to gain access to the network broadcasting its availability. Furthermore, in some local authentication schemes, an access point is adapted to allow the device-level authentication, linking and association of other supplicant mobile stations that may present acceptable device-level authentication or identifying credentials to the soliciting access point, within an activation or accession period. These schemes may permit interloping or miscreant mobile stations may be among the plural supplicant devices. Advantageously, embodiments of the present invention can limit accession by supplicant devices by terminating access point activation upon successful authentication of a supplicant device, even if the authentication period of predetermined length has not elapsed.

[0020] Thus, PWS authentication according to embodiments of the present invention, can provide a secure authentication process by which the identity of Guest 123 using DMMS 125 is verified. Although embodiments of the present invention are conveniently illustrated in the context of access points, such as DMAP 120, which are capable of providing one or both of multiple SSID and BSSID, it must be understood that PWS authentication can be implemented with DMAP 120 providing a single SSID, a single BSSID, or both. In such an instance, differentiation between provisioned and non-provisioned services (e.g., VoIP and ISP data, respectively) can be implemented in a component or function cooperating with DMAP 120, such as a router (not shown) capable of managing data packets tagged or identified by content or requisite QoS. DMAP 120 may operate with PWS authenticated mobiles stations such as DMMS 125 and may reject traffic from non-PWS-authenticated mobile stations. In such a case, DMAP 120 may accept all traffic from the PWS-authenticated client, with the router (not shown) coupled thereto, managing service differentiation. Router service differentiation, for example, may be accomplished by using internal queueing policies, by priority handling techniques generally guided by IEEE Stds. 802.1p or 802.1q, or by combinations thereof. The router (not shown) may be configured to differentially manage provisioned traffic from a PWS-authenticated mobile station, such as DMMS 125, and also may offer virtual LAN (VLAN) functions. The aforementioned IEEE Stds. 802.1p and 802.1q are hereby incorporated herein in their entirety. DMAP 120 may be configured to accept provisioned service traffic from one or more PWS-authenticated mobile stations, such as DMMS 125, and to reject non-provisioned service traffic. DMAP 120 also may be a constituent of a multifunction dual-mode wireless service apparatus in which the aforementioned router (not shown) also is a constituent device cooperating with DMAP 120.

[0021] Also disposed on the premises of PSS 115 can be subscriber home network (SHN) 140, which may subsume, and may be at least partially co-located with USW 117. SHN 140 home can include subscriber home telephone 142. If telephone 142 is an analog device, an adaptor such as foreign exchange system gateway (FXS) 144, may be coupled between SHN 140 and telephone 142. An FXS gateway can be adapted to connect a standard analog telephone or fax machine to a digital, IP-based data networks, and can be exemplified by Linksys® SPA1001 Phone Adapter, produced by Cisco/Linksys®, Irvine, CA. FXS 144 enables a user to communicate with other digital communication devices to which FXS 144 is coupled, such as DMAP 120. Advantageously, using an adaptor such as FXS 144, PSS 115 can use telephone 142 to remotely control, configure, and operate DMAP 120, at least in part, including supplying activation and security codes to DMAP 120. Conveniently, telephone 142 may be located in a room or office, on the premises of PSS 115, remote to DMAP 120 but coupled to SHN 140. SHN 140 also may include computer 146, irrespective of type or configuration (e.g., desktop, laptop, personal digital assistant), or mode of connection (e.g., wired or wireless). DMAP 120 may Computer 146 may be dispositioned with the appropriate hardware and software, which may be useful in communicating with, and at least partially configuring, DMAP 120. Also, PSS 115 may have, as part of SHN 140, wireless handset 148, which may possess dual mode mobile station functionality, or may operate as a communicating device on USW 117. Handset 148 may be adapted to allow PSS 115 to modify a configuration of DMAP 120. DMAP 120 further may be a constituent of a multifunction dual mode wireless service apparatus, which includes one or more functions of an analog telephone adaptor (ATA), having FXS and outgoing foreign-service office (FXO) features, but which may be adapted to receive signals from analog telephony devices coupled thereto, which signals can be used to modify or configure the operation or function of DMAP 120, including activating DMAP 120 for an authentication period.

[0022] DMAP 120 can include subscriber interface 160, transceiver 155, and local authenticator (LA) 150. Desirably, subscriber interface 160 includes features such as manual entry keys, and a display, which may be a screen display or other display providing DMAP-related information and feedback to PSS in a visually perceivable

format. Advantageously, all or part of subscriber interface 160 may be provided in hardware, software, or an operable combination thereof. In addition, subscriber interface 160 may be a distributed interface, in that a portion of interface 160 can be implemented on computer 146, for example, in a web browser interface. This convenient functionality can allow PSS 115 to remotely control, configure, and operate DMAP 120, at least in part, including supplying activation and security codes to DMAP 120. Conveniently, computer 146 may be located in a room or office, on the premises of PSS 115, remote to DMAP 120 but coupled to SHN 140. Typically, DMAP 120 includes transceiver 155, configured to bidirectionally wirelessly communicate with associated and supplicant wireless devices, including DMMS 125. DMAP 120 also may wirelessly communicate with computer 146 and PSS wireless handset 148 if the respective devices are configured and disposed to do so. Local authenticator (LA) 150 is a processing unit of DMAP 120, adapted to perform one or more of effecting association of supplicant wireless devices with DMAP 120 in the context of USW 117; facilitating recognition, verification, and differentiation of signals from associated devices; and to preserve and manage connectivity among associated devices coupled to DMAP 120. Moreover, LA 150 can be adapted to authenticate, in a first authentication mode, or to facilitate authentication, in a second authentication mode, of supplicant devices including DMMS 125. Also, upon authentication of DMMS 125, LA 150 can be configured to provision PWS token 127 to DMMS 125, or to pass PWS token 127 to DMMS 125, after DMMS 125 is authenticated by a PSP, such as MWSP 105 or PSV 112.

[0023] It may be desirable to differentiate between PWS and non-provisioned services, with the latter being provided, for example, by ISP 129. It also may be desirable to further differentiate between different types or classes of PWS provided by the same PSP (e.g., MWSP 105, PSV 112) or between the same type or class of PWS provided by a first PSP, e.g., MWSP 105, and a second PSP, e.g., PSV 112. To facilitate explanation of differentiated service management, PWS hereafter are referred to a "voice services," and non-provisioned services hereafter are referred to a "data services." Currently, wireless devices such as DMAP 120, typically employ a unique, typically alphanumeric, identifier, called a service set identifier (SSID) that wireless networking devices use to establish and to maintain wireless connectivity. Multiple access points on a network or sub-network, including DMAP 120, can use the same SSID to identify the particular wireless network which it forms or with which it is associated. An access point, including DMAP 120, also can employ a unique identifier, namely a basic service set identifier (BSSID) to distinguish itself from other wireless network access points. DMAP 120 can be configured with a basic service set, relative to wireless networking devices, such as DMMS 125, which may seek to associate with DMAP 120. By extension, the basic service set of DMAP 120 may be uniquely identified with a basic service set identifier (BSSID) that may be used in a manner similar to a medium access controller (MAC) address relative to other base stations. Embodiments of the present invention can be implemented where DMAP 120 is capable of producing a single SSID, which implementation may provide one undifferentiated service channel adapted to convey both provisioned data and non-provisioned data. Desirably, DMAP 120 can be capable of producing multiple SSIDs and BSSIDs. Exemplary access points capable of producing multiple, configurable SSIDs include the CISCO AIRONET 1100 Series Access Point, the LINKSYS WRTP54G Wireless Router with VoIP, and the LINKSYS WAP54GP Wireless-G Access Point, both available from Cisco Systems, Inc., San Jose, California.

[0024] In that regard, DMAP 120 may be configured to have a data-service BSSID (dBSSID 170) to identify a basic service set established for non-provisioned signal (e.g., data) communication; and a host voice-service BSSID (hvBSSID 180) to identify a basic service set established for signal communications related to provisioned wireless services, e.g., voice services. Separation of data and voice services can be advantageous when it is desirable, as here, to separately manage non-provisioned and provisioned traffic. Thus configured with plural BSSIDs, DMAP 120 can perform content filtering. In addition, it may be desirable to assign multiple hvBSSIDs 180 to DMAP 120, permitting further differentiation of provisioned services, for example, based upon predefined content characteristics. LA 150 also can include data service interface 162 and provisioned service interface 164. Data service interface 162 generally recognizes and processes data and non-provisioned service content, such that PSS 115 may have control over, and associated privacy of, the content of signals directed to dBSSID 170. Data service interface also can process traffic from SHN 140, and can direct voice service signals therefrom to provisioned service interface 164. Provisioned service interface 164 generally recognizes and processes provisioned service content, such as voice services, such that the respective PSP (e.g., MWSP 105 or PSV 112) has control over the content of signals directed to hvBSSID 180.

[0025] Desirably, vBSSID numbers may be assigned in a manner similar to MAC addresses, i.e., a range of vBSSID values for dual-mode access points, such as DMAP 120, can be allocated to defined entities, such as a PSV 112 or mobile wireless service provider (MWSP) 105. Thus, each dual mode access point, such as DMAP 110, may be provided with at least one respective unique vBSSID, such as hvBSSID 180. Typically, BSSIDs are programmable into an access point and, thus, DMAP 120 may have hvBSSID 180 pre-assigned thereto, for example, before it is placed in USW 117 for use by PSS 115. Alternately, a PSP, such as MWSP 105, or PSV 112, may remotely configure DMAP 120 by assigning a unique hvBSSID 180 as part of a registration process, and thereby establish provisioned service filtering, e.g., voice-

Samsung Ex. 1004, Page 548 of 563

service filtering, in DMAP 120. The registration process may be part of aforementioned CPE configuration and management process, in accordance with a remote management protocol, such as TR-069 CPE WAN Management Protocol. In this example, it is desirable to include in DMAP 120 managed CPE device interface 190 that can initiate and maintain filtering to implement differentiated content management, in accordance with CPE-side configuration management and maintenance functions, similar to those described in DSL Forum Technical Report TR-064. In a particular example, through the facility of interface 190, a PSP, such as MWSP 105 and PSV 112, may remotely provision services and functions of DMAP 120 in accordance with provisioning parameters for VoIP CPE services (e.g., DSL Forum Technical Report TR-104), with VoIP signals being processed differentially from others, and managed according to a VoIP provisioning agreement between the selected PSP and PSS 115. With voice-service filtering, signals received over USW 117 and directed to hvBSSID 180 can be managed, metered, and transmitted over WLN 110 to the respective PSP, e.g., PSV 112 or MWSP 105. Suitable voice signals for such voice-service filtering, can include voice-over-Internet-Protocol (VoIP) signals, as well as related voice traffic, such as voice-over-WLAN (VoWLAN) signals. Advantageously, signals not directed to hvBSSID 180 may not be controlled, altered, or affected by voice-service filtering. Accordingly, the radio set of DMAP 120, as represented of transceiver 155, may establish and manage a voice channel for provisioned voice signals (e.g., VoIP signals) separately from a data channel for non-provisioned signals (e.g., bulk data packet signals). Interface 190 may conveniently be disposed and operable within LA 150.

[0026] DMAP 120 may broadcast to indicate availability to provide wireless service. While broadcasting, DMAP 120 can transmit over voice channel 182, for example, a voice beacon bearing vSSID 178 to supplicant devices, associated devices, or both, thereby identifying voice channel 182. Similarly, DMAP 120 can transmit over data channel 184, for example, a data beacon bearing dSSID 172 to supplicant devices, associated devices, or both, thereby identifying data channel 184. Accordingly, an exemplary supplicant wireless device, which may be DMMS 125, can identify an appropriate channel 182, 184 over which to communicate with DMAP 120. Exemplary DMAP 120 can provide, through voice service interface 135, a voice-service channel typically identified by vSSID 150 and, through data service interface 137, a data-service channel typically identified by dSSID 155.

[0027] It can be expedient to allocate and assign a range, or block, of vBSSID values to an identified DMMS entity including, for example, a DMMS manufacturer, DMMS distributor, DMMS vendor, DMMS service provider, PSV 112, and MWSP 105. By associating a vBSSID in this way, gvBSSID 195 may be indicative of the provider of DMMS 125, its corresponding service capabilities, and its corresponding appliance feature sets (e.g., VoIP, MMS, video, GPS). Beneficially, DMMS 125 can be assigned unique vBSSID, for example, gvBSSID 195, as a virtual MAC address corresponding to and identifying DMMS 125. gvBSSID 195 may indicate that DMMS 125 corresponds to a series of VoIP-capable appliances of a particular manufacture; is capable of SIP-based VoIP messaging; and was supplied to guest 163 within the context of an agreement with PSV 112. Embodiments of the present invention can be implemented to configure DMAP 120 to provision, to accept, or to reject specific services to selected gvBSSID identifiers. Selection or rejection of a particular gvBSSID may be accomplished using well-known MAC filtering techniques or functional equivalents thereof. For example, DMAP 120 can be configured by PSV 112, to reject voice-service requests from those DMMS bearing gvBSSID identifiers which denote dual-mode appliances not within the scope of a voice-service agreement with PSV 112. MWSP 105 and other PSP may be able to similarly interact with DMAP 120, or the remotely managed functions of DMAP 120 may be exclusively under the control of PSV 112.

[0028] For numerous reasons, Guest 123 may wish to receive authorization to use PWS on DMMS 125. One exemplary reason may arise from DMMS 125 being located out of range of signals from SRAN 108. For example, Guest 123 may be indoors or may be in a foreign geographic region where RAN signals compatible with DMMS 125 may be unavailable. USW 117 may be disposed in a public venue such as an airport or large shopping plaza, for example, and PSS 115 may operate USW 117 in that venue. USW 117 also may be disposed outdoors, owing to the deployment of fixed wireless "neighborhood area" or "metropolitan area" networks currently undergoing widespread deployment, as well as more robust WiFi™ equipment. Conveniently, Guest 123 may be able to communicate with DMAP 120 over USW 117 using DMMS 125, and thus may seek to be provisioned with PWS, including, for example, an allocation of VoIP services, in order to make and receive calls while in range of USW 117 or a compatibly interoperating USW. Similarly, Guest 123 may wish to receive non-voice PWS (e.g., priority stock market feeds available from PSV 112), which may not otherwise be available to Guest 123 through services offered by PSS 115 through ISP 129. Alternatively, Guest 123 may be a guest in the private home of PSS 115, and PSS 115 may wish to transfer PWS token 127 to DMMS 125 of Guest 123. PWS token may be representative of a portion of preallocated PWS or credit for PWS, for which accounting may be maintained in DMAP 120 for PSS 115, or in a PWS account of PSS 115 managed by a PSP, such as MWSP 105 or PSV 112.

[0029] Beneficially, DMMS 125 can be configured to facilitate DMAP 120 with provisioning voice service (as an exemplary PWS) to DMMS 125 by adapting to communicate voice signals through provisioned service interface 164 by way of DMAP voice channel 182, which may be identified by vSSID 178. Similarly, DMMS 125

Samsung Ex. 1004, Page 549 of 563

may seek to associate with DMAP 120 and to communicate data signals through data service interface 162, using data channel 184 that can be identified by dSSID 155 and be configured separately and distinctly from voice channel 182. As indicated above, some form of authentication can be desirable for wireless communication services, particularly for provisioned services, such as voice services (e.g., VoIP services), which may use a potentially vulnerable wireless link. DMMS 125 may facilitate DMAP 120 provisioning of voice services by supplying to DMAP 120 identifying credentials during association supplication or upon request of DMAP 120. Identifying credentials may include a predetermined pass code, a predefined unique supplicant device identifier, and a combination thereof. DMAP 120 may store therein one or more pass codes and one or more predefined unique supplicant device identifiers corresponding to wireless devices that may be authenticated to DMAP 120. Authentication of DMMS 125 to DMAP 120 can be designated "PWS authentication." By providing identifying credentials, PWS authentication of the identity of supplicant device DMMS 125 can be simplified, potentially expediting authorization of DMMS 125 to be provisioned with PWS. It also may be beneficial to perform a "pre-access authorization," which may include, for example, authenticating the identity of Guest 123 using well-known authentication methods, with a successful pre-access authentication being followed by PSS 115 providing Guest 123 a PWS authentication pass code.

[0030] In a particular example of advantageous inventive embodiments herein, Guest 163 may desire to use DMMS 125 through DMAP 120 to receive provisioned voice services (e.g., VoIP) across USW 117. Although DMMS 125 may be able to couple to mobile wireless link 109 to receive voice services from MWSP 105, Guest 123 may wish to place a VoIP call through DMAP 120 and across WLN 110, perhaps because of a lower tariff charged by MWSP 105 for IP-based traffic. PSV 112 may be capable of provisioning PWS, such as VoIP voice service, to DMMS 125, for example, as a discount vendor of MWSP 105 services. PSV 112 may coordinate such third party provisioning with the MWSP AAA entity 103, so that DMMS 125 can be authorized to make and receive VoIP calls using the facilities of MWSP 105. Typically, communications between PSV 112 and MWSP AAA 103 are made using secure communication techniques, with safeguards against Internet interlopers and miscreants. Both PSV 112 and MWSP AAA 103 may decline to provision PWS requested by an outside party, such as Guest 123, unless sufficient safeguards are undertaken, including authenticating the identity of a requester, of the supplicant device for which the provisioned service is requested, or both. Therefore, to satisfy a desire of MWSP 105 and PSV 112 for secure access to provisioned services, it may be expedient to provide authentication of supplicant device DMMS 125 as it requests to be provisioned, PWS through DMAP 120, including voice service over IP-based WLN 110. PSS 115 also may desire safeguards operable with DMAP 120 to reduce the likelihood of intrusion into USW 117 by a miscreant seeking to misappropriate or misuse assets associated with DMAP 120, including for example, PWS token 127 or sensitive data and access information of PSS 115, relating to service provisioning through DMAP 120 with a PSP. At the same time, from the perspective of Guest 123 and also of PSS 115, it can be desirable to simplify the mechanics of these safeguards, particularly in scenarios where PSS 115 and Guest 123 can cooperatively operate DMAP 120 and DMMS 125, respectively, to facilitate PWS authentication of DMMS 125 for PWS provisioning, including supplying PWS token 127. In one exemplary scenario, which may be useful in circumstances where PSS 115 is a business owner offering a hotspot to customers or other transient persons, PSS 115 can verify the identity of Guest 123, that is perform pre-access authentication of Guest 123, using an identification credential such as a vehicle operator's permit (i.e., driver's license), a passport, or other form of identification suitable for the level of security desired. Biometric and other physical personal authentication techniques may be used in addition or in substitution. PSS 115 may not require Guest 123 to produce an identification credential for pre-access authentication, for example, where Guest 123 is a long-time customer, or where USW 117 is disposed in the home of PSS 115 and Guest 123 is person known to PSS 115. Upon a satisfactory pre-access authentication, or if PSS 115 is willing to proceed based on trust of Guest 123, then PSS 115 may offer Guest 123 an identification credential to be used with DMMS 125 during PWS authentication, that is, when Guest 123 operates DMMS 125 to request PWS from a PSP. Pre-access authentication may be a constituent process component of a simple but exemplary PWS authentication method embodiment according to the present invention. However, it is to be understood that PWS authentication of Guest 123 using DMMS 125 by DMAP 120 according to embodiments of the present invention is desirably a user-level authentication that does not require pre-authentication.

[0031] An exemplary PWS authentication method embodiment according to the present invention may proceed when PSS 115 activates DMAP 120 by depressing single key 177. Conveniently, activation key 177 may be dedicated to facilitating association of DMMS 125 with DMAP 120. In response to activation by key 177, DMAP 120 may broadcast, for a predefined authentication period, a voice beacon bearing vSSID 178 on voice channel 182. It can be beneficial to limit the predefined authentication period, for example, to about three minutes, to provide sufficient time for DMMS 125 to perform USW-authentication and to become associated with DMAP 120, yet to minimize the ability of a miscreant or interloper having a USW-capable device from associating with DMAP 120. The actual length of the predefined authentication period may be adjustable to meet the operating environment in which DMAP 120 is deployed. During the predefined authentication period, DMMS 125 can simi-

Samsung Ex. 1004, Page 550 of 563

larly be activated, for example, by Guest 123, causing DMMS 125 to become a supplicant device to the wireless network (USW 117) represented by DMAP 120, identifiable by broadcasting a supplicant device probe request frame on every available USW radio channel, including DMAP 120 voice channel 182. In response, DMAP 120 can transmit a voice beacon over voice channel 182 bearing vSSID 178, as a probe response frame. DMMS 125 then may select DMAP 120 for voice-service access and may send an open authentication request, a form of USW-authentication, to DMAP 120. Typically, open authentication is directed to facilitating connectivity and, once in communication with DMMS 125, LA 150 in DMAP 120 can provide a favorable authentication reply to DMMS 125. Upon successful USW-authentication, DMMS 125 may send an association request frame to DMAP 120, transmitting gvBSSID 195, which also may indicate a request to be provisioned voice-service, for example, in the form of PWS token 127 by DMAP 120, where DMAP 120 is configured to provision PWS token 127, or through DMAP 120 over data network link 120, where a PSP such as MWSP 105 or PSV 112 may be designated to engage DMMS 125 in AAA functions to establish authorization to be provisioned the requested wireless service (e.g., voice service). DMAP 120 may have stored therein gvBSSID 195, corresponding to DMMS 125, and it may be sufficient for selected embodiments of PWS authentication methods that gvBSSID 195 identifies DMMS 125 as a dual-mode device, which can be permitted to request, and to be provisioned PWS token 127 and that receipt by DMAP 120 of an identification credential from DMMS 125, in the form of gvBSSID 195, can authenticate supplicant device DMMS 125 to DMAP 120. If the request of DMMS 125 is unsuccessful (e.g., signal loss or authentication failure) during the predefined authentication period, DMAP 120 may permit to DMMS 125 having gvBSSID 195, to continue authentication and association attempts, until the predefined authentication period expires, while denying access to other supplicant devices seeking access but without gvBSSID 195.

[0032] Alternatively, PSS 115 may enter a host pass code into DMAP 120 by way of interface 160, which is stored by LA 150 during a predefined authentication period. PSS 115 can issue to Guest 123 a guest pass code that is the same as, or corresponds to, the host pass code entered by PSS 115 into DMAP 120. As Guest 123 activates DMMS 125 to become a supplicant device, Guest 123 enter the guest pass code into DMMS 125. When DMMS requests to associate with DMAP 120 during the authentication period, DMMS 125 can undertake a USW-authentication with DMAP 120, in accordance with the network authentication and encryption protocols employed in USW 117. In addition, DMMS 125 can implement an embodiment of the inventive PWS authentication methods by transmitting the guest pass code to DMAP 120. LA 150 can process the guest pass code received from DMMS 125 and compare it with the host pass code supplied by PSS 115. Upon a favorable comparison, DMMS 125 can be considered to be an authenticated device. DMMS 125 may transmit gvSSID 195 along with the guest pass code as a component of the PWS authentication identification credentials, or may transmit gvBSSID 195 subsequently, after LA 150 indicates a favorable comparison of guest pass code to stored host pass code. It pre-access authentication is employed to authenticate the identity of Guest 123, then pass code-type PWS authentication of DMMS 125 can be sufficient to infer verification of the identity of Guest 123, if such security is indicated. Otherwise, pass code-type authentication can be sufficient to verify the identity of DMMS 125. Foreseeable variations of the foregoing authentication techniques may be employed, including using biometric authentication devices coupled to DMMS 125 or DMAP 120, for example, as an adjunct to or in substitution for, codes provided by PSS 115. Even if USW-authentication and PWS authentication processes are successfully completed between DMAP 120 and DMMS 125, a successful exchange of encryption keys, such as through a WEP security encryption protocol, may be additionally implemented to permit DMMS 125 to successfully exchange voice services through DMAP 120 over wired network 120. As used herein, the term USW-authentication can include network authentication and encryption protocols such as, without limitation, WEP, WPA, WPA2, IEEE Std. 802.11i, IEEE Std. 802.1x, RADIUS, and EAP security protocols.

[0033] Although the identity of DMMS 125 may be verified, it may not be authorized (or capable) of receiving the requested PWS. Thus, LA 150 may examine gvBSSID 195 to determine whether the identity of DMMS 125 corresponds to a type of DMMS permitted to receive PWS token 127. Alternatively, DMAP 120 may direct gvBSSID 195 as an identifying credential to the PSP identified as being designated to provision PWS for requests coming from DMAP 120. e.g., PSV 112. Also, DMAP 120 may be configured by PSV 112, to examine gvBSSID 195 and to determine whether to provision DMMS 125 with requested PWS (e.g., voice services) over WLN 110, once DMMS 125 has been PWS-authenticated. In addition, embodiments of the present invention may receive or request from DMMS 125 other information which may be pertinent to determining whether to provision PSW to authenticated device DMMS 125, for example, whether authenticated device DMMS 125 is associated with an active subscription between Guest 123 and the provisioning PSP, the class of service requested, QoS requirement, the number of tokens to be allocated, etc. In certain exemplary embodiments of PSW authentication, DMAP 120 may use gvBSSID 195 to perform a type of MAC address authentication, in which the gvBSSID 195 of DMMS 125 is verified against a locally configured list of allowed guest vBSSIDs, or against AAA information maintained on an external authentication server, for example, of PSV 112, MWSP 105, or of MWSP AAA 103 (for convenience, simply "PSV 112"). Alternatively, as

Samsung Ex. 1004, Page 551 of 563

another embodiment of PSW authentication, DMAP 120 may communicate gvBSSID 195 to PSV 112, where approval or rejection of DMMS 125 may be made, based on a variety of criteria. Moreover, DMAP 120 may be configured to permit enrollment of selected DMMS 125, that is, to enter gvBSSID 195 on the locally configured list of DMAP 120, or to facilitate enrollment of DMMS 125 by forwarding gvBSSID 195 to PSV 112. Enrollment may permit DMAP 120 or PSV 112 to grant or transfer PWS access credits, including representations thereof (e.g., PWS token 127), to DMMS 125, which may permit DMMS 125 to receive voice services (e.g., make and receive VoIP calls) through DMAP 120, or to otherwise be provisioned by PSV 112 to use voice services over suitable USW other than USW 117. If DMAP 120 confirms, or is notified by PSV 112, that DMMS 125 is permitted to associate with DMAP 120, then USW-authentication may be employed. In alternative embodiments of the present invention, USW-authentication may be performed prior to PSW authentication.

[0034] FIG. 2 illustrates an embodiment of an authentication method 200 according to the present invention, namely, subscriber-provisioner DMAP PWS authentication method 200, which also may feature PWS provisioning. FIG. 2 is described with respect to FIG. 1 and the reference numerals of FIG. 2 refer to like entities in FIG. 1. Method 200 may be beneficial, for example, when a voice-services subscriber seeks to facilitate and manage the allocation of provisioned voice and selected IP services to a guest, while selectively controlling provisioning functions at the subscriber location. Method 200 may also be desirable, for example, to a small business owner, for example, PSS 115, hosting a wireless networking hotspot, for example, USW 117, through which allocation units of VoIP and other provisioned services may be purchased by customers of the small business. As used with respect to FIG. 1, a voice-service allocation unit can be designated as a "token," such as PWS token 127. Pursuant to a request or agreement by PSS 115, DMAP 120 may be authorized and configured (Step 205) by a PSP, such as PSV 112 or MWSP 105, to seek voice-service requests from supplicant devices, such as DMMS 125, and to offer to authenticated supplicant devices PWS token 127, which can be a voice-service token.

[0035] Once configured, the PSP may supply DMAP 120 with PWS tokens or functional equivalents (Step 210), which may be requested by Guest DMMS. It may be beneficial for PSS 115 to purchase selected quantities of PWS token 127, perhaps at a discount, for example, through a volume-purchaser discount agreement with a preselected PSP, e.g., MWSP 105. In addition, PSS 115 may have a defined block of provisioned service credits (e.g., PWS tokens 127) associated with an account with MWSP 105, which may be managed by MWSP AAA unit 103 and which may be supplied to properly authenticated supplicants, for example, who request PWS. Therefore, MWSP 105 can authorize DMAP 120 (step 205) to offer a defined quantity of PWS tokens to properly authorized and authenticated guest devices, such as DMMS 125. MWSP 105 also may associate with DMAP 120 a predetermined number of PWS token 127 for provisioning to DMMS 125, in addition to performing other configurations to DMAP 120, for example, in accordance with CPE management protocols, e.g., TR-064, TR-069, and TR-104.

[0036] In embodiments of PWS authentication method 200, subscriber PSS 115 can activate DMAP 120 (Step 215), for example, by entering a pass code. When activated, DMAP 120 can be enabled to broadcast availability for association requests and to accept requests for association from supplicant devices for a predefined authentication period (step 220). During the predefined authentication period, DMAP 120 can broadcast vSSID 178 (step 225) to indicate its availability for voice-service calls 182. A supplicant device, such as DMMS 125 may reply to DMAP 120 by supplying identifying credentials which may include, or be supplemented by, one or both of a pass code or gvBSSID 195 (step 230). Desirably, PSS 115 can provide the pass code to Guest 123, who enters the pass code into DMMS 125. DMAP 120 can receive the request to associate, along with the pass code, transmitted by DMMS 125, within the predefined authentication period. DMAP 120 can employ LA 150 to evaluate the identifying credentials received from DMMS 125, for example, to perform PWS authentication (step 235). Step 235 also may include USW-authentication. If the pass code supplied by DMMS 125 satisfactorily compares with an authentication credential stored in a first memory in DMAP 120 during the authentication period, then DMMS 125 can be considered to be authenticated. If, on the other hand, the comparison is unsatisfactory, DMMS 125 may reattempt to be authenticated within the predefined authentication period. The authentication period may be terminated once the authentication of DMMS 125 is successful, for example, to deter interlopers. The (first) authentication credential can include the pass code provided to Guest 123 by PSS 115; an authentication certificate, identifier, or symbol supplied securely by MWSP 105 or PSV 112; or a combination thereof. DMMS 125 also may supply DMAP 110 with an additional identifying credential concurrently with the pass code, or in response to a communication separate in time from DMMS 125 supplying the pass code. Exemplary additional identifying credentials include, without limitation, gvBSSID 195, a PWS subscriber identifier (not shown), and a unique personal identifier, such as a vehicle operator's license). LA 150 can include a second memory in which to store a second authentication credential, used to evaluate an additional identifying credential. In selected embodiments of the present invention, successful PWS authentication may be completed after LA 150 verifies the pass code, the additional identifying credential, or both.

[0037] Upon successful authentication of the identifying credentials of DMMS 125, it is desirable to determine whether supplicant device DMMS 125 is a supplicant device suitable to be granted access to PWS resources

Samsung Ex. 1004, Page 552 of 563

(step 240), including receiving relevant information from DMMS 125, including, for example, gvBSSID 195 and the terms of the PWS request (class of service, QoS, number of tokens, etc.). LA 150 can process the information gathered from DMMS 125 at Step 245, to determine whether DMMS 125 should receive PWS token 127 (step 250), as well as how many PWS token 127 and other terms of PWS provisioning. In embodiments of the present invention, LA 150 may store a list or template of gvBSSID values indicative of wireless devices which may be authorized by MWSP 105 to receive PWS token 127 from DMAP 120. LA 150 also may evaluate gvBSSID 195 to determine whether DMMS 125 is capable of using the requested PWS resources or is limited by capability or by agreement in gaining access to PWS resources. Such a list or template can be dynamically updated via WLN 110 by WMSP 105, or MWSP AAA 103.

[0038] Where LA 150 determines that the PWS request of DMMS 125 can be fulfilled (step 255), then DMAP 125 can provide voice service PWS token 127 to DMMS 125 (step 260), permitting DMMS 125 to use PWS in an allocation corresponding to granted PWS token 127. On the other hand, where LA 150 determines at Step 255 that the PWS request of DMMS 125 cannot be fulfilled, it may be desirable to permit DMMS 125 to re-attempt a request to receive an allocation of PWS before the predefined authentication period elapses (step 220). Once DMMS 125 is provisioned PWS token 127, it may be desirable to terminate the predefined authentication period, for example, to deter miscreant operators of a USW wireless device from seeking to interlope on USW 117 or impermissibly gain access to PWS.

[0039] FIG. 3 illustrates another embodiment of an authentication method 300 according to the present invention, namely subscriber-passthrough DMAP PWS authentication method 300, which also may feature PWS provisioning. Similar to FIG.2, FIG. 3 is described with respect to FIG. 1 and the reference numerals of FIG. 3 refer to like entities in FIG. 1. Method 300 may be beneficial, for example, when a voice-services subscriber seeks to facilitate and manage the allocation of provisioned voice and selected IP services to a guest, while passing through authentication and provisioning functions to a designated PSP, such as MWSP 105 or PSV 112.

[0040] As used with respect to FIG. 1, a voice-service allocation unit can be designated as a "token," such as PWS token 127. Method 300 may also be desirable, for example, to a small business owner PSS 115, hosting a wireless networking hotspot, such as USW 117, but where PSS 115 does not desire to resell PWS tokens. Method 300 also may desirable where PSS 115 operates a home network and wishes to facilitate a request of Guest 123 to receive PWS tokens 127 for DMMS 125, but not to be a host-provisioner. To commence an embodiment of the present inventive methods, namely an embodiment of a subscriber-passthrough DMAP PWS authentication method, subscriber PSS 115 can activate DMAP 120 (Step 310), for example, by entering a pass code. Activation of DMAP 120 can continue for a predefined authentication period (step 320). When activated, DMAP 120 can broadcast vSSID 178 to indicate availability (Step 325) for association requests and to accept requests for association from supplicant devices, including DMMS 125, for example, to make and receive voice-service calls over voice channel 182. A supplicant device, such as DMMS 125, may reply to DMAP 120 by supplying identifying credentials within the predefined authentication period. DMMS 125 identifying credentials may include, or be supplemented by, one or both of a pass code or gvBSSID 195 (step 330).

[0041] Desirably, where a pass code is employed, PSS 115 can provide the pass code to Guest 123, who enters the pass code into DMMS 125. PSS 115 may supply the pass code to Guest 123 subsequent to a successful pre-access authentication. DMAP 120 can receive the request to associate, along with the pass code, transmitted by supplicant device DMMS 125, and can employ LA 150 to evaluate the identifying credentials received from DMMS 125, for example, to perform PWS authentication (step 335). Step 335 also may include USW-authentication, as described with respect to Step 235 in FIG. 2. If the pass code supplied by DMMS 125 satisfactorily compares with the pass code stored in DMAP 120 during the authentication period, then DMMS 125 can be considered to be authenticated. If, on the other hand, the comparison is unsatisfactory, DMMS 125 may reattempt to be authenticated within the predefined authentication period. The authentication period may be terminated once the authentication of DMMS 125 is successful, for example, to deter interlopers. Also, it may be desirable to terminate the authentication period upon a failed authentication attempt.

[0042] Upon successful authentication of the identifying credentials of DMMS 125, it is desirable to determine whether supplicant device DMMS 125 is a supplicant device suitable to be granted access to PWS resources (step 340), which can be indicated by gvBSSID 195. Upon a favorable evaluation of DMMS 125 suitability to access PWS resources, LA 150 may receive DMMS 125 request (Step 345) for a PWS token 127, e.g., a voice service token. The request may include, without limitation, gvBSSID 195 and the terms of the PWS request (class of service, QoS, number of tokens, etc.). LA 150 can pass through (Step 350) gvBSSID 195, and other information, including that collected at Step 345, to a designated PSP, such as MWSP AAA 103 and PSV 112. PSW authentication, as well as provisioning of PSW tokens 127, can be performed and managed (Step 355) by the designated one of MWSP AAA 103 or PSV 112. Such PSP authentication and provisioning may be desirable to Guest 123, for example, where Guest 123 is a subscriber to PWS services of MWSP 105 or PSV 112, and may be using USW 117 and DMAP 120 to access PWS tokens 127, which may be associated with an existing PWS provisioning account of Guest 123 for DMMS

Samsung Ex. 1004, Page 553 of 563

125.

[0043] Upon a favorable authentication and provisioning of PWS tokens 127 on behalf of DMMS 125 at Step 355, the designated PSP may then communicate PWS tokens 127 through to DMAP 120 which, in turn, transmit the requested PWS tokens 127 to DMMS 125 (Step 360). Once DMMS 125 is provisioned PWS token 127 at Step 360, it may be desirable to terminate the predefined authentication period, for example, to deter miscreant operators of a USW wireless device from seeking to interlope on USW 117 or impermissibly gain access to PWS. It also may be desirable to permit DMMS 125 to re-attempt authorization during the predefined authentication period, as well as to terminate the authentication period upon an unsuccessful authentication attempt.

[0044] A variety of hardware and software functions have been described herein. Depending upon the implementation, many of the hardware functions may be emulated using software. Likewise, software functions may be performed using hardware components having hardwired circuitry; and some of the hardware or software functions may be configured using alternative technologies known to skilled artisans, including without limitation, firmware and application specific integrated circuits. The elements in the Figures are to be taken as logical and thus, can be implemented in a consolidated or distributed manner to achieve a desired result.

[0045] Moreover, many alterations and modifications may be made by those having ordinary skill in the art, without departing from the scope of the invention. Therefore, it must be understood that the illustrated embodiments have been set forth only for the purposes of example, and that it should not be taken as limiting the invention as defined by the following claims. The following claims are, therefore, to be read to include not only the combination of elements which are literally set forth, but all equivalent elements for performing the same function in the same way to obtain the same result. The claims are thus to be understood to include what is specifically illustrated and described above, what is conceptually equivalent, and also what incorporates the ideas of the invention.

Claims

1. A fixed wireless (USW) access point (120), comprising:

   a data service interface (162) for processing non-provisioned service content using a data service channel identified by a first Service Set Identifier, SSID (170);
   a provisioned service interface (164) for processing provisioned service content using a provisioned service channel identified by a second SSID (178); and
   a local authenticator (150) configured to perform provisioned wireless service, PWS, authentication for access to provisioned services using the provisioned service channel;
   wherein the local authenticator is configured to be activated by a subscriber;
   wherein the local authenticator is configured to receive an identifying credential from a dual mode mobile station (125);
   wherein the local authenticator is configured to analyze the identifying credential, thereby determining a PWS authentication state resulting therefrom; and
   wherein the local authenticator is configured to one of grant access and deny access by the dual mode mobile station to the USW access point for access to a provisioned wireless service using the provisioned service channel responsive to the authentication state.

2. The USW access point of Claim 1, wherein the access point is configured to accept traffic from a PWS-authenticated mobile station and reject traffic from non-PWS-authenticated mobile stations.

3. The USW access point of Claim 1:

   wherein the provisioned service interface is configured to correspond to a provisioned service basic service set identifiable by a provisioned service basic service set identifier (hvBSSID),

   wherein the hvBSSID corresponds to the second SSID and is configurably unique to the provisioned service interface, and
   wherein the signal communicated with the dual mode mobile station is a provisioned service signal communicated over the provisioned service channel to the USW access point corresponding to hvBSSID, preferably,
   wherein the provisioned service interface is configured to accept the identifying credential within a predefined authentification period and configured to determine an authentification state corresponding to an identifying credential, if accepted within the predefined authentification period.

4. The USW access point of Claim 1, wherein the local authenticator further comprises a managed Customer Premises Equipment, CPE, interface coupled to a provisioned service provider and coupled to the provisioned service interface, the managed CPE interface being remotely configurable by the provisioned service provider, the managed CPE interface modifying differential processing of the provisioned service signal in response to the authentication state.

5. The USW access point of Claim 4, wherein the identifying credential comprises a provisioned service

Samsung Ex. 1004, Page 554 of 563

basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station, and wherein the managed CPE interface is configured to modify differential processing of the provisioned service signal in response to the gvBSSID.

6. The USW access point of Claim 1 configured such that a single keystroke on a key coupled to the provisioned service interface commences the predefined authentification period and activates the provisioned service interface to determine the authentification state corresponding to the identifying credential, if accepted within the predefined authentification period.

7. A method for authenticating to a USW access point (120), a dual mode mobile station (125) seeking provisioning of a provisioned wireless service, PWS, wherein the access point provides access to provisioned and non-provisioned services via respective channels identified by respective Service Set Identifiers, SSIDs (170, 178), the method comprising:

receiving an identifying credential from the dual mode station by the USW access point;
evaluating the identifying credential from the dual mode mobile station by the USW access point relative to an authentication credential stored in the USW access point;
determining a PWS authentification state of the dual mode mobile station corresponding to the identifying credential; and
providing access to a provisioned wireless service via a provisioned service channel following a successful PWS authentication.

8. The method of Claim 7, further comprising:

if the PWS authentication state is authenticated, then receiving a request for a provisioned service token from the dual mode mobile station;
evaluating an eligibility state of the dual mode mobile station for being provisioned a provisioned service token; and
if the eligibility state is eligible, then provisioning the provisioned service token to the dual mode mobile station by the USW access point.

9. The method of Claim 7, wherein evaluating the identifying credential further comprises:

evaluating the identifying credential from the dual mode mobile station by the USW access point relative to a provisioning management configuration received from a managed Customer Premises Equipment, CPE, interface disposed in the USW access point.

10. The method of Claim 7, wherein receiving the identifying credential from the dual mode mobile station comprises receiving the identifying credential from the dual mode mobile station within a predefined authentification period.

11. The method of Claim 7, wherein the identifying credential comprises a pass code, a provisioned service basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station, or both.

12. A method for authenticating to a USW access point (120) a dual mode mobile station (125) seeking provisioning of a provisioned wireless service, PWS, wherein the access point provides access to provisioned and non-provisioned services via respective channels identified by respective Service Set Identifiers, SSIDs, (170, 178) the method comprising:

receiving a pass code from the dual mode mobile station by the USW access point;
receiving a provisioned service basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station; and
transmitting the pass code and the gvBSSID received by the USW access point to a provisioned services provider, wherein the provisioned services provider determines a PWS authentification state of the dual mode mobile station responsive to the pass code and the gvBSSID, and wherein upon authentification the provisioned services provider provisions a PWS token to dual mode mobile station for accessing a provisioned wireless service via a provisioned service channel.

13. The method of Claim 12, wherein receiving a pass code further comprises receiving the pass code within a predefined authentification period from the dual mode mobile station.

14. The method of Claim 13, wherein subsequent to transmitting to the provisioned services provider, the method further comprises:

receiving the PWS token from the provisioned services provider by the USW access point; and supplying the PWS token to the dual mode mobile station by the USW access point.

Patentansprüche

1. Fester drahtloser (USW) Zugangspunkt (120), umfassend:

eine Datendienstschnittstelle (162) zum Verarbeiten von nicht bereitgestelltem Dienstinhalt unter Verwendung eines Datendienstkanals,

Samsung Ex. 1004, Page 555 of 563

der mit einem ersten Service Set Identifier (SSID) (170) gekennzeichnet ist;
eine Schnittstelle für bereitgestellte Dienste (164) zur Verarbeitung von bereitgestelltem Dienstinhalt unter Verwendung eines Kanals für bereitgestellte Dienste, der mit einem zweiten Service Set Identifier (SSID) (178) gekennzeichnet ist; und
eine lokale Authentifizierungseinheit (150), die zum Durchführen der Authentifizierung von bereitgestelltem drahtlosem Dienst (PWS) für Zugang zu bereitgestellten Diensten unter Verwendung des Kanals für bereitgestellte Dienste konfiguriert ist;
wobei die lokale Authentifizierungseinheit zur Aktivierung durch einen Teilnehmer konfiguriert ist;
wobei die lokale Authentifizierungseinheit konfiguriert ist zum Empfangen eines identifizierenden Berechtigungsnachweises von einer Mobilstation mit zwei Betriebsarten (125);
wobei die lokale Authentifizierungseinheit konfiguriert ist zum Analysieren des identifizierenden Berechtigungsnachweises, wodurch sie einen sich daraus ergebenden PWS-Authentifizierungszustand bestimmt; und
wobei die lokale Authentifizierungseinheit dafür konfiguriert ist, dem USW-Zugangspunkt für Zugang zu einem bereitgestellten drahtlosen Dienst, auf den Authentifizierungszustand reagierend, unter Verwendung des Kanals für bereitgestellte Dienste durch die Mobilstation mit zwei Betriebsarten den Zugang zu gewähren oder den Zugang zu verweigern.

2. USW-Zugangspunkt nach Anspruch 1, wobei der Zugangspunkt zum Akzeptieren von Verkehr von einer PWS-authentifizierten Mobilstation und zum Ablehnen von Verkehr von nicht PWS-authentifizierten Mobilstationen konfiguriert ist.

3. USW-Zugangspunkt nach Anspruch 1:

wobei die Schnittstelle für bereitgestellte Dienste so konfiguriert ist, dass sie einem Basic Service Set eines bereitgestellten Dienstes entspricht, das anhand eines Basic Service Set Identifier für einen bereitgestellten Dienst (hvBSSID) identifizierbar ist,
wobei der hvBSSID dem zweiten SSID entspricht und für die Schnittstelle für bereitgestellte Dienste eindeutig konfigurierbar ist und
wobei das mit der Mobilstation mit zwei Betriebsarten übermittelte Signal vorzugsweise ein Signal des bereitgestellten Dienstes ist, das über den Kanal für bereitgestellte Dienste zu dem USW-Zugangspunkt, der dem hvBSSID entspricht, übermittelt wird,
wobei die Schnittstelle für bereitgestellte Dienste zum Akzeptieren des identifizierenden Berechtigungsnachweises innerhalb einer vordefinierten Authentifizierungsperiode konfiguriert ist und zum Bestimmen eines Authentifizierungszustands konfiguriert ist, der einem identifizierenden Berechtigungsnachweis, wenn innerhalb der vordefinierten Authentifizierungsperiode akzeptiert, entspricht.

4. USW-Zugangspunkt nach Anspruch 1, wobei die lokale Authentifizierungseinheit ferner eine verwaltete Teilnehmernetzgerät- (Customer Premises Equipment,
CEP) -Schnittstelle aufweist, die mit einem Anbieter bereitgestellter Dienste gekoppelt ist und mit der Schnittstelle für bereitgestellte Dienste gekoppelt ist, wobei die verwaltete CPE-Schnittstelle durch den Anbieter bereitgestellter Dienste fernkonfigurierbar ist, wobei die verwaltete CPE-Schnittstelle eine unterschiedliche Verarbeitung des Signals des bereitgestellten Dienstes als Reaktion auf den Authentifizierungszustand modifiziert.

5. USW-Zugangspunkt nach Anspruch 4, wobei der Berechtigungsnachweis einen Basic Service Set Identifier eines bereitgestellten Dienstes (gvBSSID) aufweist, der für die Mobilstation mit zwei Betriebsarten eindeutig konfigurierbar ist, und wobei die verwaltete CPE-Schnittstelle zum Modifizieren einer unterschiedlichen Verarbeitung des Signals des bereitgestellten Dienstes als Reaktion auf den gvBSSID konfiguriert ist.

6. USW-Zugangspunkt nach Anspruch 1, der so konfiguriert ist, dass ein einzelner Tastenanschlag an einer Taste, die mit der Schnittstelle für bereitgestellte Dienste gekoppelt ist, die vordefinierte Authentifizierungsperiode beginnt und die Schnittstelle für bereitgestellte Dienste aktiviert, um den dem identifizierenden Berechtigungsnachweis, wenn innerhalb der vordefinierten Authentifizierungsperiode akzeptiert, entsprechenden Authentifizierungszustand zu bestimmen.

7. Verfahren zur Authentifizierung einer Mobilstation mit zwei Betriebsarten (125), die die Bereitstellung eines bereitgestellten drahtlosen Dienstes (PWS) wünscht, einem USW-Zugangspunkt (120) gegenüber, wobei der Zugangspunkt Zugang zu bereitgestellten und nicht bereitgestellten Diensten über jeweilige Kanäle bereitstellt, die mit jeweiligen Service Set Identifiers (SSID) (170, 178) gekennzeichnet sind, wobei das Verfahren Folgendes aufweist:

Empfangen eines identifizierenden Berechtigungsnachweises von der Station mit zwei Betriebsarten durch den USW-Zugangspunkt;

Samsung Ex. 1004, Page 556 of 563

Bewerten des identifizierenden Berechtigungsnachweises von der Mobilstation mit zwei Betriebsarten durch den USW-Zugangspunkt relativ zu einem im USW-Zugangspunkt gespeicherten Berechtigungsnachweis;
Bestimmen eines PWS-Authentifizierungszustands der Mobilstation mit zwei Betriebsarten, der dem identifizierenden Berechtigungsnachweis entspricht; und
Bereitstellen von Zugang für einen bereitgestellten drahtlosen Dienst über einen Kanal für bereitgestellte Dienste nach einer erfolgreichen PWS-Authentifizierung.

8. Verfahren nach Anspruch 7, das ferner Folgendes aufweist:

wenn der PWS-Authentifizierungszustand authentifiziert wird, dann Empfangen einer Anfrage für ein Token für einen bereitgestellten Dienst von der Mobilstation mit zwei Betriebsarten;
Bewerten eines Berechtigungszustands der Mobilstation mit zwei Betriebsarten dafür, die Bereitstellung eines Tokens für einen bereitgestellten Dienst zu erhalten; und,
wenn der Berechtigungszustand berechtigt ist, dann Bereitstellen des Tokens für einen bereitgestellten Dienst an die Mobilstation mit zwei Betriebsarten durch den USW-Zugangspunkt.

9. Verfahren nach Anspruch 7, wobei das Bewerten des identifizierenden Berechtigungsnachweises ferner Folgendes aufweist:

Bewerten des identifizierenden Berechtigungsnachweises von der Mobilstation mit zwei Betriebsarten durch den USW-Zugangspunkt relativ zu einer von einer verwalteten Teilnehmernetzgerät- (Customer Premises Equipment, CPE) -Schnittstelle, die im USW-Zugangspunkt angeordnet ist, empfangenen Bereitstellungsmanagementkonfiguration.

10. Verfahren nach Anspruch 7, wobei das Empfangen des identifizierenden Berechtigungsnachweises von der Mobilstation mit zwei Betriebsarten das Empfangen des Berechtigungsnachweises von der Mobilstation mit zwei Betriebsarten innerhalb einer vordefinierten Authentifizierungsperiode aufweist.

11. Verfahren nach Anspruch 7, wobei der Berechtigungsnachweis einen Passcode, einen Basic Service Set Identifier für einen bereitgestellten Dienst (gvBSSID), der für die Mobilstation mit zwei Betriebsarten eindeutig konfigurierbar ist; oder beide aufweist.

12. Verfahren zur Authentifizierung einer Mobilstation mit zwei Betriebsarten (125), die die Bereitstellung eines bereitgestellten drahtlosen Dienstes (PWS) wünscht, einem USW-Zugangspunkt (120) gegenüber, wobei der Zugangspunkt Zugang zu bereitgestellten und nicht bereitgestellten Diensten über jeweilige Kanäle bereitstellt, die mit jeweiligen Service Set Identifiers (SSID) (170, 178) gekennzeichnet sind, wobei das Verfahren Folgendes aufweist:

Empfangen eines Passcodes von der Mobilstation mit zwei Betriebsarten durch den USW-Zugangspunkt;
Empfangen eines Basic Service Set Identifier für einen bereitgestellten Dienst (gvBSSID), der für die Mobilstation mit zwei Betriebsarten eindeutig konfigurierbar ist; und
Übertragen des Passcodes und des vom USW-Zugangspunkt empfangenen gvBSSID an einen Anbieter bereitgestellter Dienste, wobei der Anbieter bereitgestellter Dienste einen PWS-Authentifizierungszustand der Mobilstation mit zwei Betriebsarten, auf den Passcode und den gvBSSID reagierend, bestimmt und wobei der Anbieter bereitgestellter Dienste bei Authentifizierung ein PWS-Token einer Mobilstation mit zwei Betriebsarten für den Zugang zu einem bereitgestellten drahtlosen Dienst über einen Kanal für bereitgestellte Dienste bereitstellt.

13. Verfahren nach Anspruch 12, wobei das Empfangen eines Passcodes ferner das Empfangen des Passcodes innerhalb einer vordefinierten Authentifizierungsperiode von der Mobilstation mit zwei Betriebsarten aufweist.

14. Verfahren nach Anspruch 13, wobei das Verfahren nach der Übertragung an den Anbieter bereitgestellter Dienste Folgendes aufweist:

Empfangen des PWS-Tokens von dem Anbieter bereitgestellter Dienste durch den USW-Zugangspunkt und
Versorgen der Mobilstation mit zwei Betriebsarten durch den USW-Zugangspunkt mit dem PWS-Token.

Revendications

1. Point d'accès sans fil fixe (USW) (120), comprenant :

une interface de données de service (162) destinée à traiter un contenu de services non approvisionnés au moyen d'un canal de services de données identifié par un premier identifiant d'ensemble de services (SSID) (170) ;
une interface de services approvisionnés (164) destinée à traiter un contenu de services non

Samsung Ex. 1004, Page 557 of 563

approvisionnés au moyen d'un canal de services de données identifié par un premier identifiant d'ensemble de services (SSID) (178) ; et
un authentificateur local (150) conçu pour réaliser une authentification de services sans fil approvisionnés (PWS) en vue d'un accès à des services approvisionnés au moyen du canal de services approvisionnés ;
l'authentificateur local étant conçu pour être activé par un abonné ;
l'authentificateur local étant conçu pour recevoir un authentifiant d'identification en provenance d'une station mobile bimode (125) ;
l'authentificateur local étant conçu pour analyser l'authentifiant d'identification de manière à déterminer un état d'authentification PWS qui en résulte ; et
l'authentificateur local étant conçu pour autoriser l'accès ou refuser l'accès par la station mobile bimode au point d'accès USW en vue de l'accès à un service sans fil approvisionné au moyen du canal de services approvisionnés en réponse à l'état d'authentification.

2. Point d'accès USW selon la revendication 1, le point d'accès étant conçu pour accepter un trafic en provenance d'une station mobile authentifiée par PWS et rejeter un trafic en provenance de stations mobiles non authentifiées par PWS.

3. Point d'accès USW selon la revendication 1 :

dans lequel l'interface de services approvisionnés est conçue pour correspondre à un ensemble de services de base de services approvisionnés identifiable par un identifiant d'ensemble de services de base de services approvisionnés (hvBSSID),
dans lequel le hvBSSID correspond au second SSID et peut être configuré de façon unique pour l'interface de services approvisionnés, et
dans lequel le signal communiqué avec la station mobile bimode est un signal de service approvisionné communiqué sur le canal de services approvisionnés au point d'accès USW correspondant au hvBSSID, de préférence,
l'interface de services approvisionnés étant conçue pour accepter l'authentifiant d'identification dans une période d'authentification prédéfinie, et conçue pour déterminer un état d'authentification correspondant à un authentifiant d'identification, s'il est accepté pendant la période d'authentification prédéfinie.

4. Point d'accès USW selon la revendication 1, dans lequel l'authentificateur local comprend en outre une interface d'équipements de locaux d'abonnés (CPE) gérée couplée à un fournisseur de services approvisionnés et couplée à l'interface de services approvisionnés, l'interface CPE gérée pouvant être configurée à distance par le fournisseur de services approvisionnés, l'interface CPE gérée modifiant un traitement différentiel du signal de services approvisionnés en réponse à l'état d'authentification.

5. Point d'accès USW selon la revendication 4, dans lequel l'authentifiant d'identification consiste en un identifiant d'ensemble de services de base de services approvisionnés (gvBSSID) pouvant être configuré de façon unique pour la station mobile bimode, et dans lequel l'interface CPE gérée est conçue pour modifier un traitement différentiel du signal de services approvisionnés en réponse au gvBSSID.

6. Point d'accès USW selon la revendication 1, conçu de sorte qu'une seule frappe sur une touche couplée à l'interface de services approvisionnés commence la période d'authentification prédéfinie et active l'interface de services approvisionnés afin de déterminer l'état d'authentification correspondant à l'authentifiant d'identification, s'il est accepté pendant la période d'authentification prédéfinie.

7. Procédé d'authentification, sur un point d'accès USW (120), d'une station mobile bimode (125) cherchant à approvisionner un service sans fil approvisionné (PWS), le point d'accès fournissant un accès à des services approvisionnés et non approvisionnés par l'intermédiaire de canaux respectifs identifiés par des identifiants d'ensembles de services (SSID) (170, 178) respectifs, le procédé consistant à :

recevoir un authentifiant d'identification en provenance de la station bimode par le point d'accès USW ;
évaluer l'authentifiant d'identification en provenance de la station mobile bimode par le point d'accès USW par rapport à un authentifiant d'authentification stocké dans le point d'accès USW ;
déterminer un état d'authentification PWS de la station mobile bimode correspondant à l'authentifiant d'identification ; et
fournir un accès à un service sans fil approvisionné par l'intermédiaire d'un canal de services approvisionnés après une authentification PWS réussie.

8. Procédé selon la revendication 7, consistant en outre à :

si l'état d'authentification PWS est authentifié, recevoir ensuite une demande de jeton de service approvisionné en provenance de la station mobile bimode ;

Samsung Ex. 1004, Page 558 of 563

évaluer un état d'éligibilité de la station mobile bimode en vue de son approvisionnement par un jeton de service approvisionné ; et
si l'état d'éligibilité est éligible, approvisionner ensuite la station mobile bimode avec le jeton de service approvisionné par le point d'accès USW.

9. Procédé selon la revendication 7, dans lequel l'évaluation de l'authentifiant d'identification consiste en outre à :

évaluer l'authentifiant d'identification en provenance de la station mobile bimode par le point d'accès USW par rapport à une configuration de gestion d'approvisionnement reçue d'une interface d'équipements de locaux d'abonnés (CPE) gérée disposée dans le point d'accès USW.

10. Procédé selon la revendication 7, dans lequel la réception de l'authentifiant d'identification en provenance de la station mobile bimode consiste à recevoir l'authentifiant d'identification en provenance de la station mobile bimode dans une période d'authentification prédéfinie.

11. Procédé selon la revendication 7, dans lequel l'authentifiant d'identification comprend un code de passe et/ou un identifiant d'ensemble de services de base de services approvisionnés (gvBSSID) pouvant être configuré de façon unique pour la station mobile bimode.

12. Procédé d'authentification, sur un point d'accès USW (120), d'une station mobile bimode (125) cherchant à approvisionner un service sans fil approvisionné (PWS), le point d'accès fournissant un accès à des services approvisionnés et non approvisionnés par l'intermédiaire de canaux respectifs identifiés par des identifiants d'ensembles de services (SSID) (170, 178) respectifs, le procédé consistant à :

recevoir un code de passe en provenance de la station mobile bimode par le point d'accès USW ;
recevoir un identifiant d'ensemble de services de base de services approvisionnés (gvBSSID) pouvant être configuré de façon unique pour la station mobile bimode ; et
transmettre le code de passe et le gvBSSID reçu par le point d'accès USW à un fournisseur de services approvisionnés, le fournisseur de services approvisionnés déterminant un état d'authentification PWS de la station mobile bimode en réponse au code de passe et au gvBSSID, et à l'authentification, le fournisseur de services approvisionnés approvisionnant la station mobile bimode avec un jeton PWS afin d'accéder à un service sans fil approvisionné par l'intermédiaire d'un canal de services approvisionnés.

13. Procédé selon la revendication 12, dans lequel la réception d'un code de passe consiste en outre à recevoir le code de passe dans une période d'authentification prédéfinie en provenance de la station mobile bimode.

14. Procédé selon la revendication 13, le procédé consistant en outre, après la transmission au fournisseur de services approvisionnés, à :

recevoir le jeton PWS du fournisseur de services approvisionnés par le point d'accès USW ; et
fournir le jeton PWS à la station mobile bimode par le point d'accès USW.

Samsung Ex. 1004, Page 559 of 563

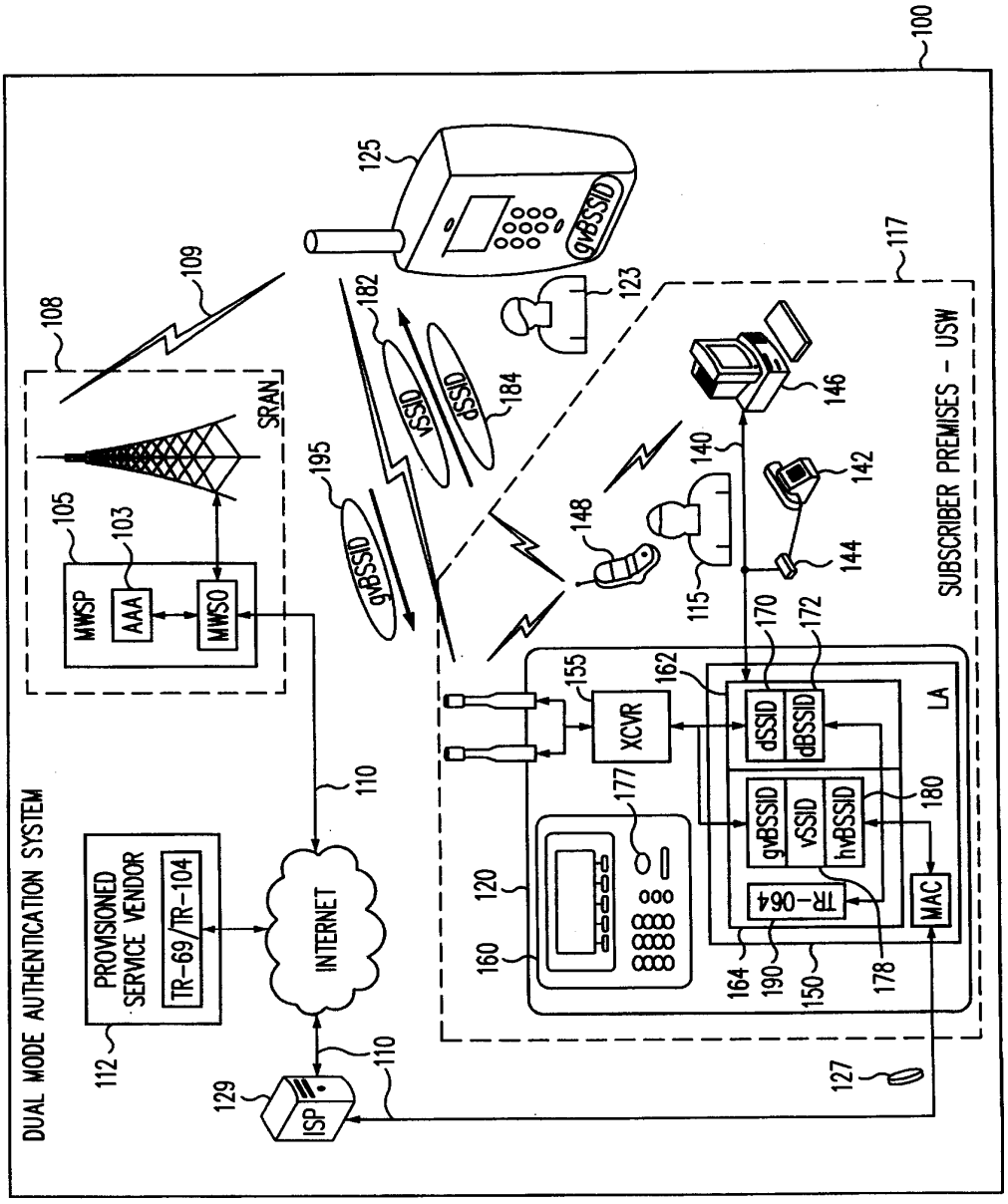

100
DUAL MODE AUTHENTICATION SYSTEM
PROVISIONED SERVICE VENDOR
TR-69/TR-104
112
INTERNET
110
129
ISP
108
109
SRAN
MWSP
AAA
MWSO
105
103
125
gWBSSID
182
vSSID
pSSID
184
195
gWBSSID
123
117
SUBSCRIBER PREMISES - USW
146
140
142
148
144
115
170
172
155
XCVR
162
dSSID
dBSSID
LA
177
120
160
gWBSSID
vSSID
hWBSSID
180
MAC
164
190
150
178
127

FIG. 1

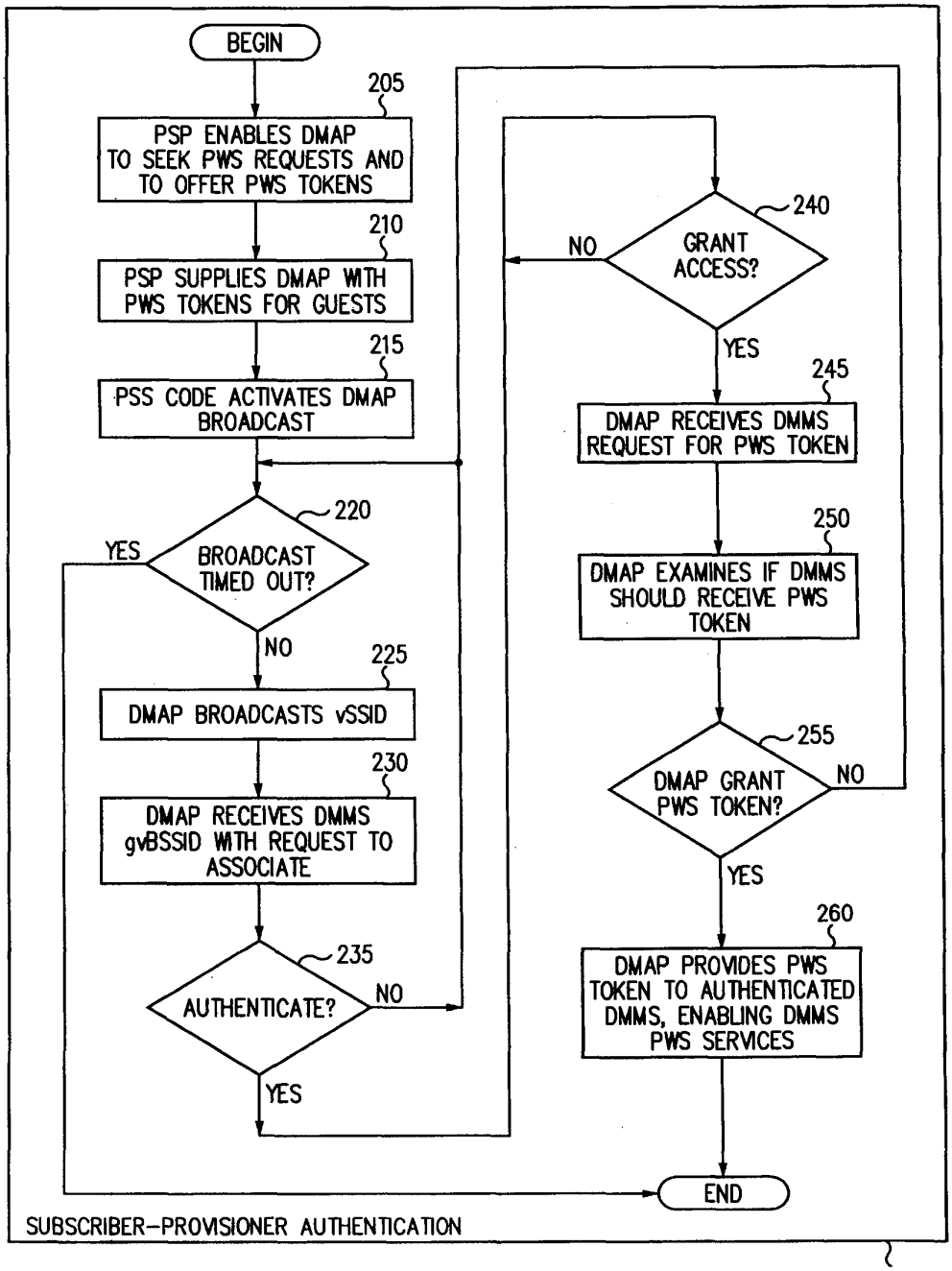

BEGIN
205
PSP ENABLES DMAP TO SEEK PWS REQUESTS AND TO OFFER PWS TOKENS
210
PSP SUPPLIES DMAP WITH PWS TOKENS FOR GUESTS
215
PSS CODE ACTIVATES DMAP BROADCAST
220
BROADCAST TIMED OUT?
YES
NO
225
DMAP BROADCASTS vSSID
230
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
235
AUTHENTICATE?
NO
YES
240
GRANT ACCESS?
NO
YES
245
DMAP RECEIVES DMMS REQUEST FOR PWS TOKEN
250
DMAP EXAMINES IF DMMS SHOULD RECEIVE PWS TOKEN
255
DMAP GRANT PWS TOKEN?
NO
YES
260
DMAP PROVIDES PWS TOKEN TO AUTHENTICATED DMMS, ENABLING DMMS PWS SERVICES
END
SUBSCRIBER-PROVISIONER AUTHENTICATION
200

FIG. 2

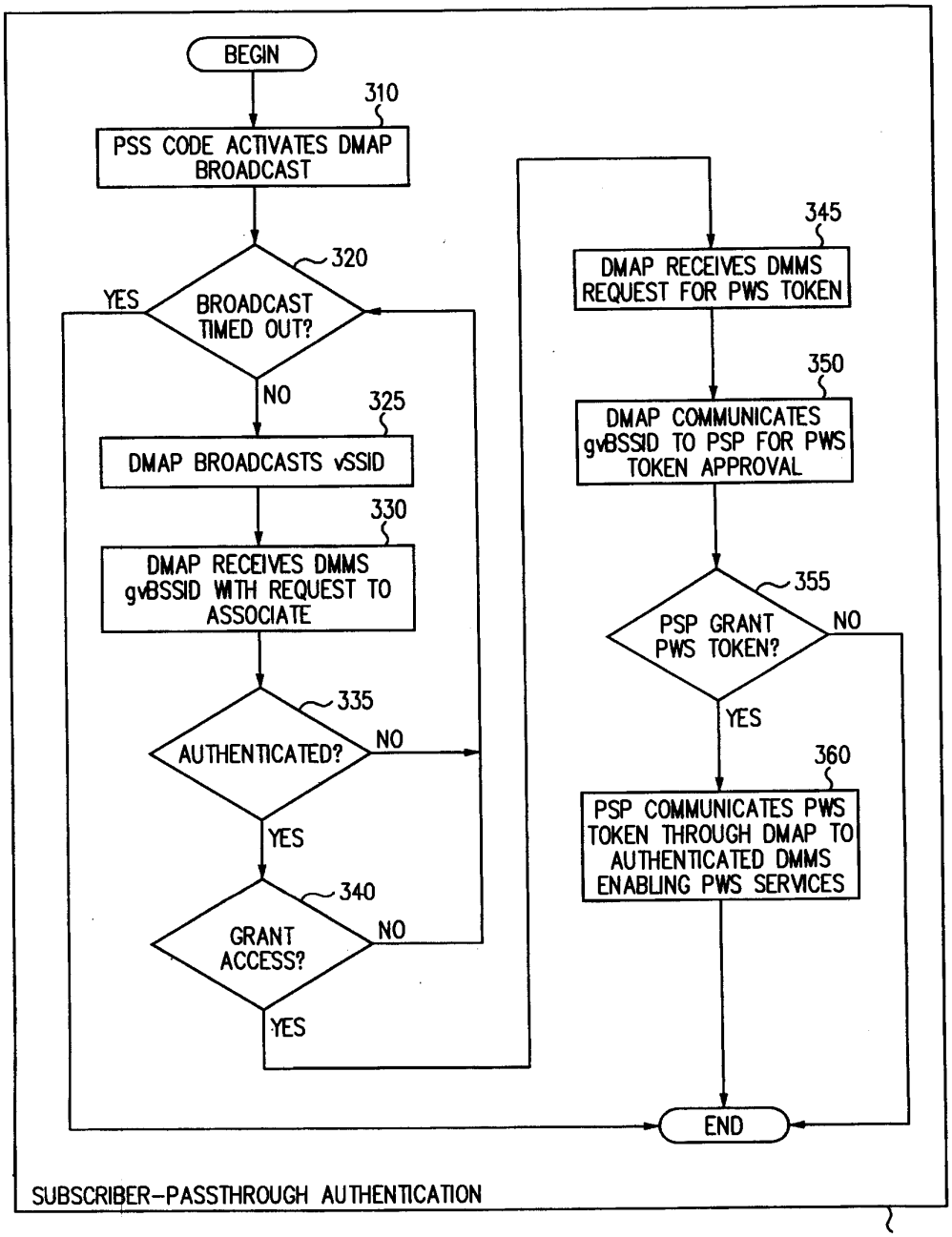

BEGIN
310
PSS CODE ACTIVATES DMAP BROADCAST
320
YES
BROADCAST TIMED OUT?
NO
325
DMAP BROADCASTS vSSID
330
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
335
AUTHENTICATED?
NO
YES
340
GRANT ACCESS?
NO
YES
345
DMAP RECEIVES DMMS REQUEST FOR PWS TOKEN
350
DMAP COMMUNICATES gvBSSID TO PSP FOR PWS TOKEN APPROVAL
355
PSP GRANT PWS TOKEN?
NO
YES
360
PSP COMMUNICATES PWS TOKEN THROUGH DMAP TO AUTHENTICATED DMMS ENABLING PWS SERVICES
END
SUBSCRIBER-PASSTHROUGH AUTHENTICATION
300

FIG. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1424810 A **[0005]**
- US 2001048744 A **[0005]**

Non-patent literature cited in the description

- **ALLIED TELESIS.** AT-WA7500 Dual Radio Wireless Access Point. *Datasheet,* 2006 **[0005]**
- *A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite,* October 2003, http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodli t/wswpf_wp.pdf **[0016]**
- Securing Home Wi-Fi® Networks: A Simple Solution Can Save Your Identity. *Wireless-WP200-x,* 18 May 2005, http://www.54g.org/pdf/Wireless-WP200-RDS.pdf **[0016]**
- *802.1x and EAP-Based Authentication Across Congested WAN Links,* March 2002, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit /authp_an.pdf **[0016]**