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.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

30565 7590 02/13/2024

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
02/13/2024	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

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.
18/448,281	13-Feb-2024	11849337

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

ELECTRONIC CERTIFICATE OF CORRECTION NOTIFICATION

Your electronic certificate of correction is now available, and can be accessed via Patent Center at https://patentcenter.uspto.gov.

The electronic certificate of correction is the official certificate of correction under 35 U.S.C. 254 or 255. For more information, please visit https://www.uspto.gov/electronicgrants.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 11,849,337 B1
APPLICATION NO. : 18/448281
DATED : December 19, 2023
INVENTOR(S) : Sai C. Manapragada

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Specification

In Column 4, Line 16, replace "requiring a peak bandwidth of 740 Mpbs. At 204, the process" with --requiring a peak bandwith of 750 Mbps. At 204, the process--

In Column 4, Line 55, replace "applications, such as "Application A"and "Application B"," with --applications, such as "Application A" and "Application B",--

In Column 9, Line 25, replace "radios A1-A7, with radio AI acting as an originating access" with --radios A1-A7, with radio A1 acting as an originating access--

In Column 10, Line 12, replace "user 9587 within the coverage of the first node may need" with --user 958 within the coverage of the first node may need--

Signed and Sealed this
Thirteenth Day of February, 2024

Katherine Kelly Vidal

Katherine Kelly Vidal
Director of the United States Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No.:	11,849,337
Issue Date:	December 19, 2023
Application No.:	18/448,281
Confirmation No.:	1540
First-Named Inventor:	Sai C. Manapragada
Attorney Docket No.:	020505-000006
Title:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT (37 CFR § 1.322 & 1.323)

A Certificate of Correction of the above-identified patent is respectfully requested to correct certain errors of a clerical or typographical nature or of minor character which appear in the patent as issued. The exact locations where the errors occur and the necessary corrections are indicated on the attached form PTO/SB/44, which form as prepared is suitable for printing.

It is believed that the errors were a combination of errors made by the applicant and errors made on the part of the Patent and Trademark Office. The required fee of $160 under 37 CFR 1.20(a) is included with this submission. However, if any additional fees are required in order to complete the Certificate of Correction, please charge them to Deposit Account No. 23-3030. A detailed explanation of each requested correction follows and documentation is attached.

In column 4, line 16, it is requested that "740 Mbps" be replaced with "750 Mbps." This is a minor typographical error. The correction does not constitute new matter as the other descriptions of the peak bandwidth for APP D refer to the corrected value, 750 Mbps. *See* column 3, lines 16-17; column 8, lines 1-2; FIG. 1; FIG. 8.

In column 4, line 55, it is requested that "Application A"and" be replaced with "Application A" and". This is a minor typographical error, as a space is currently missing between the punctuation mark (") and the word "and". As filed, the specification contained a space in the location indicated (*see* p. 7, ¶ [0028] of the as-filed specification, copy attached) and accordingly does not constitute new matter.

In column 9, line 25, it is requested that "radio Al acting" be replaced with "radio A1 acting". This is a minor typographical error, as the letter "l" appears after the letter "A" therein instead of the number "1" which should follow the letter "A" therein. As filed, the specification included the numeral after "A," *i.e.,* "A1" (*see* p. 13, ¶ [0050] of the as-filed specification, copy attached) and accordingly does not constitute new matter.

In column 10, line 12, it is requested that "user 9587" be replaced with "user 958." This is a minor typographical error. The correction does not constitute new matter as "local users, at 958 and 960" is disclosed in the preceding lines at column 10, line 10 and "958" is the reference numeral used in FIG. 11.

Please send the Certificate to Woodard, Emhardt, Henry, Reeves & Wagner, LLP, 111 Monument Circle, Suite 3700, Indianapolis, Indiana 46204.

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) 737-7561
Email: bhartz@uspatent.com

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 S/N 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", which claims the benefit of U.S. Patent Application S/N 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 S/N 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 S/N 61/897,219, filed October 30, 2013, and U.S. Provisional Patent Application S/N 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

Samsung Ex. 1004, Page 10 of 553

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 740 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 9587 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.

PTO/SB/44 (09-07)
Approved for use through 03/31/2023. OMB 0651-0033
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.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 11,849,337

APPLICATION NO.: 18/448,281

ISSUE DATE : December 19, 2023

INVENTOR(S) : Sai C. Manapragada

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Specification

In Column 4, Line 16, replace “requiring a peak bandwidth of 740 Mpbs. At 204, the process” with --requiring a peak bandwith of 750 Mbps. At 204, the process--

In Column 4, Line 55, replace “applications, such as "Application A"and "Application B",” with --applications, such as "Application A" and "Application B",--

In Column 9, Line 25, replace “radios A1-A7, with radio AI acting as an originating access” with --radios A1-A7, with radio A1 acting as an originating access--

In Column 10, Line 12, replace “user 9587 within the coverage of the first node may need” with --user 958 within the coverage of the first node may need--

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700
Indianapolis, IN 46204-5137

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. 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 1.0 hour 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: Attention Certificate of Corrections Branch, 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 #
18/448,281	01/12/2024 02:06:43 PM Z ET	020505-000006

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 #	11849337
CONFIRMATION #	1540	FILED BY	WALTER MOORE
PATENT CENTER #	63937157	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	08/11/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	E20241BE07577411	WALTER MOORE

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2811	CERTIFICATE OF CORRECTION	160.00	1	160.00
			TOTAL AMOUNT:	$160.00

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 #
18/448,281	**01/12/2024 02:06:43 PM Z ET**	**020505-000006**

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 #	11849337
CONFIRMATION #	1540	FILED BY	WALTER MOORE
PATENT CENTER #	63937157	FILING DATE	08/11/2023
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
20505-6 Request for Certificate of Correction.pdf	20	Request for Certificate of Correction	1813 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
20505-6 Request for Certificate of Correction.pdf	CAC12B0D50077453910C1722FD9126FF4512018F6CB871ED4168ECC69C426D391D5B61CCB1A6B1F06922190A41F2906A44C66DCCD8DFACA4F8E32028B8735E4E

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

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.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

30565 7590 12/19/2023

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
12/19/2023	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

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.
18/448,281	19-Dec-2023	11849337

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006

CONFIRMATION NO. 1540

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

PUBLICATION NOTICE

OC000000065526347

Date Mailed: 12/07/2023

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

Publication No.US-2023-0397014-A1
Publication Date:12/07/2023

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 accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

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 the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, 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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/448,281	12/19/2023	11849337	020505-000006	1540

30565 7590 11/29/2023

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.

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 #
18/448,281	**10/31/2023 10:33:02 AM ET**	**020505-000006**

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 #	1540	FILED BY	WALTER MOORE
PATENT CENTER #	63119710	FILING DATE	08/11/2023
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
20505-6 Issue Fee Transmittal.pdf	1	Issue Fee Payment (PTO-85B)	368 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
20505-6 Issue Fee Transmittal.pdf	73430091F0AEC3EDA4DD372366404B8A989D14FE918A083C2360E735CF04F2E2C5E6BE3EDC3850E65DF20719F17BBE0F46EC796521B5229085EDA59BEB047F3C

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 PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/448,281	10/31/2023 10:33:02 AM ET	020505-000006

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 #	1540	FILED BY	WALTER MOORE
PATENT CENTER #	63119710	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	08/11/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	E20230UA34096239	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.

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)
October 31, 2023	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
18/448,281	August 11, 2023	MANAPRAGADA, Sai C.	020505-000006	1540

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	January 30, 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	October 31, 2023
Typed or printed name	Blake R. Hartz	Registration No.	73453

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 10/30/2023

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: 10/30/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

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	01/30/2024

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 EFS-Web.

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 10/30/2023

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.

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

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	01/30/2024

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 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. _____

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.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

30565 7590 10/30/2023

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: 10/30/2023

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. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to 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)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 18/448,281	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 10/10/23.
   ☐ 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 1-9,15-16,18-23 and 25-37 . 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. **Claims 1-9, 15-16, 18-23, and 25-37** are allowed.

2. The following is a statement of reasons for the indication of allowable subject matter:

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 a wireless networking device, comprising the steps of: connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, when the wireless networking device is being used, provides first data stream and having that 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 (i) is are suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is adapted to emit radio waves 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, 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, when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication, (ii) select one transceiver of the first and second transceivers which has the most bandwidth available, (iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and (iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; wherein, if the unselected wireless

transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, then-the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and then-select the unselected transceiver, (ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and (iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers" 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.

Conclusion

3. 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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/448,281	Manapragada, Sai C.
	Examiner	Art Unit
	SAAD KHAWAR	2412

CPC - Searched*		
Symbol	Date	Examiner
H04W16	09/26/2023	/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 parent application	09/26/2023	/SK/
PE2E Search	09/26/2023	/SK/
Inventor Name Search	09/26/2023	/SK/
IP.com Search	09/26/2023	/SK/
Updated PE2E Search	10/19/2023	/SK/
Updated IP.com Search	10/19/2023	/SK/

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
H04W16		10/19/2023	/SK/

/SAAD KHAWAR/ Primary Examiner, Art Unit 2412	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/448,281	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	19 October 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20231019

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/448,281	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 (Assistant Examiner) (Date)	**Total Claims Allowed:** 30	
/SAAD KHAWAR/ Primary Examiner, Art Unit 2412 (Primary Examiner) 19 October 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/448,281	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
1	1		10	18	19	26	28	14	37						
2	2		11	19	20	27	29								
3	3		12	20	21	28	30								
4	4		13	21	22	29	31								
5	5		14	22	23	30	32								
6	6	15	15		24	10	33								
7	7	16	16	23	25	11	34								
8	8		17	24	26	12	35								
9	9	17	18	25	27	13	36								

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 30	
/SAAD KHAWAR/ Primary Examiner, Art Unit 2412 (Primary Examiner)	19 October 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No.: 20231019

18448281
Search History

Report Run Date: 2023-10-19 UTC
Searches: 1
Markers: 1

Search #	Timestamp	Results	Page
1	2023-10-19 13:38 UTC	~11,302,917	4

18448281

Content: Patents + NPL (192)

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 | 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 2023-10-19 13:38 UTC | ~11,302,917 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 a wireless networking device, comprising the steps of: connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, 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 one of the first and second wireless transceivers (i) is suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to a first and second actual bandwidth, and (iii) is adapted to emit radio waves 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, 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, when the wireless networking device is being used, to, 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, and (b) (i) identify at least one portion of each one of the first and second bandwidth availabilities of the first and second wireless transceivers, and (ii) evaluate the identified bandwidth availabilities of the first and second wireless transceivers with respect to the first bandwidth requirement of the first application; wherein, if the first bandwidth requirement is at least partially satisfied by the bandwidth availabilities of the first and second wireless transceivers, preparing the first data stream for simultaneous transmission to the recipient from both of the first and second wireless transceivers using a specific subset of frequencies corresponding to the identified at least one portions of their available bandwidth and causing the prepared first data stream to be transmitted from the first and second wireless transceivers to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein the wireless networking device's utilization of the available bandwidth of the first and second wireless transceivers does not prevent other wireless networking devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first and second wireless transceivers for data transmission purposes at the same time that processed data is being sent from the first and second wireless transceivers

Concept Modifiers: None

Filters: None

Bibliographic Data

Application No: 18/448,281

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.
08/11/2023	370	2412	020505-000006
RULE			

APPLICANTS

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

INVENTORS

Sai C. Manapragada,

CONTINUING DATA

This application is a CON of 17468509 09/07/2021

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**

08/29/2023

** 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

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) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM

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 bandwidth carrier) AND virtual ADJ2 link NOT	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:11 AM

		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 coverage WITH overlap$4 WITH linear$2 AND L53	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 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) WITH (first second) NEAR3 (link connection)	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 12:45 PM

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, 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	2023/02/01 10:55 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)				
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; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:54 AM
L87	54506	L82 AND bandwidth WITH availab$5 grant	(US-PGPUB; USPAT; USOCR; FIT (AU, AP,	OR	ON	ON	2023/02/02 10:57 AM

		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)				
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, 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	2023/02/02 10:57 AM

			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; IBM_TDB)	OR	ON	ON	2023/02/02 10:58 AM
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,	OR	ON	ON	2023/02/02 11:00 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)				
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, 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,	OR	ON	ON	2023/02/02 11:02 AM

			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,	OR	ON	ON	2023/02/02 11:09 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)				
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, 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 11:13 AM

			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" 11429407B2 "20050089064" "20070110198" "20070121573" "20070180119" "20070242605"	(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	2023/08/22 09:52 AM

		"20070270121" "20080002631" "20090034460" "20090074051" "20000141691" "20100128630" "20110110289" "20130028150" "20130258021" "20130281049").PN.	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)				
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; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 10:31 AM
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,	OR	ON	ON	2023/08/22 10:31 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)				
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, 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,	OR	ON	ON	2023/09/11 09:34 AM

			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 "20120113320" OR "20140075523" OR "20140269560" OR "20150181486" OR "20150237667" OR "5073899" OR "5818830" OR "7664072" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/26 10:14 AM

		"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 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,	OR	ON	ON	2023/09/26 11:08 AM

			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, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:17 AM
L125	110	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	2023/09/26 11:18 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)				
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 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	2023/10/19 10:07 AM

			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

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

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
* 18/448,281 *	18/448,281	Manapragada, Sai C.	
	Examiner	**Art Unit**	
	KHAWAR, SAAD	2412	

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

TERMINAL DISCLAIMER	☑ APPROVED	☐ DISAPPROVED
Date Filed: **10 October 2023**	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

/FELICIA D ROBERTS/

Technology Center: OPLC

Telephone: (571)272-0550

17/468,509

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 #
18/448,281	**10/10/2023 02:29:29 PM ET**	**020505-000006**

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 #	1540	FILED BY	W. Pat Moore
PATENT CENTER #	62963337	FILING DATE	08/11/2023
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 4

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
20505-6 Response to NonFinal Office Action.pdf		12	-	44 KB
20505-6 Response to NonFinal Office Action-A....pdf	(1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	16 KB
20505-6 Response to NonFinal Office Action-CLM.pdf	(2-10)	9	Claims	38 KB
20505-6 Response to NonFinal Office Action-REM.pdf	(11-12)	2	Applicant Arguments/Remarks Made in an Amendment	18 KB

Terminal Disclaimer 20505-6.pdf	1	Terminal Disclaimer Filed	288 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
20505-6 Response to NonFinal Office Action.pdf	5258CEE9D14F0D27EBA1E537DE24FD0F322328B751E2C1375B061F99BCCB3A0B2CE771B740BB76B88072998090F5725709FC52D85BC65085CDF293546779D492
20505-6 Response to NonFinal Office Action-A....pdf	1ABD53C45B059AD38B6D67069318F6DCB9C002480764D2BCF34B5543143CE29A784B950FB39113AFCC93C64D7FC46A57A4B8FD486AEA465F1DC14A1FD1F49958
20505-6 Response to NonFinal Office Action-CLM.pdf	8854C864E88E07A1FE2384C8A65ABC56D730EDE315F1BDB21DD96ED7F24B404BA17569CC40BD19AB835CF8955CE9AA93746C1FA848B842AF7A654357F1BB11E5
20505-6 Response to NonFinal Office Action-REM.pdf	1E182B202A50DFAC567B86CE3B529C434FE11D76E77FA8FF674EB73768F3C644451A9E331CE8ED06B0568E5A693DFE62C8D1361FDD21E36D46B7AA8841FC03C6
Terminal Disclaimer 20505-6.pdf	CC06CB3F106111FEAB7AF3EA90CCBDC8B2A721F941A64421330F8650DCA612B47079A8835E7006F0EE8FC1B8E0B70CCB29D058ADDFB41803ED709224EDD0C8A4

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 PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/448,281	10/10/2023 02:29:29 PM ET	020505-000006

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 #	1540	FILED BY	W. Pat Moore
PATENT CENTER #	62963337	AUTHORIZED BY	Blake Hartz
CUSTOMER #	30565	FILING DATE	08/11/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Sai C. Manapragada

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1649	E202300E30487306	W. Pat Moore

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

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	18/448,281
Confirmation No.:	1540
First-Named Inventor:	Manapragada, Sai C.
Filing Date:	August 11, 2023
Group Art Unit:	2412
Examiner:	Khawar, Saad
Attorney Docket No.:	020505-000006
Title:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

RESPONSE TO NON-FINAL OFFICE ACTION

In response to the Non-Final Office Action mailed on October 3, 2023, please enter the following amendments and remarks in the above-mentioned patent application. The Commissioner is authorized to charge any extensions of time as well as any additional fees or credit any overcharges to Deposit Account No. 23-3030, but not to include any payment of issue fees.

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of improving the performance of a wireless networking device, comprising the steps of:

connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, 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 (i) is suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is adapted to emit radio waves 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, 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, when the wireless networking device is being used in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication,

(ii) select one transceiver of the first and second transceivers which has the most bandwidth available,

(iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and

(iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially satisfy the first wireless bandwidth requirement of the first application;

wherein, if the unselected wireless transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and select the unselected transceiver,

(ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and

(iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and

wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers.

2. (Previously Presented) The method of claim 1,

wherein the application interface is associated with a second application, the second application providing, when the wireless networking device is being used, a second data stream and having a second wireless bandwidth requirement;

wherein the processing interface is configured to, when the wireless networking device is being used in a manner transparent to any layer of the wireless networking device above the processing interface, (i) prepare the first and second data streams for simultaneous transmission to the recipient from the selected wireless transceivers using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and (ii) cause the prepared first and second data streams to be simultaneously transmitted from the selected wireless transceivers to thereby at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

3. (Previously Presented) The method of claim 2,

wherein, if the identified at least one portion of the bandwidth of the first wireless transceiver becomes unavailable during use of the wireless networking device or if it has an unidentified portion of bandwidth availability that is greater than its identified at least one portion of bandwidth availability during use of the wireless networking device, the processing interface is configured to, as a result of the unavailability or the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one new portion of the bandwidth of the first wireless transceiver that is available for communication and then select that wireless transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces associated with any wireless transceiver, for transmission to the recipient from the first wireless transceiver using a specific subset of frequencies corresponding to its newly identified at least one portion of available bandwidth, and

(iii) cause the prepared first and second data streams to be transmitted to the recipient from the first transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

4. (Previously Presented) The method of claim 3,

wherein, if the identified at least one portion of the bandwidth of the second wireless transceiver becomes unavailable during use of the wireless networking device or if it has an unidentified portion of bandwidth availability that is greater than its identified at least one portion of bandwidth availability during use of the wireless networking device, the processing interface is configured to, as a result of the unavailability or the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one new portion of the bandwidth of the second wireless transceiver that is available for communication and then select that wireless transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces associated with any wireless transceiver, for transmission to the recipient from the second wireless transceiver using a specific subset of frequencies corresponding to its newly identified at least one portion of available bandwidth, and

(iii) cause the prepared first and second data streams to be transmitted to the recipient from the second transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

5. (Previously Presented) The method of claim 4,

wherein the processing interface is configured to, when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface, evaluate the identified bandwidth availabilities of the first and second wireless transceivers with respect to the first and second bandwidth requirements of the first and second applications; and

wherein, if, during operation of the wireless networking device, the first and second bandwidth requirements of the first and second applications are at least partially satisfied by the bandwidth availability of the selected transceiver, preparing the first and second data streams for simultaneous transmission to the recipient from both of the first and second wireless transceivers using a specific subset of frequencies corresponding to the identified at least one

portion of their available bandwidth and causing the prepared first data stream to be transmitted from the first and second wireless transceivers to thereby at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

6. (Previously Presented) The method of claim 4, further comprising the steps of:

connecting a third actual MAC interface to the processing interface;

connecting a third actual PHY interface to the third actual MAC interface;

associating a third wireless transceiver with the third actual PHY interface, wherein the third wireless transceiver (i) is suitable for use in a wireless local area network, (ii) has a third bandwidth availability up to a third actual bandwidth, and (iii) is adapted to emit radio waves in a third band of frequencies;

forming in the processing interface a third virtual PHY interface that is configured to, during operation of the wireless networking device, feed information regarding the bandwidth availability of the third wireless transceiver back to the at least one virtual MAC interface;

wherein the processing interface is configured to, when the wireless networking device is being used in a manner transparent to any layer of the wireless networking device above the processing interface, request or create a third association between the recipient and the third actual MAC and PHY interfaces;

wherein the selected transceiver comprises one of the first, second and third wireless transceivers and the unselected transceivers comprise the remaining two transceivers of the first, second and third transceivers;

wherein, if one of the unselected wireless transceivers has more bandwidth availability than the selected transceiver during use of the wireless networking device, the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of the bandwidth of at least of the one of the unselected wireless transceivers that has more bandwidth availability than the selected transceiver and select that new transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless

transceiver, for transmission to the recipient from the new transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and

(iv) cause the prepared first and second data streams to be transmitted to the recipient from the new transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second bandwidth requirements of the first and second applications; and

wherein the wireless networking device's utilization of the available bandwidth of the first, second and third wireless transceivers does not prevent other wireless networking devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first, second and third wireless transceivers for data transmission purposes at the same time that processed data is being sent from one or more of the first, second and third wireless transceivers.

7. (Original) The method of claim 6, wherein the at least one portion of the third bandwidth of the first transceiver comprises a single portion.

8. (Previously Presented) The method of claim 6, wherein the at least one portion of the third bandwidth of the third transceiver is contiguous.

9. (Original) The method of claim 6, wherein the third virtual PHY interface is not contiguous with the virtual MAC interface.

10.-14. (Canceled)

15. (Original) The method of claim 1, wherein the wireless networking device comprises a wireless access point.

16. (Original) The method of claim 1, wherein the wireless networking device comprises a handheld computing device.

17. (Canceled)

18. (Original) The method of claim 1, wherein each one of the first and second frequency bands are specified in at least one member of the family of IEEE 802.11 standards.

19. (Original) The method of claim 18, wherein the at least one member of the family of IEEE 802.11 standards was in existence as of October 30, 2013.

20. (Original) The method of claim 1, wherein the virtual MAC interface includes a decision block.

21. (Original) The method of claim 1, wherein the virtual MAC interface includes a processing block.

22. (Original) The method of claim 1, wherein the virtual MAC interface includes an ultra-streaming block.

23. (Previously Presented) The method of claim 1, wherein each of the virtual PHY interfaces includes an RF block.

24. (Canceled)

25. (Previously Presented) The method of claim 1, wherein the at least one portion of the first bandwidth of the first transceiver comprises a single portion.

26. (Previously Presented) The method of claim 1, wherein the at least one portion of the first bandwidth of the first transceiver is contiguous.

27. (Previously Presented) The method of claim 1, wherein the at least one portion of the second bandwidth of the second transceiver comprises a single portion.

28. (Previously Presented) The method of claim 1, wherein the at least one portion of the second bandwidth of the second transceiver is contiguous.

29. (Original) The method of claim 1, wherein the first virtual PHY layer is not contiguous with the virtual MAC interface.

30. (Original) The method of claim 1, wherein the second virtual PHY layer is not contiguous with the virtual MAC interface.

31. (Previously Presented) The method of claim 1, wherein the processing interface comprises multiple virtual MAC interfaces.

32. (Previously Presented) The method of claim 1, wherein the processing interface includes a bandwidth allocator.

33. (New) The method of claim 6 further comprising the step of coupling first and second buffer memories respectively to the first and second actual PHY layers, the first and second buffer memories being configured to, during use of the wireless networking device, store data prior to its actual transmission to the recipient via the first and second actual PHY layers, the capacity of the first and second buffer memories being programmable.

34. (New) The method of claim 33, wherein each of the first and second buffer memories comprises a programmable register.

35. (New) The method of claim 33, further comprising the steps of:

connecting a fourth actual MAC interface to the processing interface;

connecting a fourth actual PHY interface to the fourth actual MAC interface;

associating a fourth wireless transceiver with the actual PHY interface, wherein the fourth wireless transceiver (i) is suitable for use in a wireless local area network, (ii) has a fourth bandwidth availability up to a fourth actual bandwidth, and (iii) is adapted to emit radio waves in a fourth band of frequencies; and

forming in the processing interface a fourth virtual PHY interface that is configured to, during operation of the wireless networking device, feed information regarding the bandwidth availability of the fourth wireless transceiver back to the at least one virtual MAC interface.

36. (New) The method of claim 35,

wherein the processing interface is configured to, when the wireless networking device is being used in a manner transparent to any layer of the wireless networking device above the processing interface, request or create a fourth association between the recipient and the fourth actual MAC and PHY interfaces; and

wherein the selected transceiver comprises one of the first, second, third and fourth wireless transceivers and the unselected transceivers comprise the remaining three transceivers of the first, second, third and fourth transceivers.

37. (New) The method of claim 35, wherein the fourth virtual PHY interface is not contiguous with the virtual MAC interface.

REMARKS

Reconsideration and further examination are respectfully requested in view of the present amendments and remarks, and the terminal disclaimer submitted herewith.

Status of the Claims

Below is the status of the claims in this application.

1. Claim(s) pending: 1-9, 15-16, 18-23 and 25-37.
2. Claim(s) canceled: 10-14, 17, 24.
3. Claim(s) added: 33-37.
4. Claims withdrawn from consideration but not canceled: None.

Applicant notes that under the amendments presented herein there are still 30 total claims pending in accordance with the requirements of the Track One program.

Claim Amendments and Support

The amended and new claims are supported by the application as originally filed as well as the provisional applications filed on October 30, 2013. See, for example, at least Figures 1, 4, 5A, 5B, and 6 and ¶¶ [0021]–[0024], [0028]–[0033] of the instant application as filed. No new matter has been added. The new claims are dependent on allowable claims and accordingly do not require any additional search or examination.

Double Patenting

The Office Action provisionally rejects the claims for non-statutory double patenting in view of co-pending application serial number 17468509. Applicant thanks the Examiner for the indications that the pending claims are allowable, subject to submission of a terminal disclaimer relative to the '509 application. Such a terminal disclaimer is submitted herewith, and Applicant respectfully requests withdrawal of the rejection.

Conclusion

If after the Examiner feels that any issues remain which must be resolved before the application can be passed to allowance, the Examiner is invited to contact the undersigned representative to resolve such issues.

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/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) 020505-000006

In re Application of: Sai C. Manapragada

Application No.: 18/448,281

Filed: August 11, 2023

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 17/468,509, filed, September 7, 2021, 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/	October 10, 2023
Signature	Date
Blake R. Hartz, Reg. No. 73453	
Typed or printed name	
Attorney of Record	317-634-3456
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/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 18/448,281	Filing Date 08/11/2023	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $ 192 =	
☐ 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).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	10/10/2023	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 30	Minus	** 30	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0		x $ 192 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/AMANDA N FORD/
*** 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 number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. 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 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

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.
18/448,281	08/11/2023	Sai C. Manapragada	020505-000006	1540

30565 7590 10/03/2023

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
10/03/2023	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

Office Action Summary	**Application No.** 18/448,281	**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 --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 9/18/23.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-10,12-16 and 18-32 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-10,12-16 and 18-32 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, 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.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8/11/23 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Arguments

3. Applicant's arguments filed 9/18/23 have been fully considered.

4. Applicant's arguments, on page 11, with regards to double patenting rejection have been fully considered but are not persuasive. While the terminal disclaimer filed with this application overcomes the potential double patenting rejection in regards to application 18447597, a terminal disclaimer is also required to overcome the double patenting rejection in regards to application 17468509. A terminal disclaimer having been filed for application 17468509 in regards to the instant application is not sufficient to overcome this double patenting rejection.

5. Applicant's arguments, starting on page 11, with regards to the patentability of the claims have been fully considered and are agreed with in part. The examiner agrees that the claims contain allowable subject matter for the reasons provided by applicant. However, due to the pending double patenting rejection the claims are not in condition for allowance.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s)

because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The filing of a terminal disclaimer by itself is not a complete reply to a nonstatutory double patenting (NSDP) rejection. A complete reply requires that the terminal disclaimer be accompanied by a reply requesting reconsideration of the prior Office action. Even where the NSDP rejection is provisional the reply must be complete. See MPEP § 804, subsection I.B.1. For a reply to a non-final Office action, see 37 CFR 1.111(a). For a reply to final Office action, see 37 CFR 1.113(c). A request for reconsideration while not provided for in 37 CFR 1.113(c) may be filed after final for consideration. See MPEP §§ 706.07(e) and 714.13.

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The actual filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/apply/applying-online/eterminal-disclaimer.

7. **Claims 1-10, 12-16, and 18-32** are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claim 22 and 29 of copending Application No. **17468509** (reference application).

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

8. Regarding claim 1, the claims of **17468509** disclose:

"A method of improving the performance of a wireless networking device, comprising the steps of: connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, when the wireless networking device is being used, provides first data stream and having that a first wireless bandwidth requirement;" **([claim 22]: "A wireless networking device, comprising: an application interface connected to a processing interface, the application interface being associated with a first application, the first application providing, that-when the wireless networking device is being used, provides first data stream and having a first wireless bandwidth requirement;")**

"connecting first and second actual MAC interfaces to the processing interface;" **([claim 22]: "first, second, and third actual MAC interfaces connected to the processing interface;")**

"connecting first and second actual PHY interfaces respectively to the first and second actual MAC interfaces;" **([claim 22]: "first, second, and third actual PHY interfaces connected to the first, second, and third 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 (i) is are suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is adapted to emit radio waves in first and second different bands of frequencies;" **([claim 22]: "first, second, and third wireless transceivers respectively associated with the first, second, and third actual PHY interfaces, wherein each one of the first, second, and third wireless transceivers (i) is are-suitable for use in a wireless local area network, (ii) has a first, second, and third bandwidth availability up to a first, second, and third actual bandwidth, and (ii) is adapted to emit radio waves in first, second, and third 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, 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;" **([claim 22]: "wherein the processing interface comprises (i) at least one virtual MAC interface and (ii) first, second, and third virtual PHY interfaces that, during operation of the wireless networking device, feed information regarding the bandwidth availabilities of the first, second, and third wireless transceivers back to the at least one virtual MAC interface;")**

"wherein the processing interface is configured to, when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface," **([claim 22]: "wherein the processing interface is configured to, when the wireless network device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface,")**

"(i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication," **([claim 22]: "(i) identify at least one portion of each one of the first, second, and third bandwidths of the first, second, and third wireless transceivers that are available for communication, and")**

"(ii) select one transceiver of the first and second transceivers which has the most bandwidth available," **([claim 22]: "(ii) evaluate the identified bandwidth availabilities of the first, second, and third wireless transceivers with respect to the first bandwidth requirement of the first application;")**

"(iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and" **([claim 22]: "preparing the first data stream for simultaneous transmission to a recipient from both the selected transceivers of the first, second, and third wireless transceivers using a specific subset of frequencies corresponding to the identified portions of their available bandwidth")**

"(iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially satisfy the first wireless bandwidth requirement of the first application;" **([claim**

22]: "causing the prepared first data to be transmitted from the selected two transceivers of the first, second, and third wireless transceivers to thereby at least partially satisfy the first wireless bandwidth requirement of the first application")

"wherein, if the unselected wireless transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, then the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and then-select the unselected transceiver," **([claim 22]: "wherein, if the first bandwidth requirement is at least partially satisfied by the bandwidth availabilities of a selected two transceivers of the first, second, and third wireless transceivers" ; [claim 29]: "if the identified bandwidth of the first wireless transceiver becomes unavailable during use of the wireless networking device, then the processing interface is adapted to, as a result of the unavailability and in a manner transparent to any layer of the wireless networking device above the processing interface, identify another at least one portion of the bandwidth of any of the first, second or third wireless transceivers and then prepare the first data stream for transmission to the recipient additionally using a specific subset of frequencies corresponding to the newly identified at least one portion of bandwidth of any of the first, second or third wireless transceivers to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application.")**

"(ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and" **([claim 22]: "preparing the first data stream for simultaneous transmission to a recipient from both the selected transceivers of the first, second, and third wireless transceivers using a specific subset of frequencies corresponding to the identified portions of their available bandwidth")**

"(iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces

of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and" **([claim 22]: "causing the prepared first data to be transmitted from the selected two transceivers of the first, second, and third wireless transceivers to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; and")**

"wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers." **([claim 22]: "wherein the wireless networking device's utilization of the available bandwidth of the first, second, and third wireless transceivers does not prevent other wireless networking devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first, second, and third wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected one of the first, second, and third wireless transceivers.")**

Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1 of the instant application merely broaden the scope of claims 22 and 29 of **17468509** by omitting limitations, such as "first, second, and third frequency bands both being higher in frequency than the first frequency band", or by broadening limitations, such as from being based on no bandwidth availability to being based on less bandwidth availability. It has been held that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA), also note Exparte Rainu, 168 USPQ 375 (Bd. App. 1969); the omission of a reference element whose function is not needed would be obvious to one skilled in the art.

9. The remaining claims depend on claim 1 and are rejected for similar reasons.

Allowable Subject Matter

10. **Claims 1-10, 12-16, and 18-32** would be allowable if rewritten or amended to overcome the double patenting rejections set forth in this Office action.

11. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 22, 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 a wireless networking device, comprising the steps of: connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, when the wireless networking device is being used, provides first data stream and having that 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 (i) is are suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is adapted to emit radio waves 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, 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, when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication, (ii) select one transceiver of the first and second transceivers which has the most bandwidth available, (iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and (iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially

satisfy the first wireless bandwidth requirement of the first application; wherein, if the unselected wireless transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, then-the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and then-select the unselected transceiver, (ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and (iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers." 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.

Conclusion

12. 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

Notice of References Cited	Application/Control No. 18/448,281	Applicant(s)/Patent Under Reexamination Manapragada, Sai C.	
	Examiner SAAD KHAWAR	Art Unit 2412	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080084855-A1	04-2008	Rahman; Shahriar I.	H04W24/04	370/342
*	B	US-20110128919-A1	06-2011	KIM; Soeng-Hun	H04W48/18	370/360
*	C	US-20150098359-A1	04-2015	YEN; Kuang-Yu	H04W48/16	370/254
*	D	US-20060140123-A1	06-2006	Conner; W. Steven	H04L45/02	370/238
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/448,281	Manapragada, Sai C.
	Examiner	Art Unit
	SAAD KHAWAR	2412

CPC - Searched*		
Symbol	Date	Examiner
H04W16	09/26/2023	/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 parent application	09/26/2023	/SK/
PE2E Search	09/26/2023	/SK/
Inventor Name Search	09/26/2023	/SK/
IP.com Search	09/26/2023	/SK/

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/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) SAME indicat$3	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/11 10:32 AM

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 bandwidth carrier) AND virtual ADJ2 link NOT	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 10:11 AM

		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 coverage WITH overlap$4 WITH linear$2 AND L53	(US-PGPUB; USPAT)	OR	ON	ON	2019/07/12 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) WITH (first second) NEAR3 (link connection)	(US-PGPUB; USPAT)	OR	ON	ON	2021/01/18 12:45 PM

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, 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	2023/02/01 10:55 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)				
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; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/02/02 10:54 AM
L87	54506	L82 AND bandwidth WITH availab$5 grant	(US-PGPUB; USPAT; USOCR; FIT (AU, AP,	OR	ON	ON	2023/02/02 10:57 AM

		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)				
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, 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	2023/02/02 10:57 AM

			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; IBM_TDB)	OR	ON	ON	2023/02/02 10:58 AM
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,	OR	ON	ON	2023/02/02 11:00 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)				
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, 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,	OR	ON	ON	2023/02/02 11:02 AM

			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,	OR	ON	ON	2023/02/02 11:09 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)				
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, 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 11:13 AM

			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" 11429407B2 "20050089064" "20070110198" "20070121573" "20070180119" "20070242605"	(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	2023/08/22 09:52 AM

		"20070270121" "20080002631" "20090034460" "20090074051" "20000141691" "20100128630" "20110110289" "20130028150" "20130258021" "20130281049").PN.	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)				
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; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/22 10:31 AM
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,	OR	ON	ON	2023/08/22 10:31 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)				
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, 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,	OR	ON	ON	2023/09/11 09:34 AM

			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 "20120113320" OR "20140075523" OR "20140269560" OR "20150181486" OR "20150237667" OR "5073899" OR "5818830" OR "7664072" OR	(US-PGPUB; USPAT)	OR	ON	ON	2023/09/26 10:14 AM

		"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 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,	OR	ON	ON	2023/09/26 11:08 AM

			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, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/09/26 11:17 AM
L125	110	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	2023/09/26 11:18 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)				
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

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	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/22 10:32 AM

		AND feed$4).CLM.					
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

18448281
Search History

Report Run Date: 2023-09-26 UTC
Searches: 1
Markers: 1

Search #	Timestamp	Results	Page
1	2023-09-26 15:09 UTC	~9,005,963	4

Content: Patents + NPL (192)

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 | 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 2023-09-26 15:09 UTC | ~9,005,963 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 a wireless networking device, comprising the steps of: connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing, when the wireless networking device is being used, provides first data stream and having that 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 (i) is are suitable for use in a wireless local area network, (ii) has a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is adapted to emit radio waves 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, 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, when the wireless networking device is being used, in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication, (ii) select one transceiver of the first and second transceivers which has the most bandwidth available, (iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and (iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially satisfy the first wireless bandwidth requirement of the first application; wherein, if the unselected wireless transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, then-the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface, (i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and then-select the unselected transceiver, (ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and (iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers.

Concept Modifiers: None

Filters: None

Samsung Ex. 1004, Page 132 of 553

Bibliographic Data

Application No: 18/448,281

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.
08/11/2023	370	2412	020505-000006
RULE			

APPLICANTS

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

INVENTORS

Sai C. Manapragada,

CONTINUING DATA

This application is a CON of 17468509 09/07/2021

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**

08/29/2023

** 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

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 5

Complete if Known	
Application Number	New Application
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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-11115834 B2	09-07-2021	Manapragada	
	3	US-11429407 B2	08-30-2022	Smith et al.	
	4	US-20050089064 A1	04-28-2005	Zimmerman et al.	
	5	US-20060140123 A1	06-29-2006	Conner et al.	
	6	US-20070110198 A1	05-17-2007	Skarby et al.	
	7	US-20070121573 A1	05-31-2007	Zuckerman et al.	
	8	US-20070180119 A1	08-02-2007	Khivesara et al.	
	9	US-20070242695 A1	10-18-2007	Xu	
	10	US-20070270121 A1	11-22-2007	Shao et al.	
	11	US-20080002631 A1	01-03-2008	Ramachandran	
	12	US-20080084855 A1	04-10-2008	Rahman	
	13	US-20090034460 A1	02-05-2009	Moratt et al.	
	14	US-20090074051 A1	03-19-2009	Manapragada et al.	
	15	US-20090141691 A1	06-04-2009	Jain	
	16	US-20100128630 A1	05-27-2010	Barak et al.	
	17	US-20110110289 A1	05-12-2011	Venkatachalam et al.	
	18	US-20110128919 A1	06-02-2011	KIM et al.	
	19	US-20110211541 A1	09-01-2011	Yuk et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country Code [3] 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	TW I500350B	04-16-2015	Yen et al.		✓

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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 assistance 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 5

Complete if Known	
Application Number	New Application
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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
	21	US-20130028150 A1	01-31-2013	Ma et al.	
	22	US-20130196653 A1	08-01-2013	Morrison	
	23	US-20130258921 A1	10-03-2013	Gevorkov et al.	
	24	US-20130281049 A1	10-24-2013	Lee et al.	
	25	US-20140003449 A1	01-02-2014	Li	
	26	US-20140056209 A1	02-27-2014	Park et al.	
	27	US-20140075189 A1	03-13-2014	Abraham et al.	
	28	US-20140213219 A1	07-31-2014	MOHEBBI	
	29	US-20140269610 A1	09-18-2014	HIBEN et al.	
	30	US-20150023245 A1	01-22-2015	Du et al.	
	31	US-20150098359 A1	04-09-2015	YEN et al.	
	32	US-20150110036 A1	04-23-2015	Zhang et al.	
	33	US-20160014127 A1	01-14-2016	Mohebbi	
	34	US-7373443 B2	05-13-2008	Seto	
	35	US-9160396 B2	10-13-2015	Soltanian et al.	
	36	US-9198184 B2	11-24-2015	Yeh et al.	
	37	US-9467379 B2	10-11-2016	Merlin et al.	
	38	US-9526022 B2	12-20-2016	Gupta	
	39	US-9560656 B2	01-31-2017	Damnjanovic 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/ (09/26/2023)	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 assistance 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 5

Complete if Known	
Application Number	New Application
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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
	40	US-9603192 B2	03-21-2017	Mohebbi	
	41	US-9736714 B2	08-15-2017	Zhao et al.	
	42	US-9743345 B2	08-22-2017	Yen et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country Code [3] 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/ (09/26/2023)	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 assistance 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	4	of	5

Complete if Known	
Application Number	New Application
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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]
	43	Choi et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part I". IEEE 11-14/0804r1. [PowerPoint presentation].	
	44	Choi et al. (November 11, 2013) "Discussion on OFDMA in HEW". LG Electronics. [PowerPoint presentation].	
	45	English Abstract of TWI500350B obtained from Espacenet.net on July 7, 2023.	
	46	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.	
	47	Hiertz et al. (November 12, 2013) "Proposed direction and priorities for HEW". IEEE 11-13-1331-01. [PowerPoint presentation].	
	48	Huang et al. (September 16, 2013) "DL-MU-MIMO Transmission with Unequal Bandwidth". IEEE 802.11-13/1154r1. [PowerPoint presentation].	
	49	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).	
	50	Inoue et al. (March 19, 2013) "Beyond 802.11ac – A Very High Capacity WLAN". IEEE 11-13/0287r3. [PowerPoint presentation].	
	51	Kakumanu, S. and Sivakumar, R. "Glia: A Practical Solution for Effective High Datarate Wifi-Arrays". MobiCom '09, September 20-25, 2009.	
	52	Kim et al. (September 16, 2013) "Multicast Transmission for HEW". IEEE 802.11-13/1061r0. [PowerPoint presentation].	

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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	5	of	5

Complete if Known	
Application Number	New Application
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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]
	53	Koskela et al. (July 15, 2013) "Discussion on Potential Techniques for HEW". IEEE 802.11-13/0871r0. [PowerPoint presentation].	
	54	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.	
	55	Lim et al. (July 14, 2014) "Envisioning 11ax PHY Structure - Part II". IEEE 11-14/0801r0. [PowerPoint presentation].	
	56	Liu et al. (May 9, 2013) "Discussions on 11ac PHY Efficiency". IEEE 802.11-13/0544r3. [PowerPoint presentation].	
	57	Prasad, S.S; Shukla, C.K.; and Chisab, R.F. "Performance Analysis of OFDMA in LTE" in: IEEE (July 26-28, 2012).	
	58	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.	
	59	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.	
	60	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	
	61	Yang et al. (September 18, 2013) "Discussion on Access Mechanism for HEW". IEEE 11-13/1105r0. [PowerPoint presentation].	

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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/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 3

Complete if Known	
Application Number	18/448,281
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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-20020152305 A1	10-17-2002	Jackson et al.	
	2	US-20040053602 A1	03-18-2004	Wurzburg	
	3	US-20060114851 A1	06-01-2006	Gupta et al.	
	4	US-20090290524 A1	11-26-2009	Seok	
	5	US-20120113320 A1	05-10-2012	PLATZER	
	6	US-20140075523 A1	03-13-2014	TUOMAALA et al.	
	7	US-20140269560 A1	09-18-2014	Jain et al.	
	8	US-20150181486 A1	06-25-2015	Vallabhu et al.	
	9	US-20150237667 A1	08-20-2015	GHAI et al.	
	10	US-5073899	12-17-1991	Collier et al.	
	11	US-5818830	10-06-1998	Daane et al.	
	12	US-7664072 B1	02-16-2010	Ho et al.	
	13	US-7784076 B2	08-24-2010	Demircin et al.	
	14	US-7797723 B2	09-14-2010	Demircin et al.	
	15	US-8411608 B2	04-02-2013	Chandra et al.	
	16	US-8718558 B2	05-06-2014	Montemurro	
	17	US-8818276 B2	08-26-2014	Kiukkonen et al.	
	18	US-8837454 B2	09-16-2014	Hegde	
	19	US-8923816 B2	12-30-2014	Lee et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initial *	Cite No. [1]	Foreign Patent Document Country Code [3] 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	WO 2014020407 A1	02-06-2014	Huang et al.		
	22	EP 2016750 B1	01-21-2009	Lee et al.		
	23	EP 2055072 B1	05-06-2009	Falk et al.		
	24	EP 2713670 A1	04-02-2014	Smadi		
	25	EP 3174323 B1	11-14-2018	Montemurro		

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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 assistance 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 3

Complete if Known	
Application Number	18/448,281
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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-8982762 B2	03-17-2015	Smadi et al.	
	27	US-8989101 B1	03-24-2015	Mishra	
	28	US-9258712 B2	02-09-2016	Kiukkonen et al.	
	29	US-9560661 B2	01-31-2017	Elhaddad et al.	
	30	US-9706383 B2	07-11-2017	Kiukkonen 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
	31	EP 3220697 B1	06-06-2018	Kiukkonen		✓

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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 assistance 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	3	of	3

Complete if Known	
Application Number	18/448,281
Filing Date	August 11, 2023
First Named Inventor	Sai C. Manapragada
Art Unit	Not Yet Known
Examiner Name	Not Yet Known
Attorney Docket Number	020505-000006

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]
	32	English Translation of EP2055072B1 obtained from Google Patents on September 1, 2023.	

Examiner Signature	/SAAD KHAWAR/ (09/26/2023)	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./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	18/448,281
Confirmation No.:	1540
First-Named Inventor:	Manapragada, Sai C.
Filing Date:	August 11, 2023
Group Art Unit:	Not Yet Known
Examiner:	Not Yet Known
Attorney Docket No.:	020505-000006
Title:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS

PRELIMINARY AMENDMENT

Please enter the following amendments and remarks in the above-mentioned patent application.

The Commissioner is authorized to charge any extensions of time as well as any additional fees or credit any overcharges to Deposit Account No. 23-3030, but not to include any payment of issue fees.

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of improving the performance of a wireless networking device, comprising the steps of:

connecting an application interface to a processing interface, the application interface being associated with a first application, the first application providing ~~that~~, when the wireless networking device is being used, ~~provides~~ a first data stream and having ~~that has~~ 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 (i) is ~~are~~ suitable for use in a wireless local area network, (ii) has~~ve~~ a first and second bandwidth availability up to first and second actual bandwidths, and (iii) is~~are~~ adapted to emit radio waves 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, 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, when the wireless networking device is being used~~, to,~~ in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of each one of the first and second actual bandwidths of the first and second wireless transceivers that are available for communication,

(ii) select one transceiver of the first and second transceivers which has the most bandwidth available,

(iii) prepare the first data stream for transmission to a recipient from the selected wireless transceiver using a specific subset of frequencies corresponding to the identified at least one portion of its available bandwidth, and

(iv) cause the prepared first data stream to be transmitted from the selected wireless transceiver to thereby at least partially satisfy the first wireless bandwidth requirement of the first application;

wherein, if the unselected wireless transceiver has more bandwidth availability than the selected transceiver during use of the wireless networking device, ~~then~~ the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of the bandwidth of the unselected transceiver that is available for communication and ~~then~~ select the unselected transceiver,

(ii) prepare the first data stream, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the unselected transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and

(iii) cause the prepared first data stream to be transmitted to the recipient from the unselected transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first wireless bandwidth requirement of the first application; and

wherein the wireless networking device's utilization of the available bandwidth of the selected and unselected transceivers does not prevent ~~any~~ other wireless networking device from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availabilities of the selected and unselected wireless transceivers for data transmission purposes at the same time that processed data is being sent from the selected and unselected wireless transceivers.

2. (Currently Amended) The method of claim 1,

wherein the application interface is associated with a second application, the second application providing ~~that~~, when the wireless networking device is being used, ~~provides~~ a second data stream and having~~s~~ a second wireless bandwidth requirement;

wherein the processing interface is configured to, when the wireless networking device is being used~~, to,~~ in a manner transparent to any layer of the wireless networking device above the processing interface, (i) prepare the first and second data streams for simultaneous transmission to the recipient from ~~both of~~ the selected ~~first and second~~ wireless transceiver~~s~~ using a specific subset of frequencies corresponding to the identified at least one portion of its ~~their~~ available bandwidth, and (ii) cause the prepared first and second data streams to be simultaneously transmitted from the selected ~~first and second~~ wireless transceiver~~s~~ to thereby at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

3. (Currently Amended) The method of claim 2,

wherein, if the identified at least one portion of the bandwidth of the first wireless transceiver becomes unavailable during use of the wireless networking device or if it has an unidentified portion of bandwidth availability that is greater than its identified at least one portion of bandwidth availability during use of the wireless networking device, ~~then~~ the processing interface is configured ~~adapted~~ to, as a result of the unavailability or the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one new portion of the bandwidth of the first wireless transceiver that is available for communication and then select that wireless transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces associated with any wireless transceiver, for transmission to the recipient from the first wireless transceiver using a specific subset of frequencies corresponding to its newly ~~un~~identified at least one portion of available bandwidth, and

(iii) cause the prepared first and second data streams to be transmitted to the recipient from the first transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

4. (Currently Amended) The method of claim 3,

wherein, if the identified at least one portion of the bandwidth of the second wireless transceiver becomes unavailable during use of the wireless networking device or if it has an unidentified portion of bandwidth availability that is greater than its identified at least one portion of bandwidth availability during use of the wireless networking device, ~~then~~ the processing interface is configured ~~adapted~~ to, as a result of the unavailability or the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one new portion of the bandwidth of the second wireless transceiver that is available for communication and then select that wireless transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces associated with any wireless transceiver, for transmission to the recipient from the second wireless transceiver using a specific subset of frequencies corresponding to its newly ~~un~~identified at least one portion of available bandwidth, and

(iii) cause the prepared first and second data streams to be transmitted to the recipient from the second transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

5. (Currently Amended) The method of claim 4,

wherein the processing interface is configured to, when the wireless networking device is being used, ~~to,~~ in a manner transparent to any layer of the wireless networking device above the processing interface, evaluate ~~compare the magnitude of the first bandwidth requirement of the first application to~~ the identified bandwidth availabilities of the first and second wireless transceivers with respect to the first and second bandwidth requirements of the first and second applications; and

wherein, if, during operation of the wireless networking device, the first and second bandwidth requirements of the first and second applications are ~~is not~~ at least partially satisfied by the bandwidth availability of the selected transceiver, ~~then~~ preparing the first and

second data streams for simultaneous transmission to the recipient from both of the first and second wireless transceivers using a specific subset of frequencies corresponding to the identified at least one portion of their available bandwidth and ~~then~~ causing the prepared first data stream to be transmitted from the first and second wireless transceivers to thereby at least partially satisfy the first and second wireless bandwidth requirements of the first and second applications.

6. (Currently Amended) The method of claim 4~~5~~, further comprising the steps of:

connecting a third actual MAC interface to the processing interface;

connecting a third actual PHY interface to the third actual MAC interface;

associating a third wireless transceiver with the third actual PHY interface, wherein the third wireless transceiver (i) is suitable for use in a wireless local area network, (ii) has a third bandwidth availability up to a third actual bandwidth, and (iii) is adapted to emit radio waves in a third band of frequencies;

forming in the processing interface a third virtual PHY interface that is configured to, during operation of the wireless networking device, feed~~s~~ information regarding the bandwidth availability of the third wireless transceiver back to the at least one virtual MAC interface;

wherein the processing interface is configured to, when the wireless networking device is being used~~, to,~~ in a manner transparent to any layer of the wireless networking device above the processing interface, request or create a third association between the recipient and the third actual MAC and PHY interfaces;

wherein the selected transceiver comprises one of the first, second and third wireless transceivers and the unselected transceivers comprise the remaining two transceivers of the first, second and third transceivers;

wherein, if one of the unselected wireless transceivers has more bandwidth availability than the selected transceiver during use of the wireless networking device, ~~then~~ the processing interface is adapted to, as a result of the increased bandwidth availability and in a manner transparent to any layer of the wireless networking device above the processing interface,

(i) identify at least one portion of the bandwidth of at least of the one of the unselected wireless transceivers that has more bandwidth availability than the selected transceiver and ~~then~~ select that new transceiver,

(ii) prepare the first and second data streams, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, for transmission to the recipient from the new transceiver using a specific subset of frequencies corresponding to its identified at least one portion of available bandwidth, and

(iv) cause the prepared first and second data streams to be transmitted to the recipient from the new transceiver, without requiring the disassociation of the recipient from the actual MAC and PHY interfaces of any wireless transceiver, to thereby continue to at least partially satisfy the first and second bandwidth requirements of the first and second applications; and

wherein the wireless networking device's utilization of the available bandwidth of the first, second and third wireless transceivers does not prevent ~~any~~ other wireless networking devices from utilizing a range of frequencies corresponding to the remaining portion of the bandwidth availability of the first, second and third wireless transceivers for data transmission purposes at the same time that processed data is being sent from one or more of the first, second and third wireless transceivers.

7. (Original) The method of claim 6, wherein the at least one portion of the third bandwidth of the first transceiver comprises a single portion.

8. (Currently Amended) The method of claim 6, wherein the at least one portion of the third bandwidth of the third transceiver is contiguous.

9. (Original) The method of claim 6, wherein the third virtual PHY interface is not contiguous with the virtual MAC interface.

10. (Currently Amended) The method of claim 6, wherein at least one of the first, second and third wireless transceivers ~~are~~is adapted to communicate with a recipient via a variable and

programmable duplex link that exhibits an asymmetric transmit and receive profile that is programmable.

11. (Canceled)

12. (Currently Amended) The method of claim 6~~11~~, wherein the wireless networking device comprises a first wireless access point that provides access to the internet within a first coverage area, the processing interface of the first wireless access point being configured to, during operation of the first wireless access point, establish a wireless link to a second wireless access point that has a second coverage area and a processing interface, the processing interfaces of the first and second wireless access points being configured to, during their operation, ~~to~~ communicate with each other regarding at least one aspect of operation of the first wireless access point.

13. (Original) The method of claim 12, wherein the processing interface of the first wireless access point cooperates with the processing interface of the second wireless access point to define a distributed processing logic.

14. (Original) The method of claim 13, wherein the aspect of operation of the first wireless access point comprises aggregation of the bandwidth availabilities of the first, second and third wireless transceivers in a virtual link.

15. (Original) The method of claim 1, wherein the wireless networking device comprises a wireless access point.

16. (Original) The method of claim 1, wherein the wireless networking device comprises a handheld computing device.

17. (Canceled)

18. (Original) The method of claim 1, wherein each one of the first and second frequency bands are specified in at least one member of the family of IEEE 802.11 standards.

19. (Original) The method of claim 18, wherein the at least one member of the family of IEEE 802.11 standards was in existence as of October 30, 2013.

20. (Original) The method of claim 1, wherein the virtual MAC interface includes a decision block.

21. (Original) The method of claim 1, wherein the virtual MAC interface includes a processing block.

22. (Original) The method of claim 1, wherein the virtual MAC interface includes an ultra-streaming block.

23. (Currently Amended) The method of claim 1, wherein each ~~one~~ of the virtual PHY interfaces includes an RF block.

24. (Original) The method of claim 1, wherein the wireless networking device comprises a telephone.

25. (Currently Amended) The method of claim 1, wherein the at least one portion of the first bandwidth of the first transceiver comprises a single portion.

26. (Currently Amended) The method of claim 1, wherein the at least one portion of the first bandwidth of the first transceiver is contiguous.

27. (Currently Amended) The method of claim 1, wherein the at least one portion of the second bandwidth of the second transceiver comprises a single portion.

28. (Currently Amended) The method of claim 1, wherein the at least one portion of the second bandwidth of the second transceiver is contiguous.

29. (Original) The method of claim 1, wherein the first virtual PHY layer is not contiguous with the virtual MAC interface.

30. (Original) The method of claim 1, wherein the second virtual PHY layer is not contiguous with the virtual MAC interface.

31. (New) The method of claim 1, wherein the processing interface comprises multiple virtual MAC interfaces.

32. (New) The method of claim 1, wherein the processing interface includes a bandwidth allocator.

REMARKS

Status of All of the Claims

Below is the status of the claims in this application.

1. Claim(s) pending: 1-10, 12-16, and 18-32.
2. Claim(s) canceled: 11 and 17.
3. Claim(s) added: 31-32.
4. Claims withdrawn from consideration but not canceled: None.

Applicant notes that under the amendments presented herein there are still 30 total claims pending in accordance with the requirements of the Track One program.

Claim Support

It is believed that the above-identified amended claims are supported by the application as originally filed including priority to two provisional applications that were filed on October 30, 2013. See, for example, Figure 1 of the application as filed which is included in the 10/30/2013 provisional, Ser. No. 61/897,216. See also, for example, the priority charts that were included in a response filed in application Ser. No. 17/468,509 on 8/8/2023.

Double Patenting

In an effort to expedite the prosecution of this application, a terminal disclaimer was submitted upon filing to obviate any double patenting rejections that might be made with respect to any patents or applications that are related to this application. In particular, a terminal disclaimer was submitted relative to Ser. No. 17/468,509. That '509 Application has, in turn, terminal disclaimers granted relative to all patents and pending applications relating to this application, including the present application and co-pending Ser. No. 18/447,597. The Examiner's confirmation that the claims presented herein are not subject to rejection on a double patenting basis is respectfully requested.

Patentability of the Claims

In the last office action for a related application (Ser. No. 17/468,509), the Examiner indicated that (now-) cancelled claim 5, concerning feeding back to processing circuitry

information regarding the bandwidth availability of multiple transceivers, would be allowable if rewritten in independent form. Please note that this feature is included in all of the new claims as "wherein… 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" in independent claim 1. The claims presented herein also include a limitation regarding "band selection" whereby, for each transmission opportunity, a single transceiver is used that has the most bandwidth availability as compared to that of the other transceiver. The feedback provided to the at least one virtual MAC regarding bandwidth availabilities allows the networking device to switch between bands during operation without requiring disassociation of the networking device from any recipient.

It is respectfully submitted that no prior art reference of record either taken alone or in combination with any other reference(s) of record render the above-described claims anticipated or obvious. For at least these reasons, it is respectfully submitted that the claims are in condition for allowance.

Conclusion

If after reviewing this amendment the Examiner feels that any issues remain which must be resolved before the application can be passed to allowance, the Examiner is invited to contact the undersigned representative to resolve such issues.

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 2 016 750 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 156 of 553

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

Samsung Ex. 1004, Page 157 of 553

(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 160 of 553

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 161 of 553

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 162 of 553

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 163 of 553

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 164 of 553

(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 165 of 553

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 166 of 553

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 167 of 553

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 168 of 553

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 169 of 553

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 170 of 553

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 171 of 553

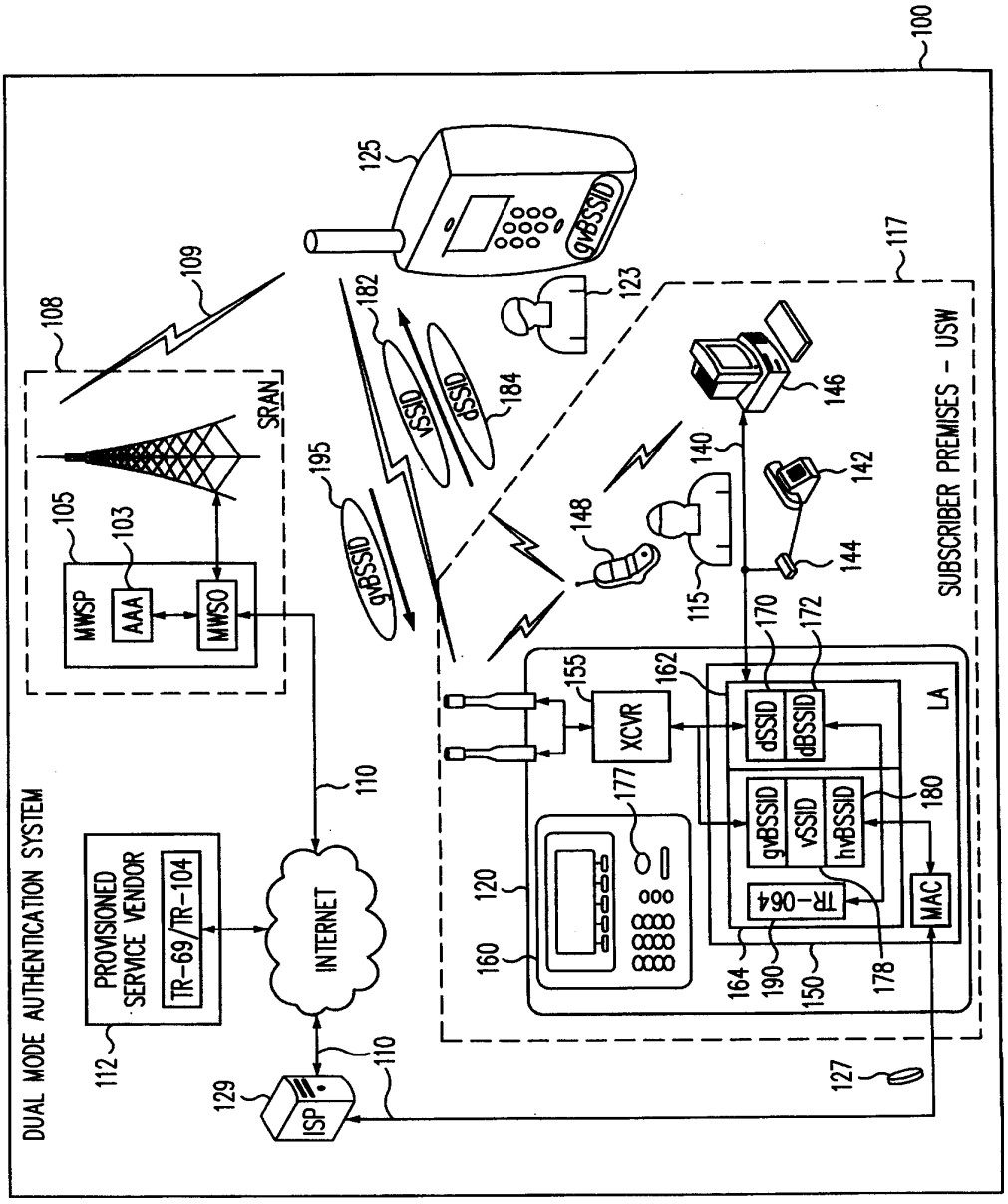

100
DUAL MODE AUTHENTICATION SYSTEM
SUBSCRIBER PREMISES - USW
117
125
gWBSSID
109
108
SRAN
182
vSSID
pSSID
184
123
195
gWBSSID
105
MWSP
103
AAA
MWSO
148
140
146
142
144
115
170
172
155
XCVR
162
dSSID
dBSSID
LA
177
gWBSSID
vSSID
hWBSSID
180
120
160
164
190
150
178
MAC
110
PROVISIONED SERVICE VENDOR
TR-69/TR-104
112
INTERNET
129
ISP
110
127

FIG. 1

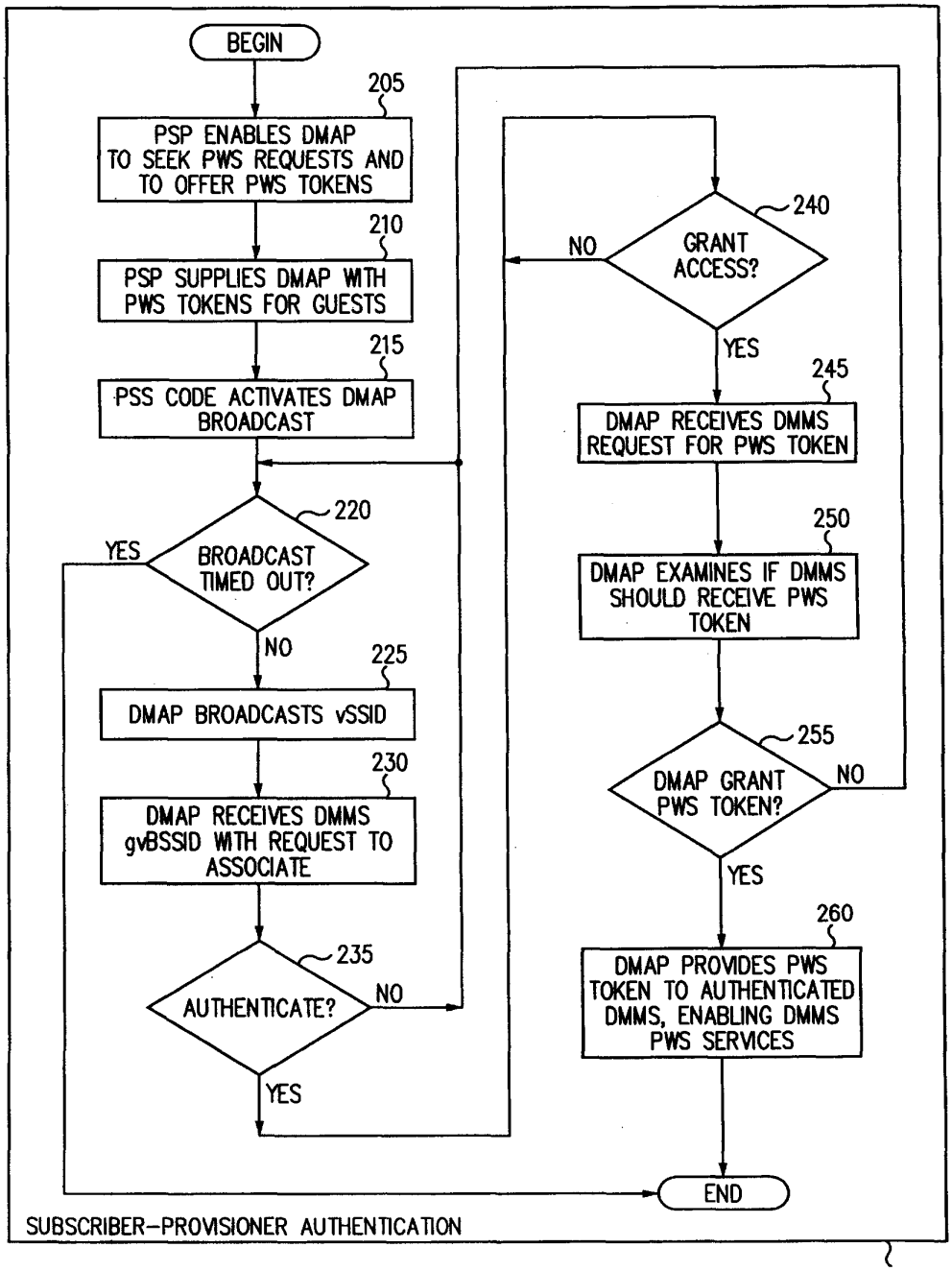

BEGIN
205
PSP ENABLES DMAP TO SEEK PWS REQUESTS AND TO OFFER PWS TOKENS
210
PSP SUPPLIES DMAP WITH PWS TOKENS FOR GUESTS
215
PSS CODE ACTIVATES DMAP BROADCAST
220
BROADCAST TIMED OUT?
YES
NO
225
DMAP BROADCASTS vSSID
230
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
235
AUTHENTICATE?
NO
YES
240
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

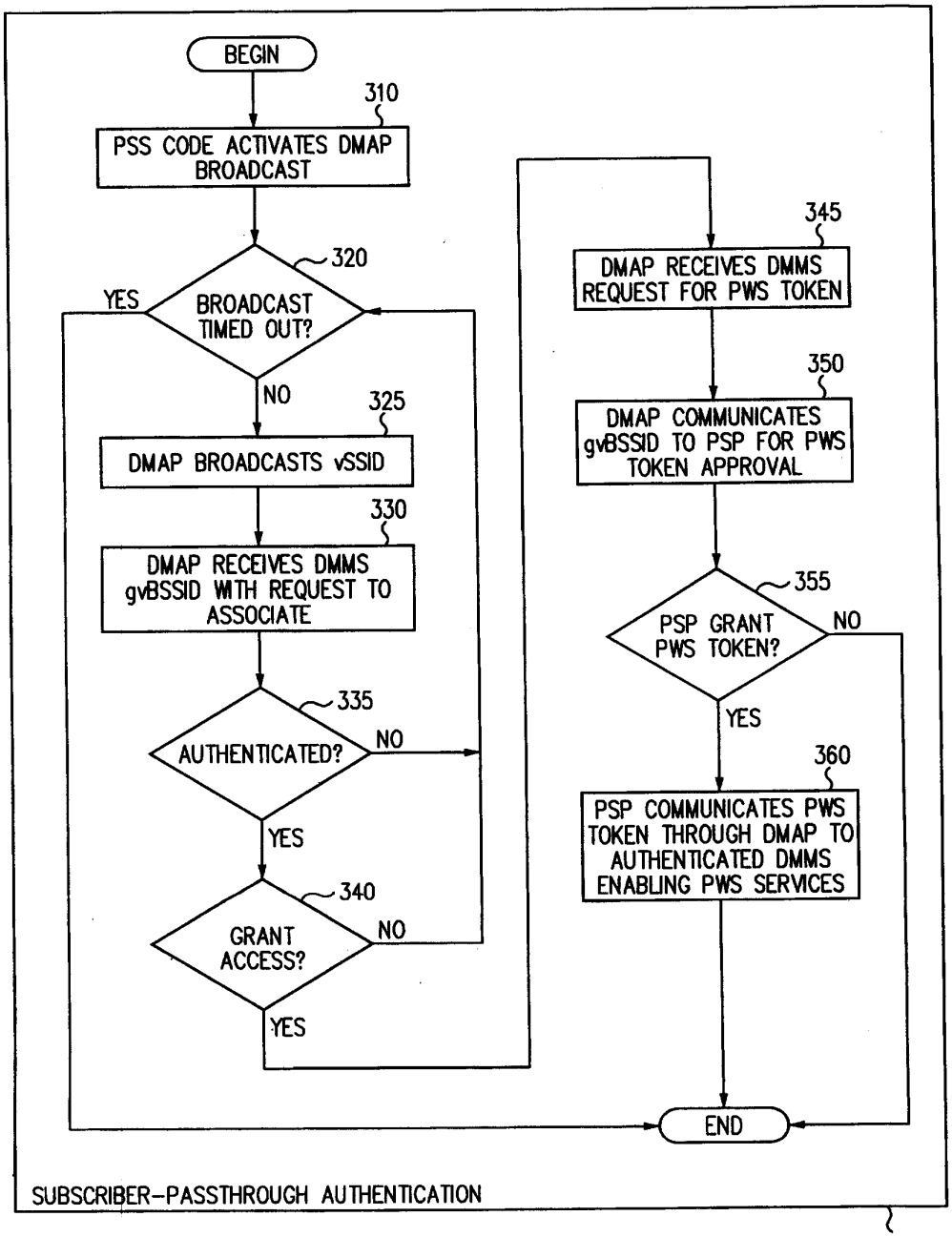

BEGIN
310
PSS CODE ACTIVATES DMAP BROADCAST
320
YES
BROADCAST TIMED OUT?
NO
325
DMAP BROADCASTS vSSID
330
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
335
AUTHENTICATED?
NO
YES
340
GRANT ACCESS?
NO
YES
345
DMAP RECEIVES DMMS REQUEST FOR PWS TOKEN
350
DMAP COMMUNICATES gvBSSID TO PSP FOR PWS TOKEN 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]**

Samsung Ex. 1004, Page 175 of 553

(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

Samsung Ex. 1004, Page 177 of 553

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 179 of 553

[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 180 of 553

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 181 of 553

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 182 of 553

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 183 of 553

[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 184 of 553

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 185 of 553

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 186 of 553

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 187 of 553

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 188 of 553

[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 189 of 553

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 190 of 553

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 191 of 553

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 192 of 553

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 193 of 553

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 :

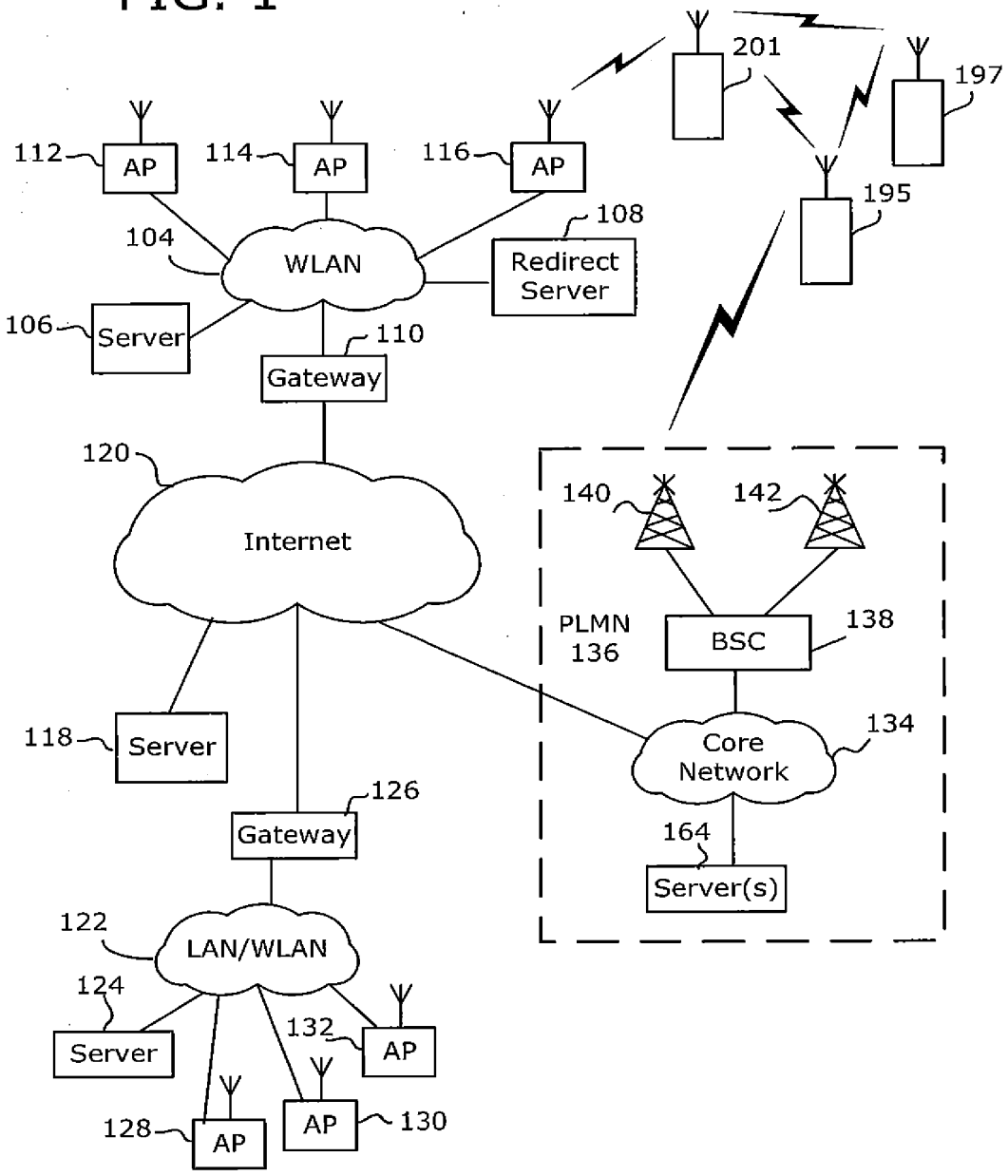
un support non transitoire lisible par ordinateur ;
des instructions informatiques stockées dans le support non transitoire lisible par ordinateur ; et
les instructions informatiques pouvant être exécutées par un ou plusieurs processeur(s) d'un dispositif de communication sans fil (201) qui comporte 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 194 of 553

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

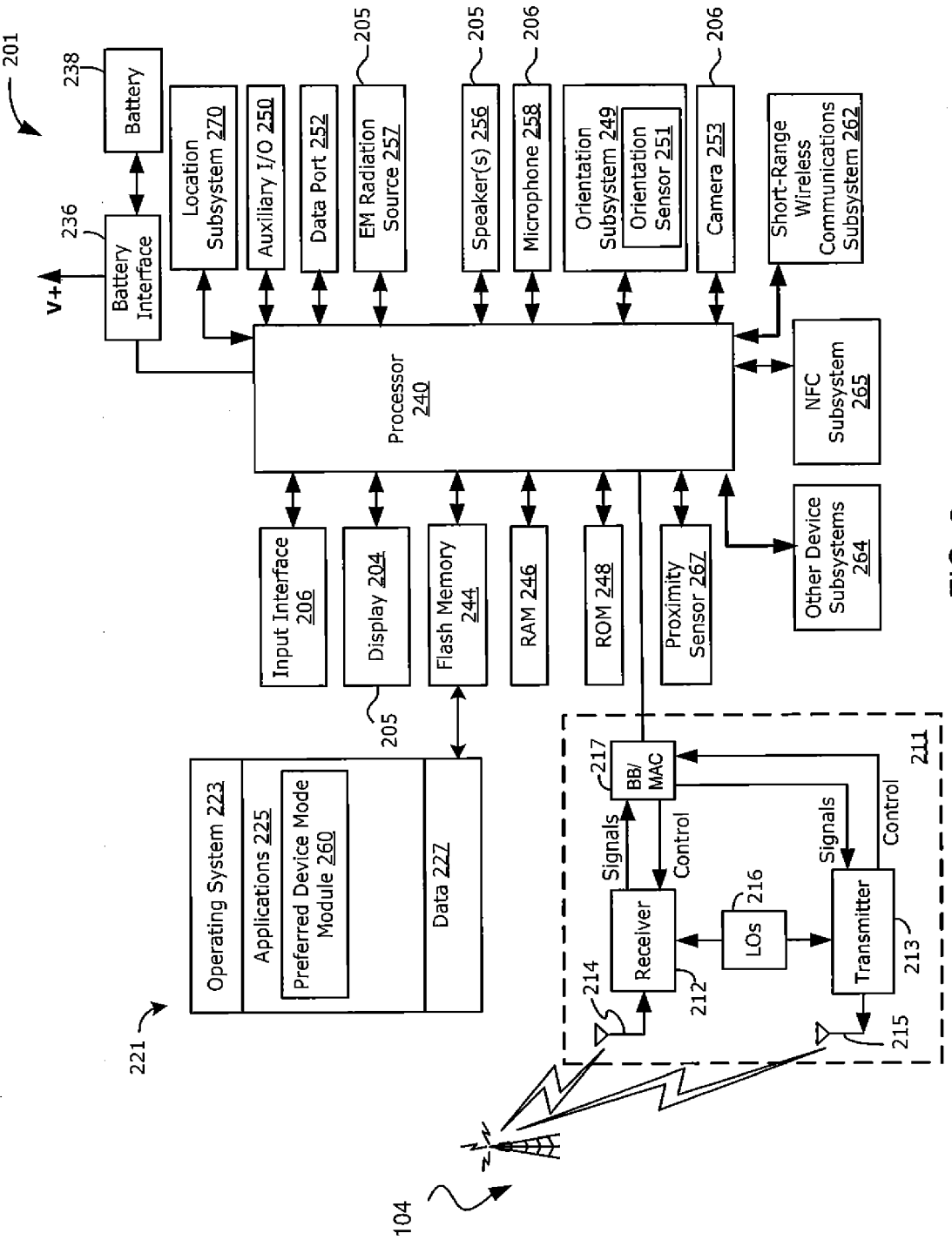

201
238
Battery
236
Battery Interface
V+
Location Subsystem 270
Auxiliary I/O 250
Data Port 252
205
EM Radiation Source 257
205
Speaker(s) 256
206
Microphone 258
Orientation Subsystem 249
Orientation Sensor 251
206
Camera 253
Short-Range Wireless Communications Subsystem 262
Processor 240
NFC Subsystem 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
Signals
Control
Receiver
LOs
216
Transmitter
214
212
213
215
104

FIG. 2

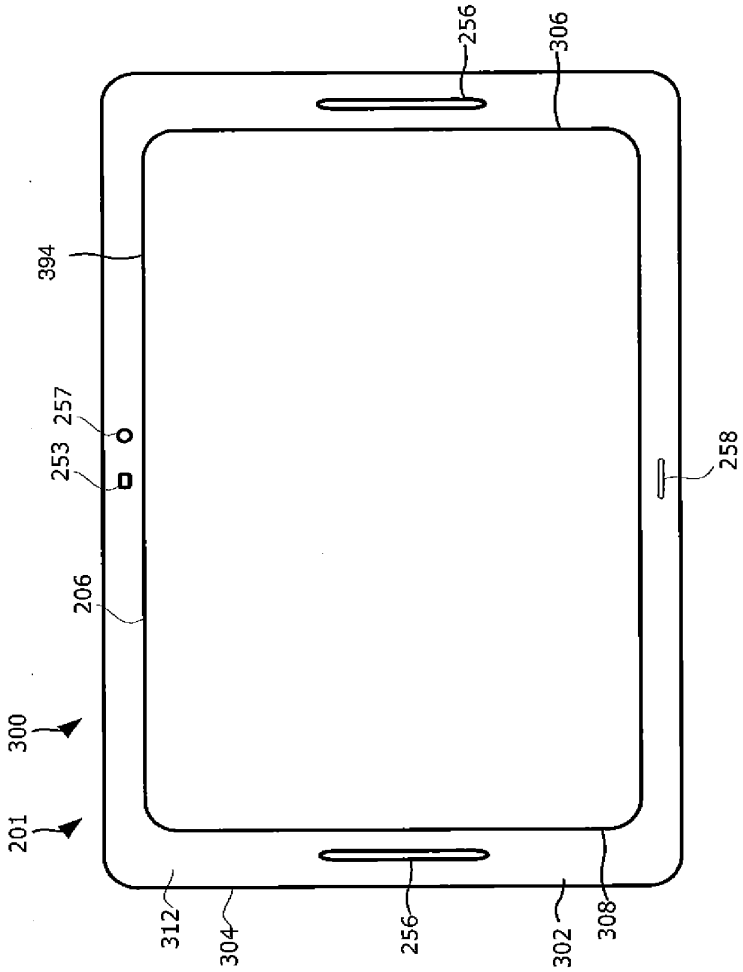

256
306
394
257
253
258
206
300
201
312
304
256
302
308

FIG. 4

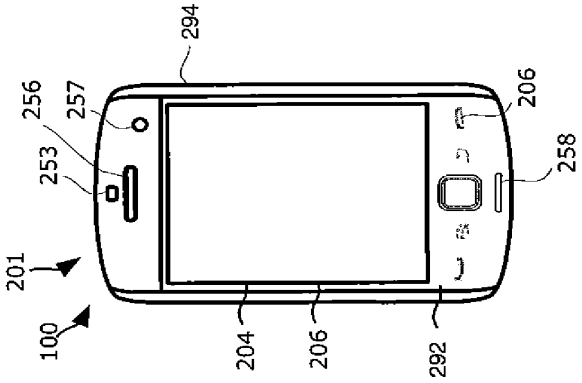

294
256
257
206
253
258
201
100
204
206
292

FIG. 3

FIG. 5

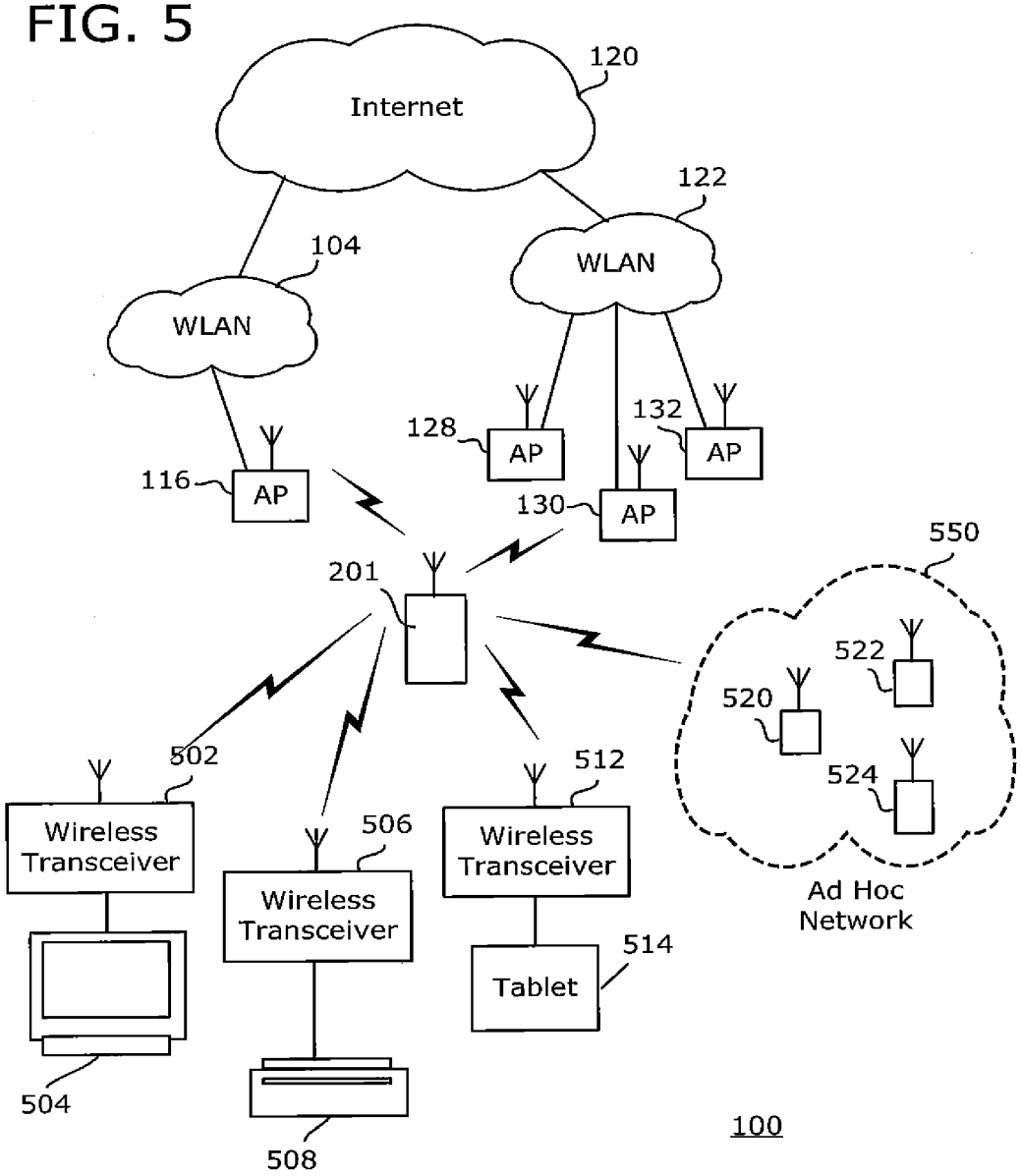

Internet
120
122
WLAN
104
WLAN
128
AP
132
AP
116
AP
130
AP
201
550
522
520
524
Ad Hoc
Network
502
Wireless
Transceiver
506
Wireless
Transceiver
512
Wireless
Transceiver
514
Tablet
504
508
100

FIG. 6

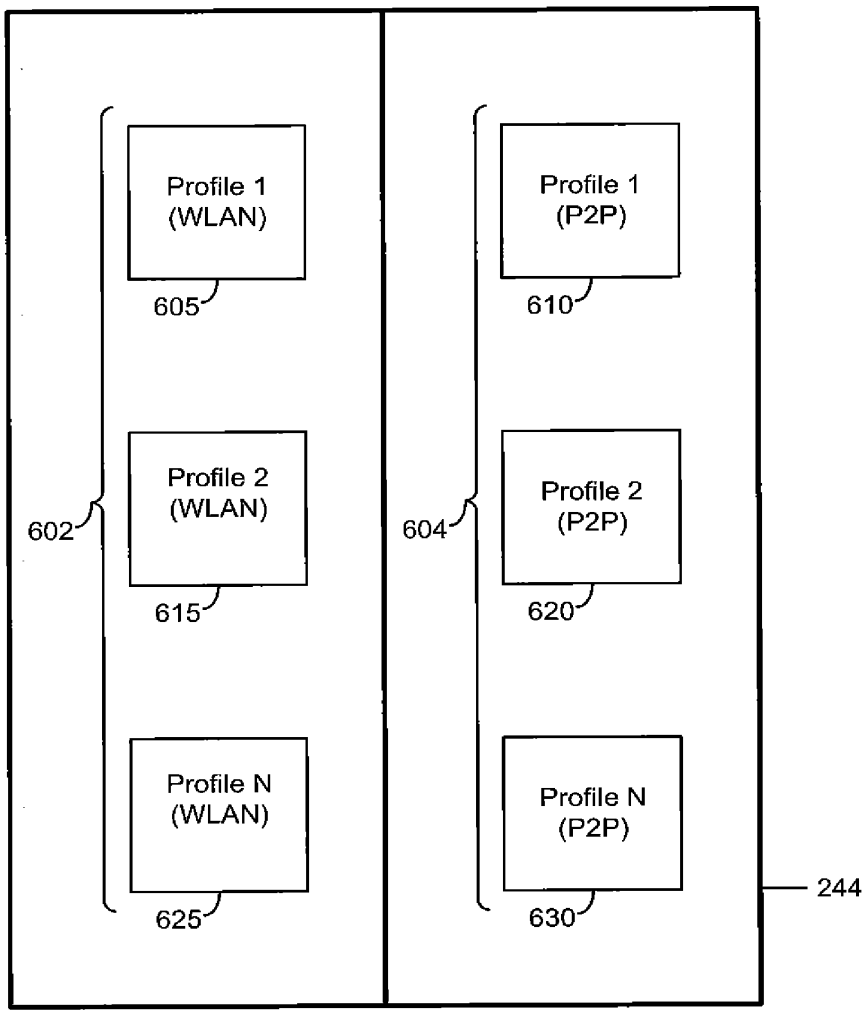
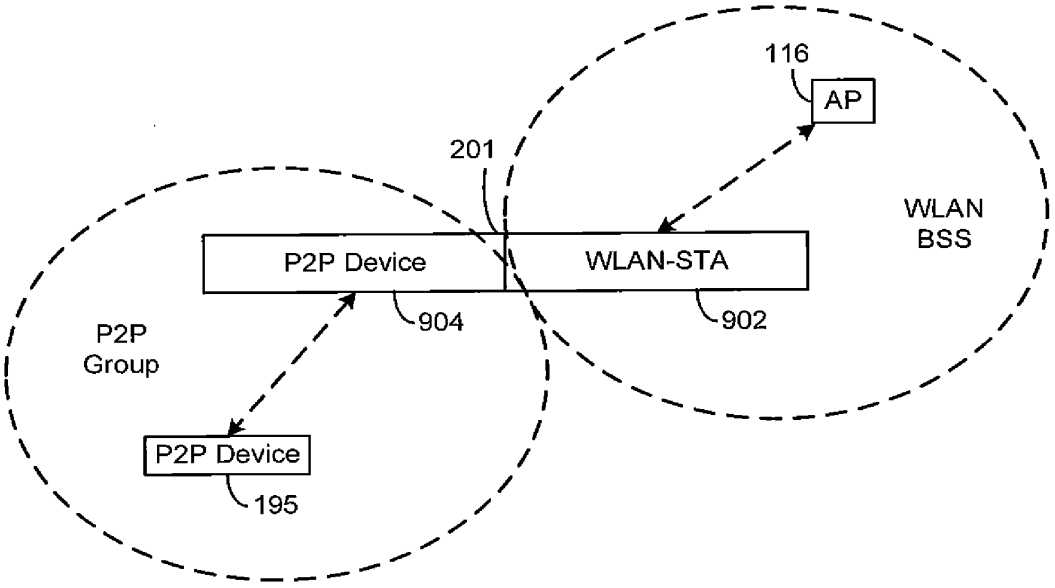

Profile 1
(WLAN)
605
Profile 2
(WLAN)
615
Profile N
(WLAN)
625
602
Profile 1
(P2P)
610
Profile 2
(P2P)
620
Profile N
(P2P)
630
604
244

FIG. 7


116
AP
201
WLAN
BSS
P2P Device
WLAN-STA
904
902
P2P
Group
P2P Device
195

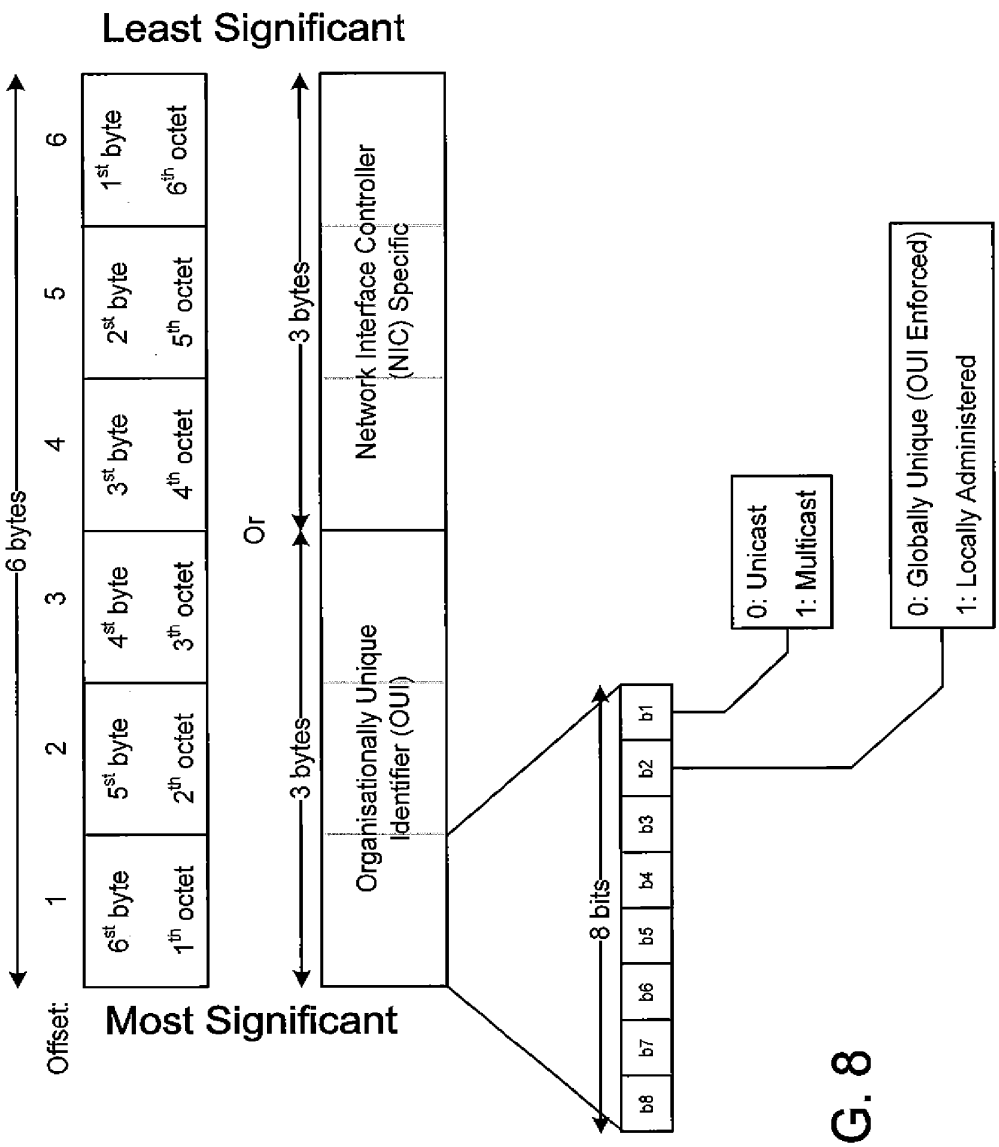
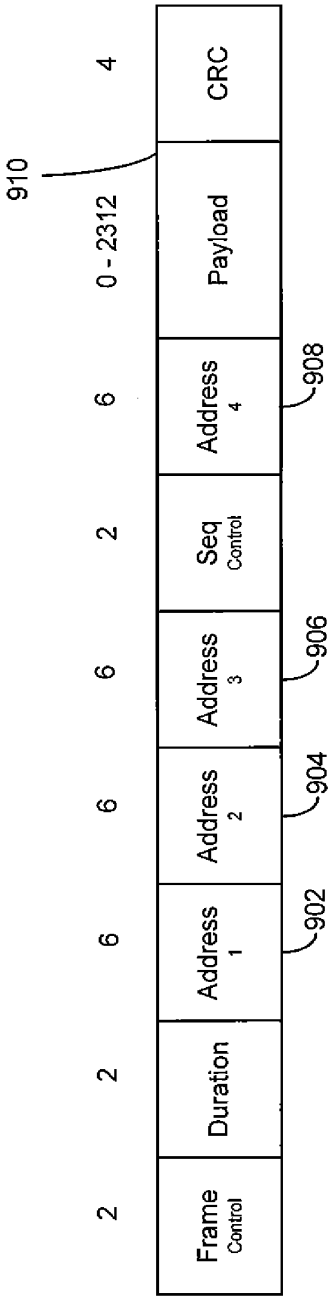

Least Significant
Most Significant
Offset:
1
2
3
4
5
6
6 bytes
6st byte
1th octet
5st byte
2th octet
4st byte
3th octet
3st byte
4th octet
2st byte
5th octet
1st byte
6th octet
Or
3 bytes
3 bytes
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b1
b2
b3
b4
b5
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

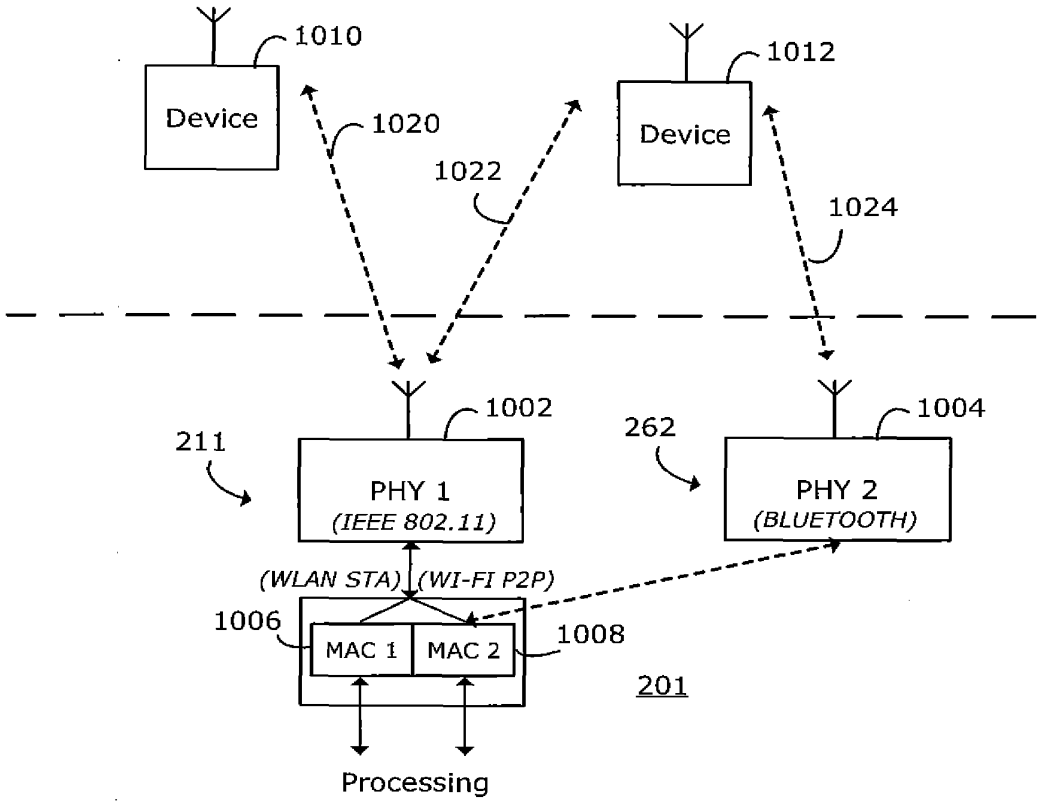

Device
1010
1020
1022
Device
1012
1024
1002
1004
211
262
PHY 1
(IEEE 802.11)
PHY 2
(BLUETOOTH)
(WLAN STA)
(WI-FI P2P)
1006
MAC 1
MAC 2
1008
201
Processing

FIG. 11

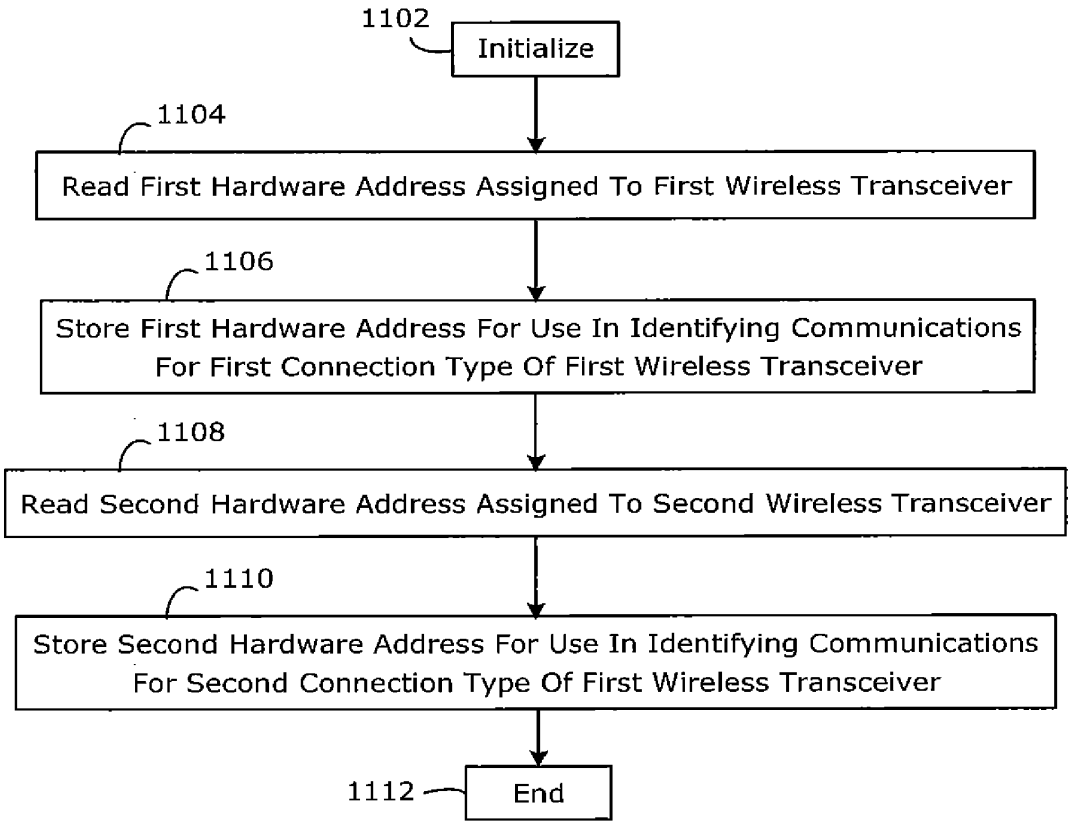
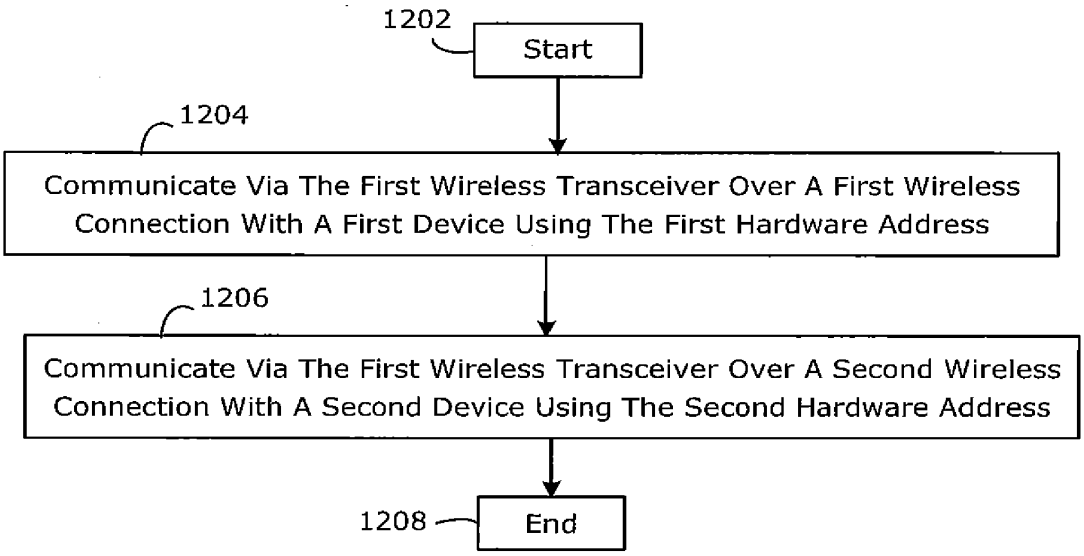

1102
Initialize
1104
Read First Hardware Address Assigned To First Wireless Transceiver
1106
Store First Hardware Address For Use In Identifying Communications For First Connection Type Of First Wireless Transceiver
1108
Read Second Hardware Address Assigned To Second Wireless Transceiver
1110
Store 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 206 of 553

(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 209 of 553

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 210 of 553

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 211 of 553

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-

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 213 of 553

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 214 of 553

[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 215 of 553

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 216 of 553

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 217 of 553

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 218 of 553

(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 219 of 553

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 220 of 553

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 221 of 553

"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 222 of 553

(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 223 of 553

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 224 of 553

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 225 of 553

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 226 of 553

FIG 1

Stand der Technik

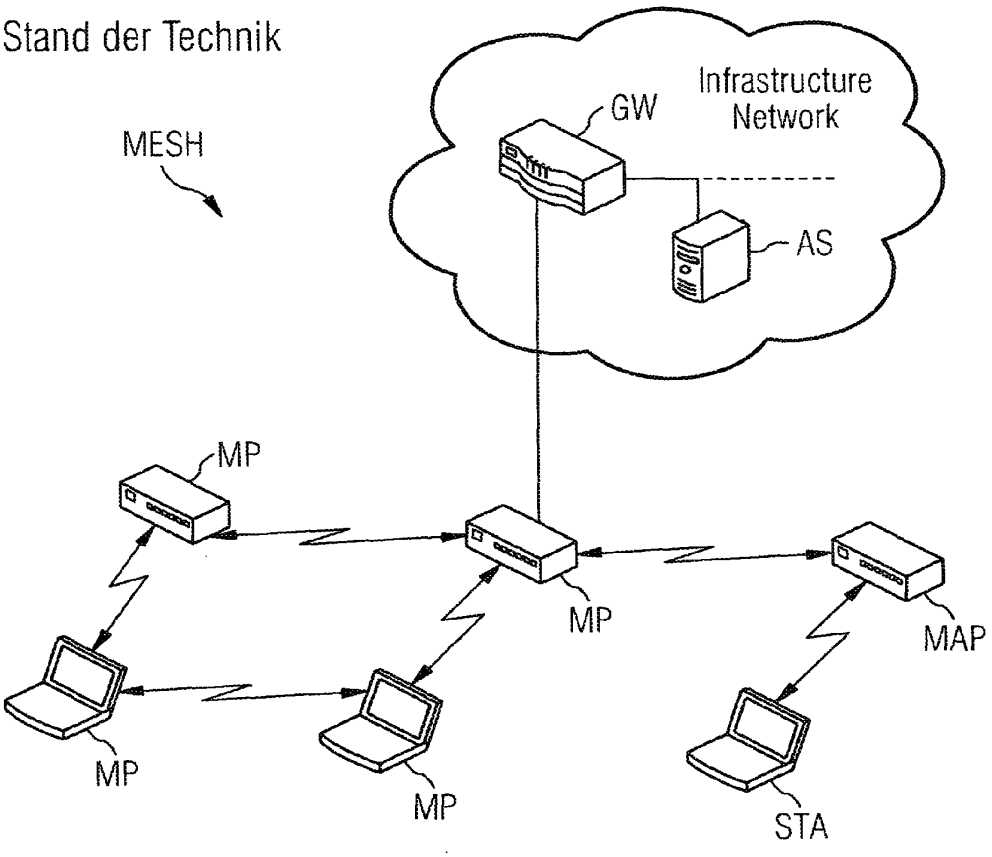


FIG 2
Stand der Technik

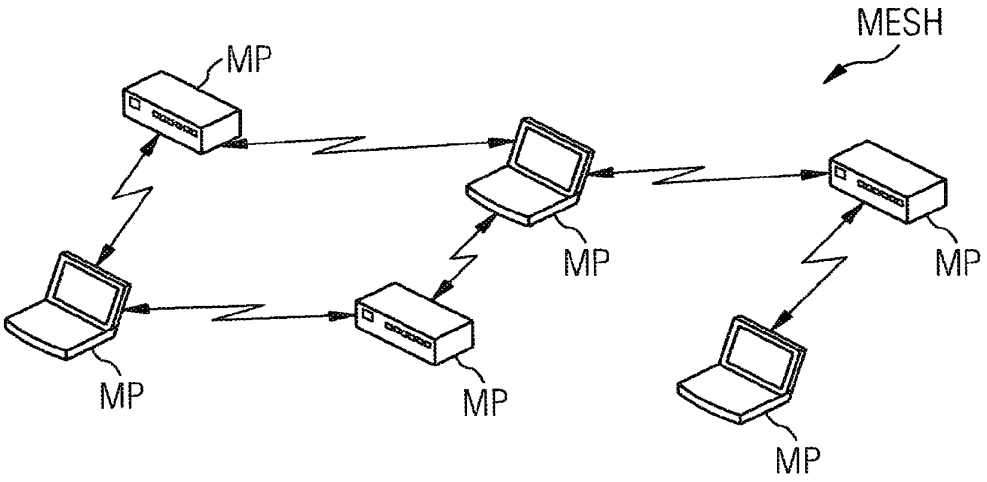


FIG 3
Stand der Technik

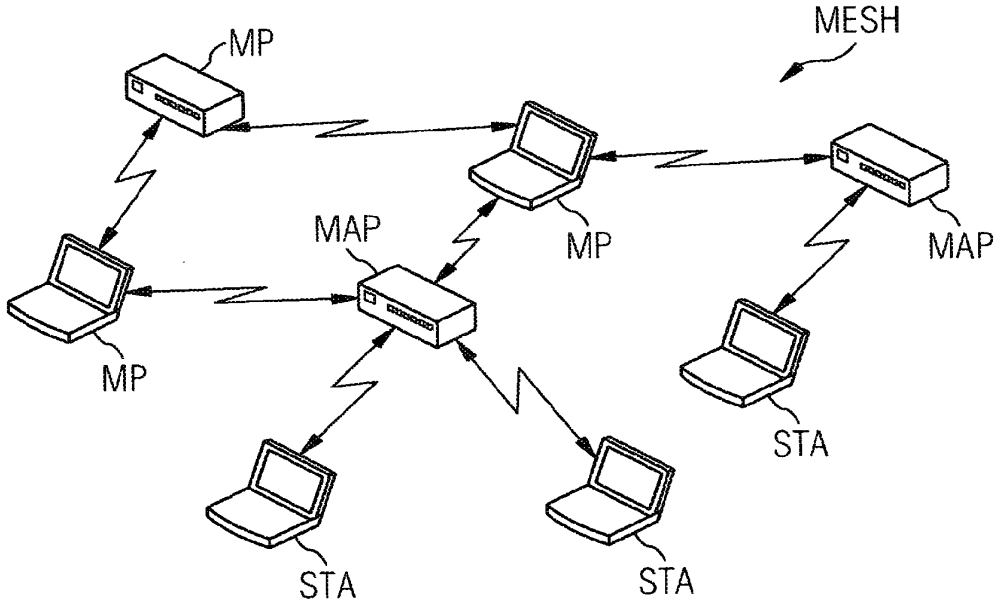


FIG 4
Stand der Technik

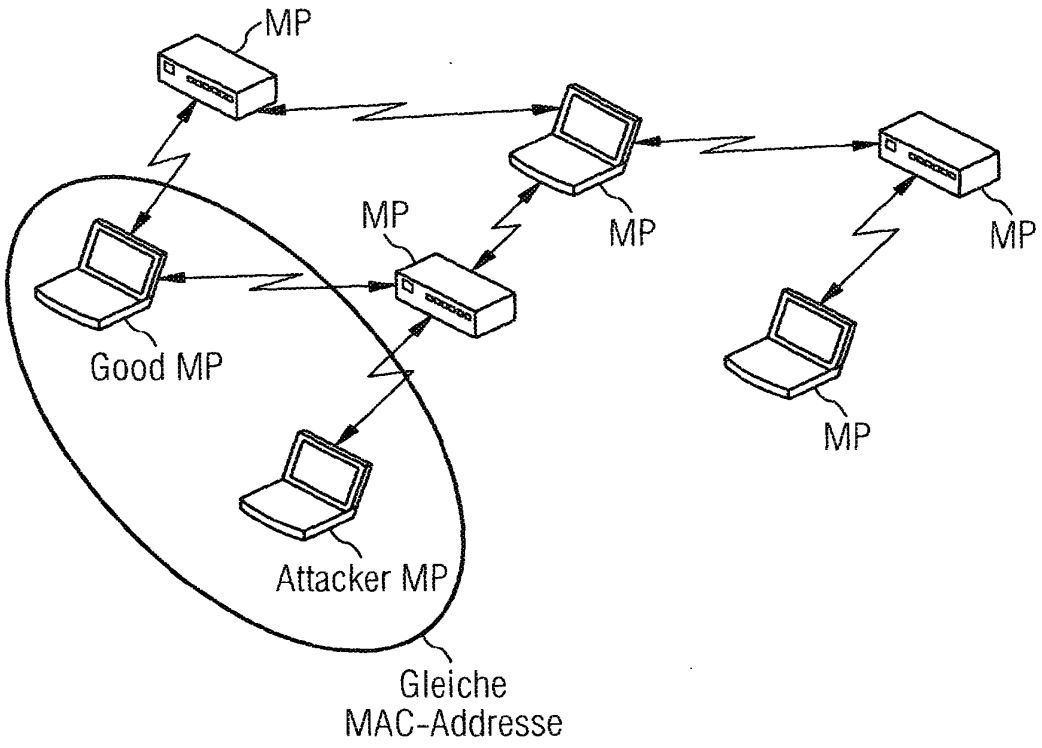


FIG 5

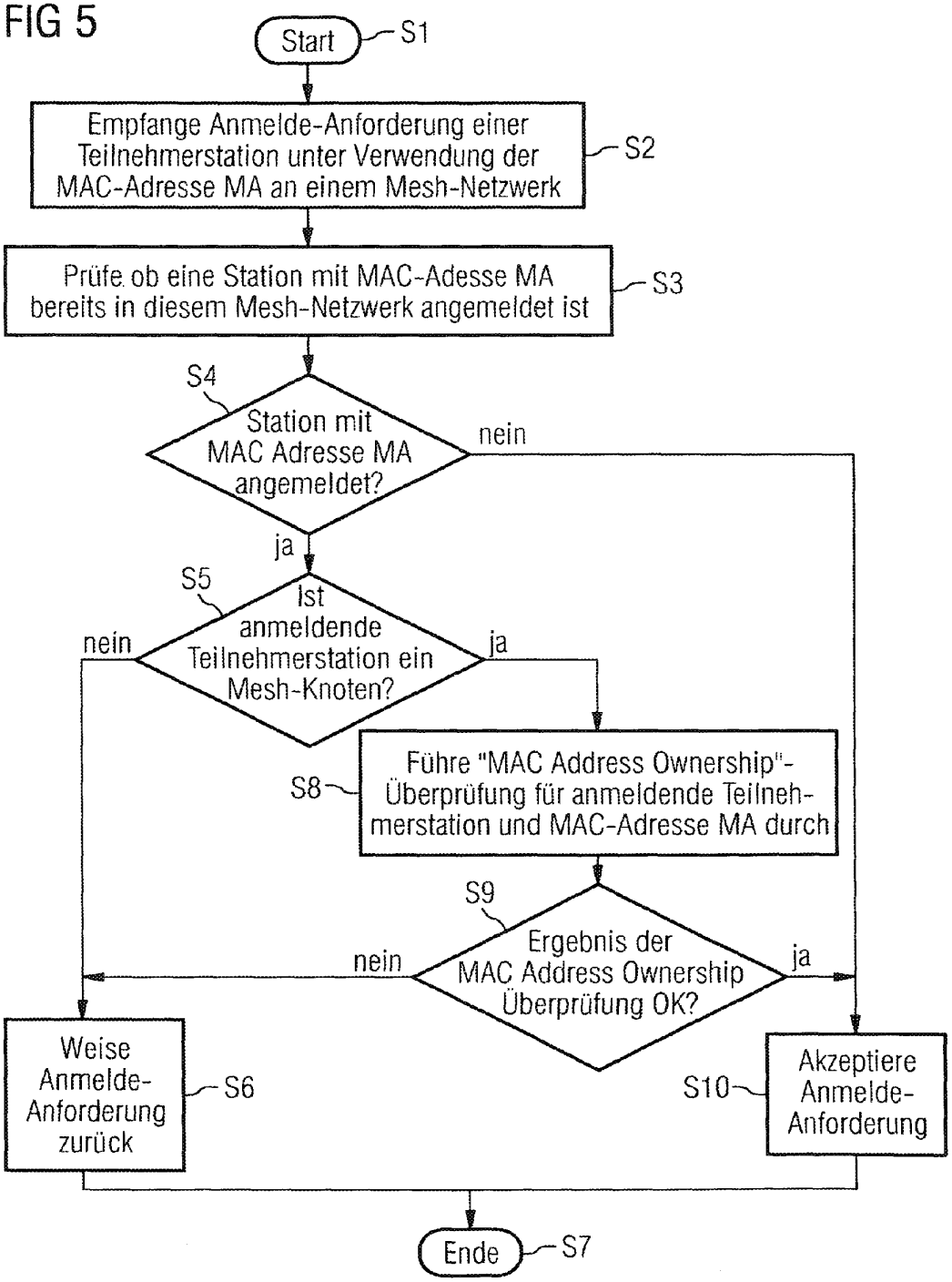
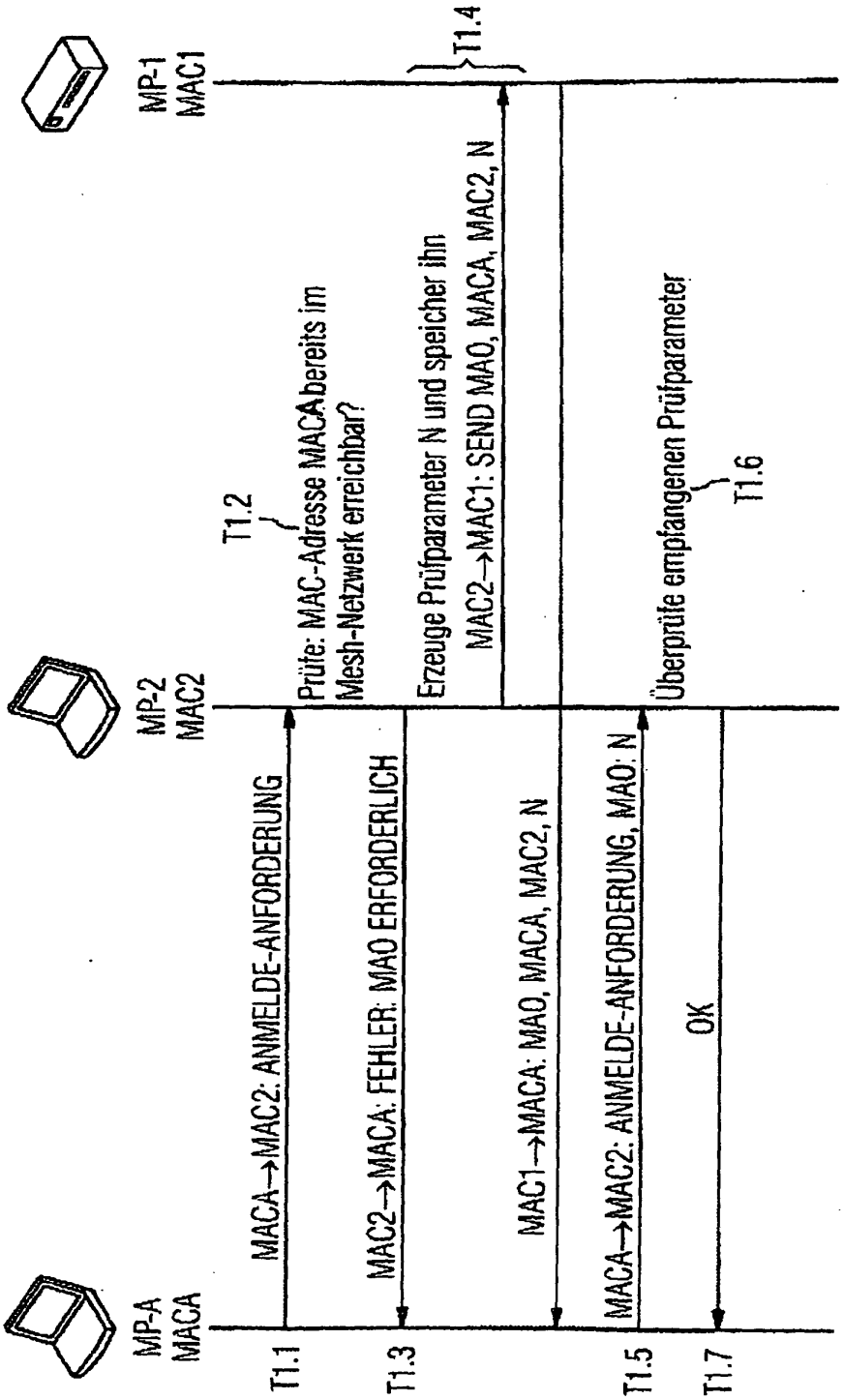

Start
S1
Empfange Anmelde-Anforderung einer Teilnehmerstation unter Verwendung der MAC-Adresse MA an einem Mesh-Netzwerk
S2
Prüfe ob eine Station mit MAC-Adesse MA bereits in diesem Mesh-Netzwerk angemeldet ist
S3
S4
Station mit MAC Adresse MA angemeldet?
nein
ja
S5
Ist anmeldende Teilnehmerstation ein 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



Samsung Ex. 1004, Page 231 of 553

FIG 7

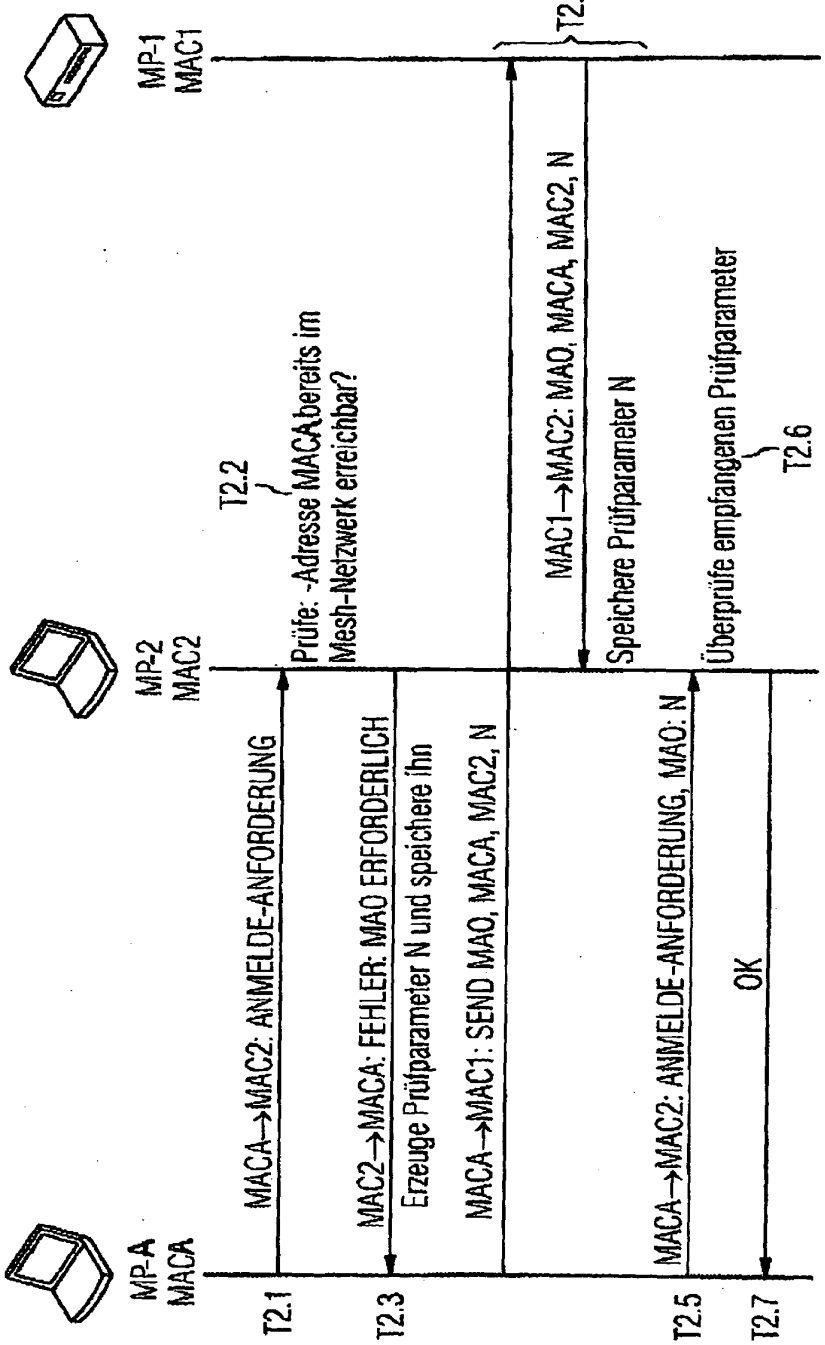

MP-A
MACA
MP-2
MAC2
MP-1
MAC1
MACA→MAC2: ANMELDE-ANFORDERUNG
T2.1
T2.2
Prüfe: -Adresse MACA bereits im Mesh-Netzwerk erreichbar?
MAC2→MACA: FEHLER: MAO ERFORDERLICH
T2.3
Erzeuge Prüfparameter N und speichere ihn
MACA→MAC1: SEND MAO, MACA, MAC2, N
MAC1→MAC2: MAO, MACA, MAC2, N
T2.4
Speichere Prüfparameter N
MACA→MAC2: ANMELDE-ANFORDERUNG, MAO: N
T2.5
Überprüfe empfangenen Prüfparameter
T2.6
OK
T2.7

FIG 8

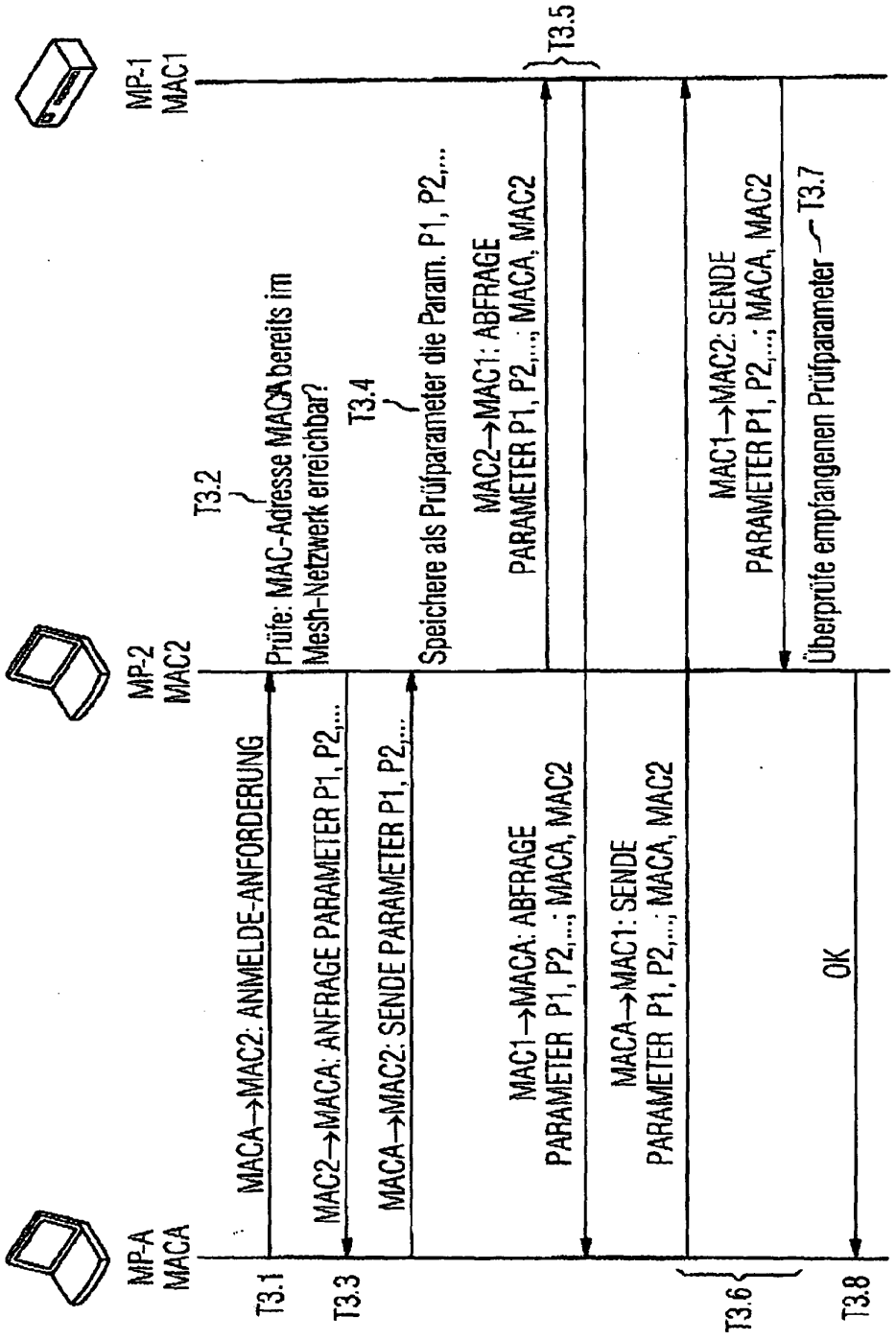

MP-A
MACA
MP-2
MAC2
MP-1
MAC1
T3.1
MACA→MAC2: ANMELDE-ANFORDERUNG
T3.2
Prüfe: MAC-Adresse MACA bereits im Mesh-Netzwerk erreichbar?
T3.3
MAC2→MACA: ANFRAGE PARAMETER P1, P2,...
MACA→MAC2: SENDE PARAMETER P1, P2,...
T3.4
Speichere als Prüfparameter die Param. P1, P2,...
MAC2→MAC1: ABFRAGE PARAMETER P1, P2,...; MACA, MAC2
T3.5
MAC1→MACA: ABFRAGE PARAMETER P1, P2,...; MACA, MAC2
MACA→MAC1: SENDE PARAMETER P1, P2,...; MACA, MAC2
MAC1→MAC2: SENDE PARAMETER P1, P2,...; MACA, MAC2
T3.6
Überprüfe empfangenen Prüfparameter
T3.7
OK
T3.8

FIG 9

Stand der Technik

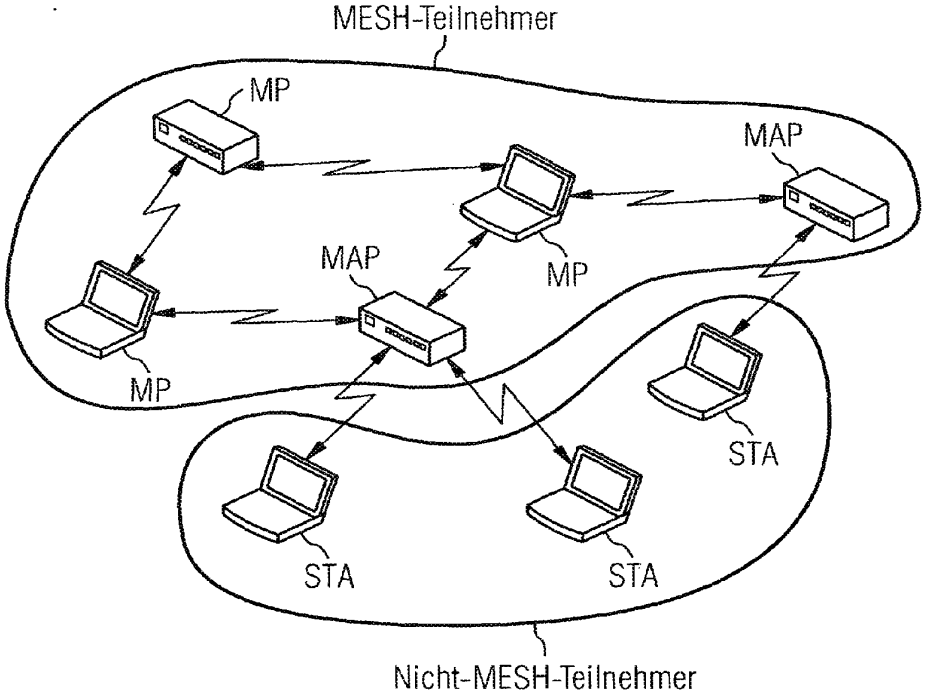


FIG 10

Stand der Technik

RA	TA	DA	SA	DATA	FCS

FIG 11 Stand der Technik

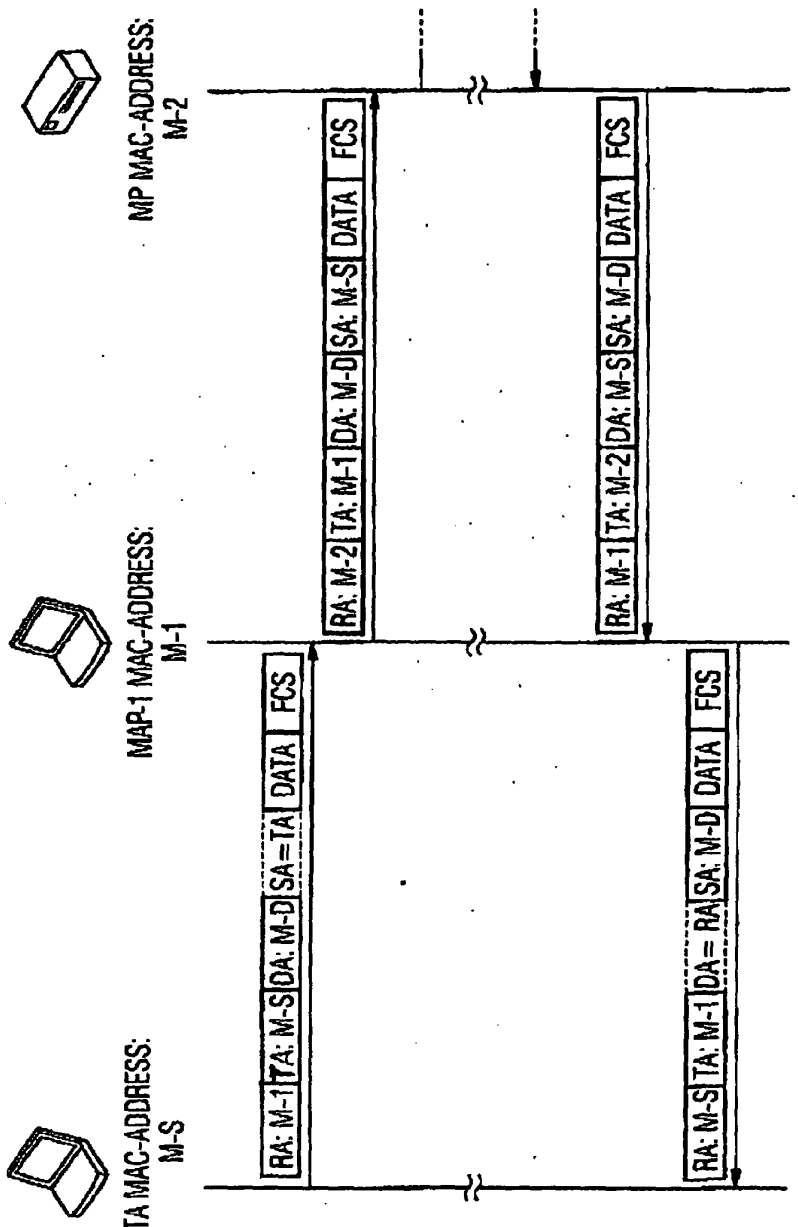
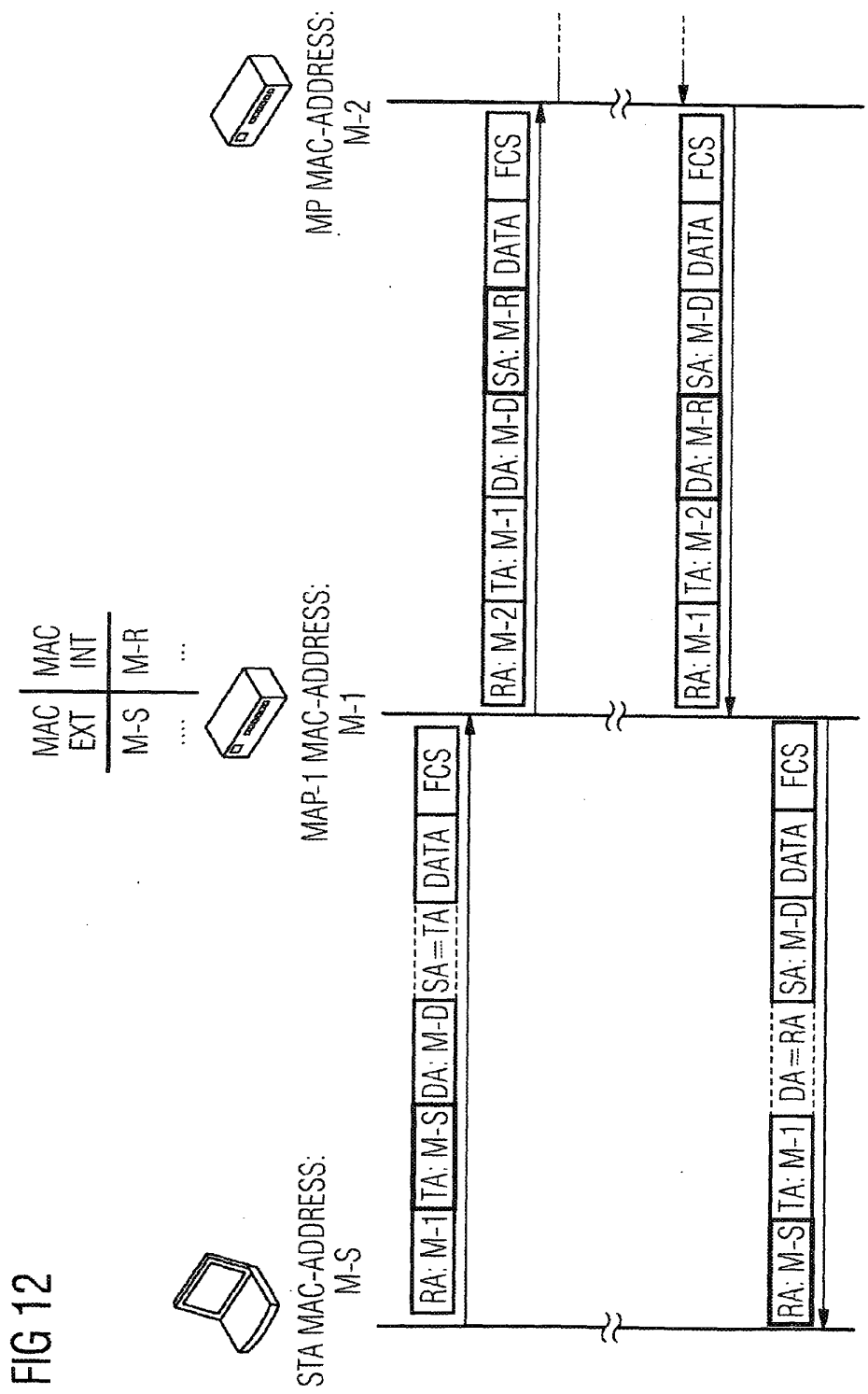


FIG 12


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 237 of 553

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 #
18/448,281	**09/18/2023 03:28:09 PM ET**	**020505-000006**

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 #	1540	FILED BY	W. Pat Moore
PATENT CENTER #	62815809	FILING DATE	08/11/2023
CUSTOMER #	30565	FIRST NAMED INVENTOR	Sai C. Manapragada
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Blake Hartz

Documents

TOTAL DOCUMENTS: 13

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
Preliminary Amendment_20505-6.pdf		12	-	46 KB
Preliminary Amendment_20505-6-A.PE.pdf	(1-1)	1	Preliminary Amendment	16 KB
Preliminary Amendment_20505-6-CLM.pdf	(2-10)	9	Claims	38 KB
Preliminary Amendment_20505-6-REM.pdf	(11-12)	2	Applicant Arguments/Remarks Made in an Amendment	19 KB

IDS transmittal_20505-6.pdf	4	Transmittal Letter	24 KB
20505-6 PTOSB08.pdf	3	Information Disclosure Statement (IDS) Form (SB08)	540 KB

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

for_EP3174323B1.pdf	31	Foreign Reference	398 KB
for_EP2016750B1.pdf	22	Foreign Reference	353 KB
for_EP2713670A1.pdf	28	Foreign Reference	501 KB
for_WO2014020407A1.pdf	45	Foreign Reference	1644 KB
for_EP3220697B1.pdf	41	Foreign Reference	1663 KB
for_EP2055072B1.pdf	31	Foreign Reference	513 KB
npl_Eng EP2055072B1 - Method and arrangement for provision of a wire-free mesh network - Google Patents.pdf	15	Non Patent Literature	8871 KB
for_EP1878169B1.pdf	91	Foreign Reference	18974 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Preliminary Amendment_20505-6.pdf	A1AB092A83B8EF4AD486A185915DE34AFBE270D25A6A58FB1816987B7DBEE7CC9068075A577887AC518D607946B2274495BCCDDFF7984FD7689079A02336B7E7
Preliminary Amendment_20505-6-A.PE.pdf	9DFB4A3B0891C79D7AC54A88225CBC5A98877F285349BCC7A2BB63470871088057CD4504A873D2F058A590AD8D148FC9B12317608DFBF8A1ECCEA65C63F5A10E

Preliminary Amendment_20505-6-CLM.pdf	8B7684847CC34E76394B23C4390D82F84596EA8342660B632F FDA8FBA3A914887A814CAA4B40434DEB8AE7B6FB2501F0B0F 02094225FB54F1BDB25008106BF7A
Preliminary Amendment_20505-6-REM.pdf	A850F92305D2757214802CB9248FAE746F7D4554D4FD8FAD3 E8CB728BF279F54B92C9CDD1F8D00703B140B25F2748757558 C0CEB5890C57890631E1DECC270E2
IDS transmittal_20505-6.pdf	8B5B587EE6E31A0097E7EBDE13940325E2D6882438BBF1FC0 D35921D90001A049754B9AADEC3FCA6975495E9924E0E83E9 22001E99DB4569B0F852460E9FA6B6
20505-6 PTOSB08.pdf	64EC774A8641E7CD40DF9B8934B0093CC9C336F53C8AACB8 886F29462236C186CECEC60B31CFAC82EB478D797DD9FE913 966AC9C8AB54CC13844DCDC60968E73
for_EP3174323B1.pdf	1106407D4184786449FC2C0AAF990B2A7928D5C5743B445A45 91223710FD8938B330B14937CD1D098C41A331D3AED41D0B2 4526B715303D11E95C8D7FB5E3ED5
for_EP2016750B1.pdf	5C2CA4633498891C7CC37DB3D9B87702AA75A840BFDA049E B70B9DF40E2A7E77C429001C0ADED3ACA8A1BB0DA64DCA9 D1A489124D4EE33B4C04DC0C8F2A4BA24
for_EP2713670A1.pdf	D309034C1D92F0223E7354D2F2AB7A427F9712B7D1F54274A7 BE1130CBA231A130FB52A6FB214A1D81DD47F1ACBA1CFB0B 27927943387783C54815EE77E63BE6
for_WO2014020407A1.pdf	E27965FE5F588B5E251353BDF7141D2AF4B2665731BE7A7069 14E9571215FAB45498B82C265DA589B10BD0DFD040FEEC73C 7B5041F1ACE7B5D6F37AF5AFE2AC0
for_EP3220697B1.pdf	F90C74266902E8C14C2107CC02FC21AA7B12C24525115339B2 F956DA61382FC8F5531433176FF9CE367DBA1BACD72CF13EB 962F23E1F076B105D3756CB464C4C
for_EP2055072B1.pdf	9D25FDA5D3D2C02FCBC8A5B945681B3C974A5FF0A763B9AF E4EF22999433924A774DBF183FCD6A6C8AAB23282CCCAF840 20449A0F33B8219F17B220654FF3021

npl_Eng EP2055072B1 - Method and arrangement for provision of a wire-free mesh network - Google Patents.pdf	B1D0A0D1282AAB7D17634DF41E9857F520075CB38FAA0ECC3B538B7E607C7EFDF784589057C510567FDFBAE477ADBA94FCCF5834A13A944BDBBBBC9C1737AC87
for_EP1878169B1.pdf	15B257C7642CD41194758BC8B3E51E4B22AB4E855BCD100DBBD391C97DE8C69A88329DADAC9EA0227506BC9425EFF504BC5202601116E3A09F2E454B78C4A275

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 0a0238' 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 248 of 553

- 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 250 of 553

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.

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.

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 253 of 553

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 254 of 553

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 255 of 553

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 257 of 553

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 258 of 553

- 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 259 of 553

[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 260 of 553

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 261 of 553

- 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 262 of 553

[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

Samsung Ex. 1004, Page 263 of 553

(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 264 of 553

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 265 of 553

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 266 of 553

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 267 of 553

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 268 of 553

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 269 of 553

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 270 of 553

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 271 of 553

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 272 of 553

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 273 of 553

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 274 of 553

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 275 of 553

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 276 of 553

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 277 of 553

[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 278 of 553

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 279 of 553

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 280 of 553

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 281 of 553

- 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

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 283 of 553

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 284 of 553

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. 2j.
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 285 of 553

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

Samsung Ex. 1004, Page 287 of 553

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 289 of 553

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

Samsung Ex. 1004, Page 290 of 553

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 291 of 553