

wobei der Zugangsknoten **dadurch gekennzeichnet ist, dass**

- der Zugangsknoten eine erste virtuelle lokale Netzwerkfunktion zum Implementieren eines ersten virtuellen lokalen Netzwerks (43) aufweist, das den Zugangsknoten und eine lokale virtuelle Router-Funktionseinheit (49) des Breitband-Fernzugangsservers aufweist,
- für jedes einzelne der Mehrzahl von Dienst bereitstellenden Netzwerken, der Zugangsknoten eine zweite virtuelle lokale Netzwerkfunktion aufweist, wobei jede zweite virtuelle lokale Netzwerkfunktion dem Implementieren eines entsprechenden zweiten virtuellen lokalen Netzwerks (41.1, 41.2) dient, das den Zugangsknoten und eine entsprechende von zugeordneten virtuellen Router-Funktionseinheiten (47.1, 47.2) des Breitband-Fernzugangsservers aufweist, wobei die entsprechende der zugeordneten virtuellen Router-Funktionseinheiten der Kommunikation mit dem entsprechenden von der Mehrzahl von Dienst bereitstellenden Netzwerken dient, wobei die entsprechende zugeordnete virtuelle Router-Funktionseinheit angepasst ist, um Ethernet-Rahmen direkt von und zu einem Breitband-Zugangsserver (19) des entsprechenden der Dienst bereitstellenden Netzwerke zu übertragen,
- der Speicher Identifizierungen von Ethernet-Rahmen speichert, die in
 - dem ersten virtuellen lokalen Netzwerk und
 - den zweiten virtuellen lokalen Netzwerken übertragen werden,

und

- der Zugangsknoten eine mit der Handhabungseinheit verbundene Steuereinheit umfasst,

wobei die Steuereinheit vorgesehen ist, zum

- Befehlen der Handhabungseinheit, Rahmen von einer neuen Benutzervorrichtung, die sich selbst mit dem Zugangspunkt verbunden hat, in das erste virtuelle lokale Netzwerk zu übertragen,
- Empfangen von Information von dem Breitband-Fernzugangsserver in Bezug auf ein Routen von Rahmen, und
- Befehlen der Handhabungseinheit, Rahmen von einer Benutzervorrichtung, die mit dem Zugangspunkt verbunden ist, anstelle von in das erste virtuelle lokale Netzwerk in eines der zweiten virtuellen lokalen Netzwerke zu übertragen, wie durch von dem Breitband-Fernzugangsserver erhaltene Information angegeben wird, wobei die Rahmen dadurch zu dem Breitband-Zugangsserver des entsprechenden Dienst bereitstellenden Netzwerks übertragen werden.

2. Zugangsknoten nach Anspruch 1, wobei die Steuereinheit angepasst ist, um Information zu empfangen, die eine Medium Access Control, MAC, Adresse eines mit dem Zugangspunkt verbundenen Benutzervorrichtung aufweist, und um der Handhabungseinheit zu befehlen, Rahmen von dieser Adresse in das eine der zweiten virtuellen lokalen Netzwerke zu übertragen.

3. Zugangsknoten nach Anspruch 2, wobei die MAC-Adresse eine virtuelle MAC-Adresse ist und der Zugangsknoten eine Übersetzungseinheit zum Übersetzen der virtuellen MAC-Adresse in eine MAC-Adresse der Benutzervorrichtung aufweist.

4. Verfahren für eine Benutzervorrichtung (15, 15'), zum Verbinden mit einem von einer Mehrzahl von Dienst bereitstellenden Netzwerken (3.1, 3.2) durch ein Breitband-Zugangsnetzwerk (29), wobei das Verfahren die folgenden Schritte aufweist:

- die Benutzervorrichtung verbindet mit dem Breitband-Zugangsnetzwerk,
- ein Zugangsknoten (13) empfängt einen Rahmen oder mehrere Rahmen von der Benutzervorrichtung und leitet den Rahmen oder die Rahmen in ein erstes virtuelles lokales Netzwerk (43) weiter,
- eine lokale virtuelle Router-Funktionseinheit (49) empfängt den Rahmen oder die Rahmen, die in dem ersten virtuellen lokalen Netzwerk empfangen wurden,
- wobei das Verfahren **dadurch gekennzeichnet ist, dass** das Verfahren weiter die folgenden Schritte umfasst:
- die lokale virtuelle Router-Funktionseinheit beginnt einen Identifizierungs- und Authentifizierungsvorgang für die Benutzervorrichtung,
- die Benutzervorrichtung sendet in dem Identifizierungs- und Authentifizierungsvorgang Auswahlinformation, die eines von einer Mehrzahl von Dienst bereitstellenden Netzwerken anzeigt,
- nach einem erfolgreichen Identifizierungs- und Authentifizierungsvorgang empfängt der Zugangsknoten eine Anweisung von einem Breitband-Fernzugangsserver (17), um eine Adresse der Benutzervorrichtung einem der

- zweiten virtuellen lokalen Netzwerke (41.1, 41.2) zuzuordnen, wobei jedes der virtuellen lokalen Netzwerke den Zugangsknoten und eine von zugeordneten virtuellen Router-Funktionseinheiten (47.1, 47.2) des Breitband-Fernzugangsservers aufweist, wobei die eine der zugeordneten virtuellen Router-Funktionseinheiten der Auswahlinformation entspricht, und basierend auf der Anweisung die von der Benutzervorrichtung empfangenen Rahmen in das eine der zweiten virtuellen lokalen Netzwerke weiterleitet anstelle von in das erste virtuelle lokale Netzwerk, wobei jede der virtuellen Router-Funktionseinheiten angepasst ist, um Ethernet-Rahmen direkt von und zu einem Breitband-Zugangsserver (19) eines entsprechenden von den Dienst bereitstellenden Netzwerken (3.1, 3.2) zu übertragen, und
- der Breitband-Fernzugangsserver leitet Rahmen von der Benutzervorrichtung, die in dem einen der zweiten virtuellen lokalen Netzwerke empfangen wurden, in das entsprechende eine von der Mehrzahl von Dienst bereitstellenden Netzwerken weiter.
5. Verfahren nach Anspruch 4, wobei in dem Schritt, in dem die Benutzervorrichtung mit dem Breitband-Zugangsnetzwerk verbindet, diese mit dem Zugangspunkt des Breitband-Zugangsnetzwerks verbindet.
6. Verfahren nach Anspruch 4, wobei in dem Schritt, in dem der Rahmen oder die Rahmen in dem ersten virtuellen lokalen Netzwerk empfangen werden, der Rahmen oder die Rahmen von der lokalen virtuellen Router-Funktionseinheit, die den Identifizierungs- und Authentifizierungsvorgang beginnt, empfangen werden.
7. Verfahren nach Anspruch 4, wobei bei dem Identifizierungs- und Authentifizierungsvorgang die Benutzervorrichtung durch Senden von Identifizierungsinformation, die die Auswahlinformation von einem von der Mehrzahl von Dienst bereitstellenden Netzwerken aufweist, beginnt.
8. Breitband-Fernzugangsserver (17) zum Bereitstellen, für Benutzervorrichtungen (15, 15'), die mit dem Breitband-Fernzugangsserver durch einen Zugangsknoten (13) oder einen Zugangspunkt (7) verbunden sind, von Breitbandzugang zu einer Mehrzahl von Dienst bereitstellenden Netzwerken (3.1, 3.2), die von Dienst bereitstellenden Heimnetzwerken von Benutzern der Benutzervorrichtungen verschieden sind, wobei der Breitband-Fernzugangsserver aufweist:
- eine Diensteinheit zum Speichern und Bereitstellen von Information über die Mehrzahl von Dienst bereitstellenden Netzwerken, wobei der Breitband-Fernzugangsserver **dadurch gekennzeichnet ist, dass** der Breitband-Fernzugangsserver angepasst ist, um:
 - eine Benutzervorrichtung mit der Diensteinheit zu verbinden, wobei die Diensteinheit angepasst ist, um Information über die Mehrzahl von Dienst bereitstellenden Netzwerken an die Benutzervorrichtung zu senden,
 - von einer Benutzervorrichtung Information über ein ausgewähltes von der Mehrzahl von Dienst bereitstellenden Netzwerken zu empfangen,
 - anschließend Information über ein ausgewähltes von der Mehrzahl von Dienst bereitstellenden Netzwerken, wie von der Benutzervorrichtung empfangen, an das ausgewählte eine von den Dienst bereitstellenden Netzwerken weiterzuleiten,
 - anschließend Authentifizierungsinformation zwischen dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken und der Benutzervorrichtung auszutauschen,
 - anschließend Information über den Erfolg oder mangelnden Erfolg des Authentifizierungsvorgangs zu empfangen, und
 - schließlich die empfangene Information zu verwenden, wenn Erfolg angezeigt wird, um Daten von der Benutzervorrichtung zu dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu routen und um Daten von dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu der Benutzervorrichtung zu routen,
- wobei der Breitband-Fernzugangsserver aufweist
- eine lokale virtuelle Router-Funktionseinheit (49),
- wobei der Breitband-Fernzugangsserver angepasst ist, um die lokale virtuelle Router-Funktionseinheit in einem ersten virtuellen lokalen Netzwerk (43) aufzuweisen, das auch den Zugangsknoten oder den Zugangspunkt aufweist, und
- zugeordnete virtuelle Router-Funktionseinheiten (47.1, 47.2), wobei jede zugeordnete virtuelle Router-Funktionseinheit angepasst ist, um mit einem entsprechenden einen von einer Mehrzahl von zweiten virtuellen

lokalen Netzwerken (41.1, 41.2) zu kommunizieren, wobei jedes der zweiten virtuellen lokalen Netzwerke den Zugangsknoten oder den Zugangspunkt aufweist,

5 wobei jede der zugeordneten virtuellen Router-Funktionseinheiten angepasst ist, um Daten direkt von dem entsprechenden einen der Dienst bereitstellenden Netzwerke zu dem Zugangsknoten oder dem Zugangspunkt und von dem Zugangsknoten oder dem Zugangspunkt zu dem entsprechenden einen der Dienst bereitstellenden Netzwerke zu übertragen,

wobei der Breitband-Fernzugangsserver angepasst ist, um einen Befehl zu dem Zugangsknoten oder dem Zugangspunkt bereitzustellen,

10 wobei der Befehl den Zugangsknoten oder den Zugangspunkt anweist, Daten von der Benutzervorrichtung in das eine von zweiten virtuellen lokalen Netzwerken zu senden, in dem sich eine virtuelle Router-Funktionseinheit, die dem ausgewählten einen von den Dienst bereitstellenden Netzwerken zugeordnet ist, befindet, und Daten von dem einen von zweiten virtuellen lokalen Netzwerken, in dem sich eine virtuelle Router-Funktionseinheit, die dem ausgewählten einen von den Dienst bereitstellenden Netzwerken zugeordnet ist, befindet, zu der Benutzervorrichtung zu senden,

15 wodurch Daten von der Benutzervorrichtung zu dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken geroutet werden und Daten von dem ausgewählten einen von der Mehrzahl von Dienst bereitstellenden Netzwerken zu der Benutzervorrichtung geroutet werden.

20 9. Breitband-Fernzugangsserver nach Anspruch 8, wobei der Breitband-Fernzugangsserver weiter umfasst:

- eine Authentifizierungsanordnung, die einen Authentifizierungsklienten (23) und einen Authentifizierungsserver (27) aufweist,

25 wobei die lokale virtuelle Router-Funktionseinheit angeordnet ist, um, wenn Daten von einer zuvor nicht verbundenen Benutzervorrichtung empfangen werden, einen Identifizierungsvorgang mit der Benutzervorrichtung einzuleiten und eine von der Benutzervorrichtung empfangene Antwort zu der Authentifizierungsanordnung weiterzuleiten,

wobei die Authentifizierungsanordnung angeordnet ist, um, wenn eine von der Benutzervorrichtung weitergeleitete Antwort empfangen wird, Information in der Antwort mit gespeicherter Information über die Dienst bereitstellenden Netzwerke zu vergleichen, und

30 wobei die Dienstseinheit angeordnet ist, um, in dem Fall, in dem das Ergebnis des Vergleichs das ist, das die Benutzervorrichtung oder der Benutzer der Benutzervorrichtung keine Vereinbarung mit einem von den mit ihnen verbundenen Dienst bereitstellenden Netzwerken hat, die Information über die Dienst bereitstellenden Netzwerke an die Benutzervorrichtung zu übertragen.

35 10. Breitband-Fernzugangsserver nach Anspruch 9, der angepasst ist, um Nachrichten von der Benutzervorrichtung an einen Dynamic Host Configuration Protocol, DHCP, Server zu übergeben, um eine Nachricht von dem DHCP-Server zu übergeben, die der Benutzervorrichtung eine Adresse zuordnet, um die zugeordnete Adresse zu verwenden, um die Benutzervorrichtung mit der Dienstseinheit zu verbinden, und um die zugeordnete Adresse zu verwenden, um die Information über die Dienst bereitstellenden Netzwerke von der Dienstseinheit zu der Benutzervorrichtung zu übertragen.

40 11. Breitband-Fernzugangsserver nach Anspruch 10, der angeordnet ist, um nach dem Empfangen, von der Benutzervorrichtung, von Informationen über ein ausgewähltes der Dienst bereitstellenden Netzwerke, die Adresse zu löschen und einen Authentifizierungsvorgang mit der Benutzervorrichtung zu starten.

Revendications

50 1. Noeud d'accès (13) conçu pour être connecté à un réseau de type Ethernet entre un point d'accès (1) de dispositifs utilisateur (15, 15') et un serveur d'accès distant à large bande (17) pour fournir un accès à large bande à une pluralité de réseaux fournissant des services (3.1, 3.2), le noeud d'accès incluant

- une unité de traitement pour traiter des réseaux locaux virtuels, l'unité de traitement incluant une mémoire,

55 le noeud d'accès étant caractérisé en ce que

- le noeud d'accès a une première fonction de réseau local virtuel pour mettre en oeuvre un premier réseau

local virtuel (43) incluant le noeud d'accès et une unité faisant fonction de routeur virtuel local (49) du serveur d'accès distant à large bande,

- pour chacun de ladite pluralité de réseaux fournissant des services, le noeud d'accès a une seconde fonction de réseau local virtuel, chaque seconde fonction de réseau local virtuel servant à mettre en oeuvre un second réseau local virtuel respectif (41.1, 41.2) incluant le noeud d'accès et une unité respective d'unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2) du serveur d'accès distant à large bande, l'unité respective des unités faisant fonction de routeurs virtuels dédiés servant à la communication avec le réseau respectif de ladite pluralité de réseaux fournissant des services, l'unité faisant fonction de routeur virtuel dédié respective étant conçue pour transférer directement des trames Ethernet en provenance et vers un serveur d'accès à large bande (19) du réseau respectif des réseaux fournissant des services,

- la mémoire stocke des identifications de trames Ethernet transmises dans

-- le premier réseau local virtuel, et
-- les seconds réseaux locaux virtuels,

et

- le noeud d'accès comprend une unité de commande connectée à l'unité de traitement,

l'unité de commande servant à

-- commander l'unité de traitement pour transmettre des trames depuis un nouveau dispositif utilisateur qui s'est connecté au point d'accès dans le premier réseau local virtuel,
-- recevoir des informations à partir du serveur d'accès distant à large bande en ce qui concerne l'acheminement de trames,

et

-- commander l'unité de traitement pour transmettre des trames depuis un dispositif utilisateur qui est connecté au point d'accès dans un des seconds réseaux locaux virtuels comme donné par des informations reçues en provenance du serveur d'accès distant à large bande, au lieu du premier réseau local virtuel, les trames étant de ce fait transmises au serveur d'accès à large bande du réseau respectif fournissant des services.

2. Noeud d'accès selon la revendication 1, dans lequel l'unité de commande est conçue pour recevoir des informations incluant une adresse de Commande d'Accès au Support, MAC, du dispositif utilisateur connecté au point d'accès et pour commander l'unité de traitement afin de transmettre des trames en provenance de cette adresse jusque dans ledit réseau des seconds réseaux locaux virtuels.

3. Noeud d'accès selon la revendication 2, dans lequel l'adresse MAC est une adresse MAC Virtuelle et le noeud d'accès inclut une unité de translation pour faire subir une translation à l'adresse MAC virtuelle en une adresse MAC du dispositif utilisateur.

4. Procédé pour connecter un dispositif utilisateur (15, 15') à un réseau d'une pluralité de réseaux fournissant des services (3.1, 3.2) par l'intermédiaire d'un réseau d'accès à large bande (29), le procédé incluant les étapes suivantes :

- le dispositif utilisateur est connecté au réseau d'accès à large bande,
- un noeud d'accès (13) reçoit une trame ou des trames envoyées depuis le dispositif utilisateur et fait suivre la trame ou les trames jusque dans un premier réseau local virtuel (43),
- une unité faisant fonction de routeur virtuel local (49) reçoit la trame ou les trames reçues dans le premier réseau local virtuel,

le procédé étant caractérisé en ce que le procédé comprend en outre les étapes suivantes :

- l'unité faisant fonction de routeur virtuel local démarre une procédure d'identification et d'authentification pour le dispositif utilisateur,
- le dispositif utilisateur envoie dans la procédure d'identification et d'authentification des informations de sélection indiquant un réseau de la pluralité de réseaux fournissant des services,
- après une procédure d'identification et d'authentification couronnée de succès, le noeud d'accès reçoit une instruction en provenance d'un serveur d'accès distant à large bande (17) pour associer une adresse du dispositif utilisateur à l'un de seconds réseaux locaux virtuels (41.1, 41.2), chacun desdits réseaux locaux virtuels incluant

le noeud d'accès et l'une desdites unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2) du serveur d'accès distant à large bande, ladite unité des unités faisant fonction de routeurs virtuels dédiés correspondant aux informations de sélection, et sur la base desdites instructions, fait suivre les trames reçues en provenance du dispositif utilisateur jusqu'à dans ledit réseau de seconds réseaux locaux virtuels au lieu du premier réseau local virtuel, chacune desdites unités faisant fonction de routeurs virtuels étant conçue pour directement transférer des trames Ethernet en provenance et vers un serveur d'accès à large bande (19) d'un réseau respectif des réseaux fournissant des services (3.1, 3.2), et

- le serveur d'accès distant à large bande fait suivre des trames provenant du dispositif utilisateur reçues dans ledit réseau de seconds réseaux locaux virtuels dans ledit réseau respectif de la pluralité de réseaux fournissant des services.

5. Procédé selon la revendication 4, dans lequel dans l'étape du dispositif utilisateur se connectant au réseau d'accès à large bande, il se connecte au point d'accès du réseau d'accès à large bande.

6. Procédé selon la revendication 4, dans lequel, dans l'étape de réception de la trame ou des trames dans le premier réseau local virtuel, la trame ou les trames sont reçues par l'unité faisant fonction de routeur virtuel local démarant la procédure d'identification et d'authentification.

7. Procédé selon la revendication 4, dans lequel, dans la procédure d'identification et d'authentification, le dispositif utilisateur démarre en envoyant des informations d'identification incluant lesdites informations de sélection d'un réseau de la pluralité de réseaux fournissant des services.

8. Serveur d'accès distant à large bande (17) pour fournir, pour des dispositifs utilisateur (15, 15') connectés au serveur d'accès distant à large bande par l'intermédiaire d'un noeud d'accès (13) ou point d'accès (7), un accès à large bande à une pluralité de réseaux fournissant des services (3.1, 3.2) différents de réseaux fournissant des services domestiques d'utilisateurs des dispositifs utilisateur, le serveur d'accès distant à large bande incluant :

- une unité de service pour stocker et fournir des informations concernant ladite pluralité de réseaux fournissant des services.

le serveur d'accès distant à large bande étant

caractérisé en ce que le serveur d'accès distant à large bande est conçu pour :

- connecter un dispositif utilisateur à l'unité de service, l'unité de service étant conçue pour envoyer au dispositif utilisateur des informations concernant ladite pluralité de réseaux fournissant des services.

- recevoir en provenance d'un dispositif utilisateur des informations concernant un réseau sélectionné de ladite pluralité de réseaux fournissant des services.

- après cela faire suivre des informations concernant un réseau sélectionné de ladite pluralité de réseaux fournissant des services, lorsque reçues en provenance du dispositif utilisateur, audit réseau sélectionné des réseaux fournissant des services.

- après cela faire passer des informations d'authentification entre ledit réseau sélectionné de ladite pluralité de réseaux fournissant des services et le dispositif utilisateur.

- après cela recevoir des informations, concernant le succès ou l'absence de succès de la procédure d'authentification, et

- finalement, en utilisant les informations reçues, lorsqu'elles indiquent un succès, acheminer des données, en provenance du dispositif d'utilisateur vers ledit réseau sélectionné de la pluralité de réseaux fournissant des services et acheminer des données en provenance dudit réseau sélectionné de la pluralité de réseaux fournissant des services au dispositif utilisateur.

dans lequel le serveur d'accès distant à large bande inclut

- une unité faisant fonction de routeur virtuel local (49).

dans lequel le serveur d'accès distant à large bande est conçu pour inclure l'unité faisant fonction de routeur virtuel local dans un premier réseau local virtuel (43) incluant également le noeud d'accès ou le point d'accès, et

- des unités faisant fonction de routeurs virtuels dédiés (47.1, 47.2), dans lesquelles chaque unité faisant fonction de routeur virtuel dédié est conçue pour communiquer avec un réseau correspondant d'une pluralité de seconds

réseaux locaux virtuels (41.1, 41.2), chacun desdits seconds réseaux locaux virtuels incluant ledit noeud d'accès ou point d'accès,

chacune desdites unités faisant fonction de routeurs virtuels dédiés étant conçue pour transférer directement des données, en provenance du réseau respectif des réseaux fournissant des services audit noeud d'accès ou point d'accès, et en provenance dudit noeud d'accès ou point d'accès au réseau respectif des réseaux fournissant des services,

le serveur d'accès distant à large bande étant conçu pour fournir une commande audit noeud d'accès ou point d'accès, ladite commande ordonnant au noeud d'accès ou point d'accès d'envoyer des données en provenance du dispositif utilisateur dans ce réseau de seconds réseaux locaux virtuels dans lequel il y a une unité faisant fonction de routeur virtuel associée au réseau sélectionné des réseaux fournissant des services, et d'envoyer au dispositif utilisateur des données en provenance du réseau de seconds réseaux locaux virtuels dans lequel il y a une unité faisant fonction de routeur virtuel associée au réseau sélectionné des réseaux fournissant des services, acheminant de ce fait des données en provenance du dispositif utilisateur vers ledit réseau sélectionné de la pluralité de réseaux fournissant des services et en acheminant des données en provenance dudit réseau sélectionné de la pluralité de réseaux fournissant des services au dispositif utilisateur.

9. Serveur d'accès distant à large bande selon la revendication 8, dans lequel le serveur d'accès distant à large bande inclut en outre :

un agencement d'authentification incluant un client d'authentification (23) et un serveur d'authentification (27),

dans lequel l'unité faisant fonction de routeur virtuel local est agencée, lors de la réception des données en provenance d'un dispositif utilisateur précédemment non connecté, pour amorcer une procédure d'identification avec le dispositif d'utilisateur et pour faire suivre une réponse reçue en provenance du dispositif utilisateur vers l'agencement d'authentification,

dans lequel l'agencement d'authentification est agencé pour comparer, lors de la réception d'une réponse réexpédiée en provenance du dispositif utilisateur, des informations dans la réponse à des informations stockées concernant lesdits réseaux fournissant des services, et

dans lequel l'unité de service est agencée, dans un cas où le résultat de la comparaison est que le dispositif utilisateur ou l'utilisateur du dispositif utilisateur n'a aucun accord avec l'un quelconque des réseaux fournissant des services pour se connecter à eux, pour transférer lesdites informations concernant lesdits réseaux fournissant des services au dispositif utilisateur.

10. Serveur d'accès distant à large bande selon la revendication 9, conçu pour passer à un serveur de protocole de configuration d'hôte dynamique, DHCP, des messages en provenance du dispositif utilisateur, pour passer un message en provenance du serveur DHCP attribuant une adresse au dispositif utilisateur, en utilisant l'adresse attribuée, pour connecter le dispositif utilisateur à l'unité de service, et en utilisant l'adresse attribuée, pour transférer depuis l'unité de service au dispositif utilisateur lesdites informations concernant lesdits réseaux fournissant des services.

11. Serveur d'accès distant à large bande selon la revendication 10, agencé, après réception en provenance du dispositif d'utilisateur d'informations concernant un réseau sélectionné des réseaux fournissant des services, pour annuler ladite adresse et amorcer une procédure d'authentification avec le dispositif utilisateur.

Fig. 1a

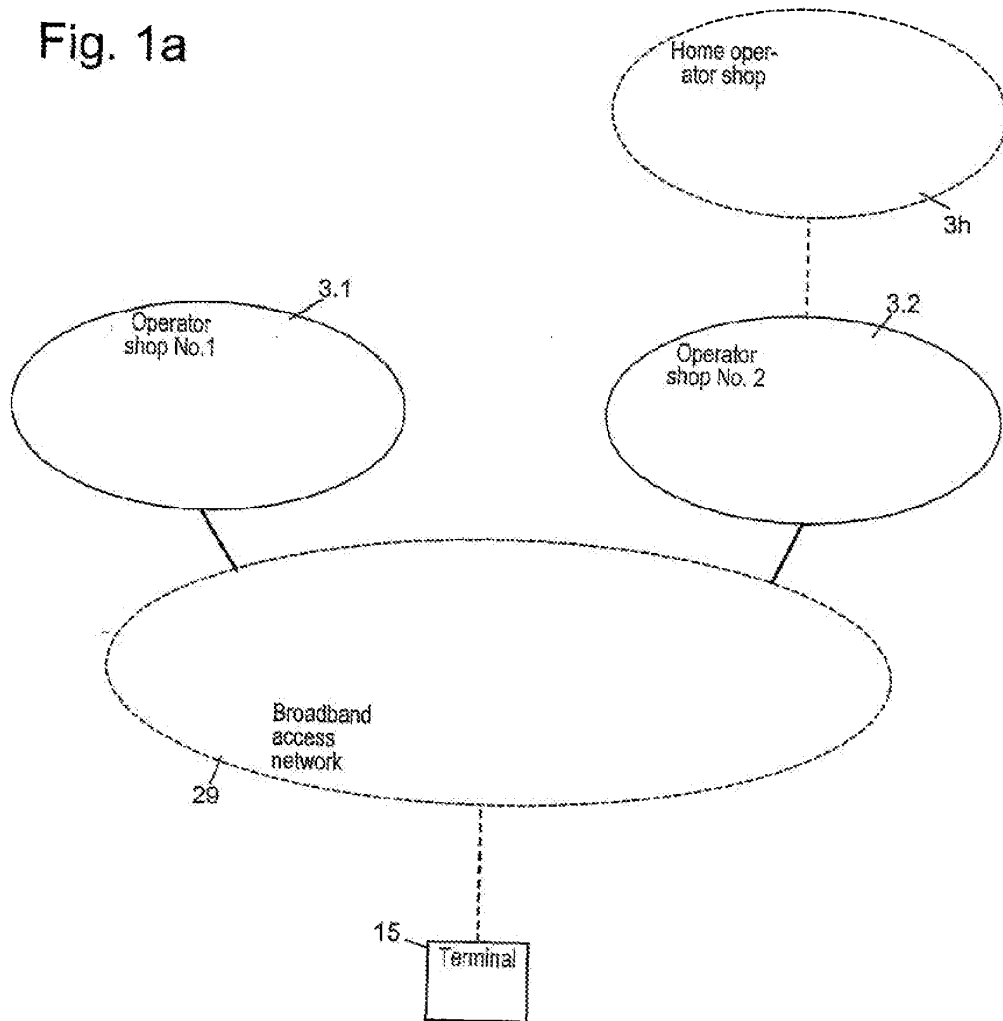


Fig. 1b

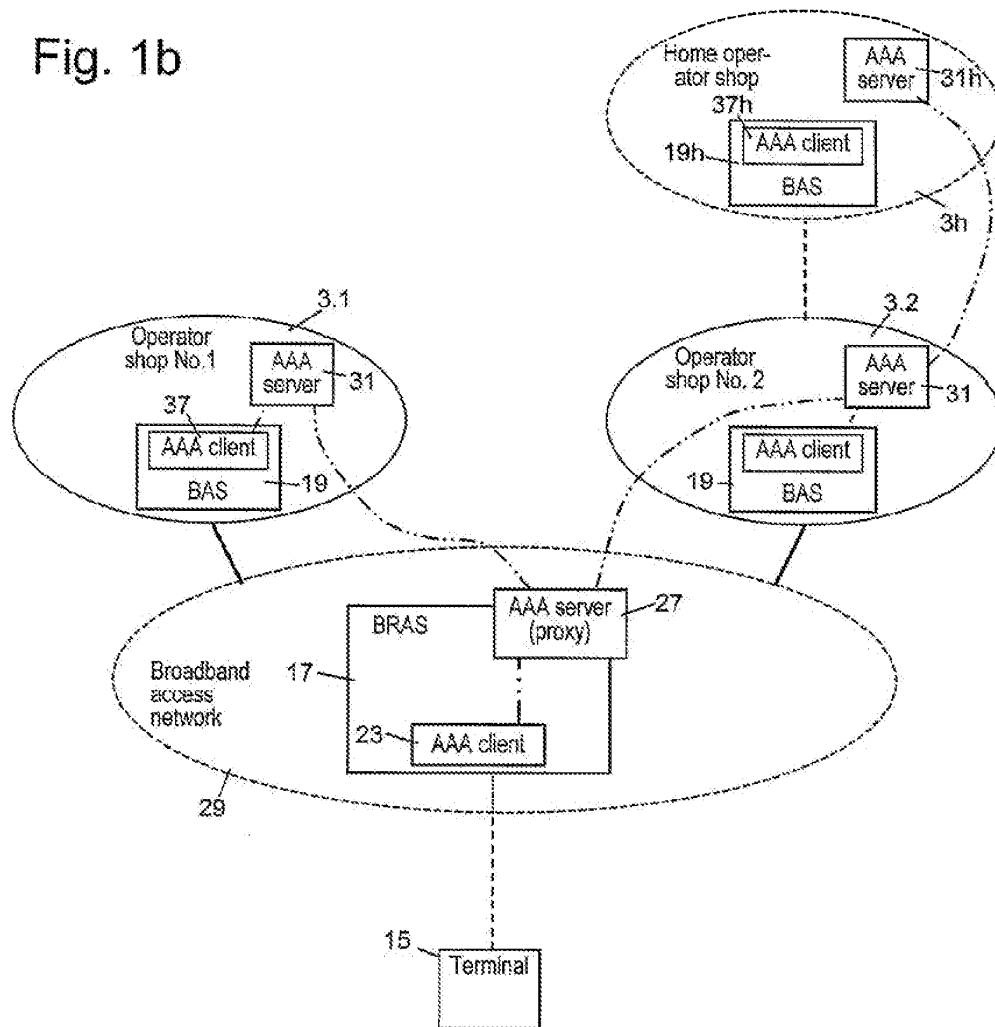


Fig. 1c

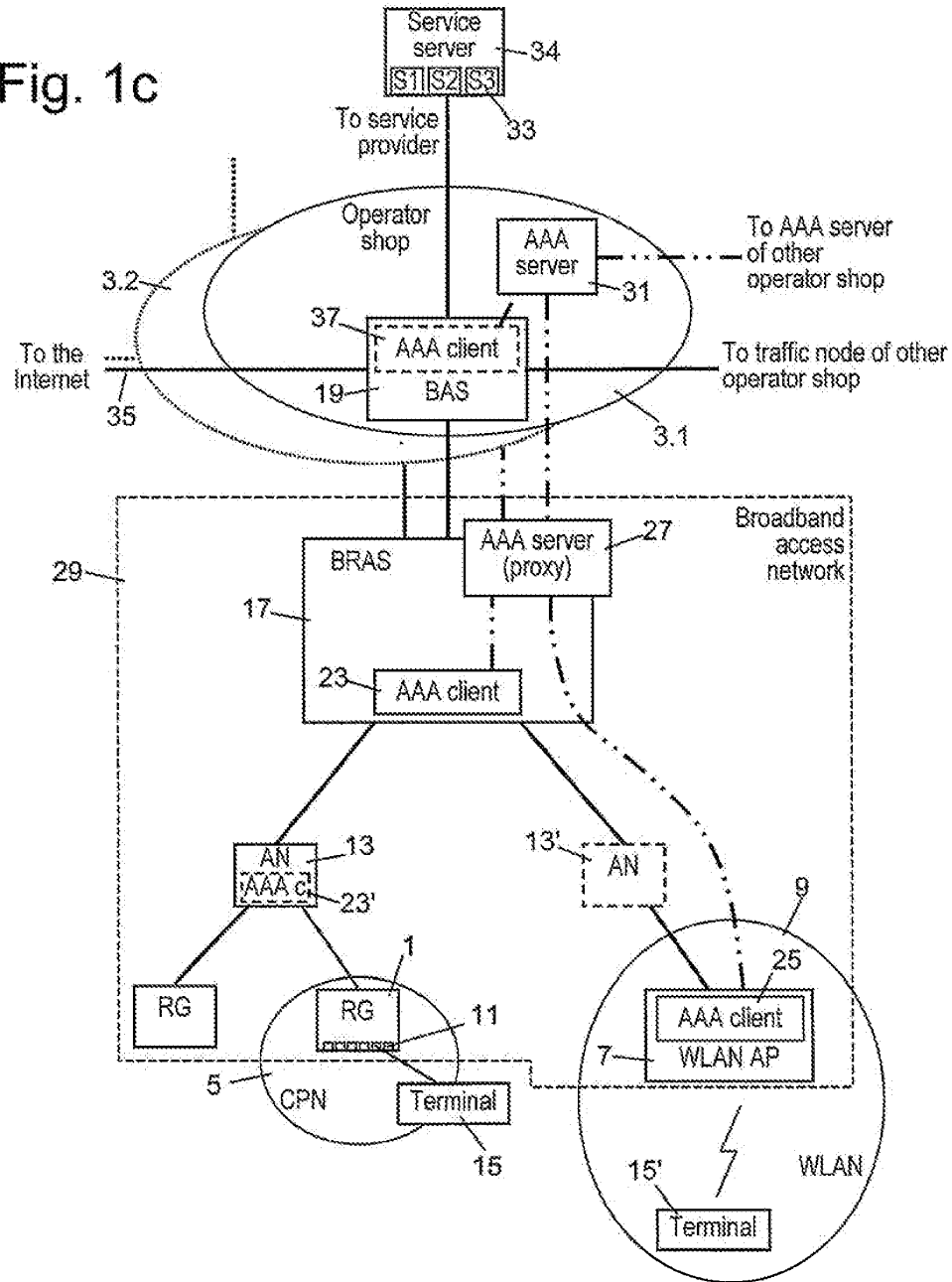
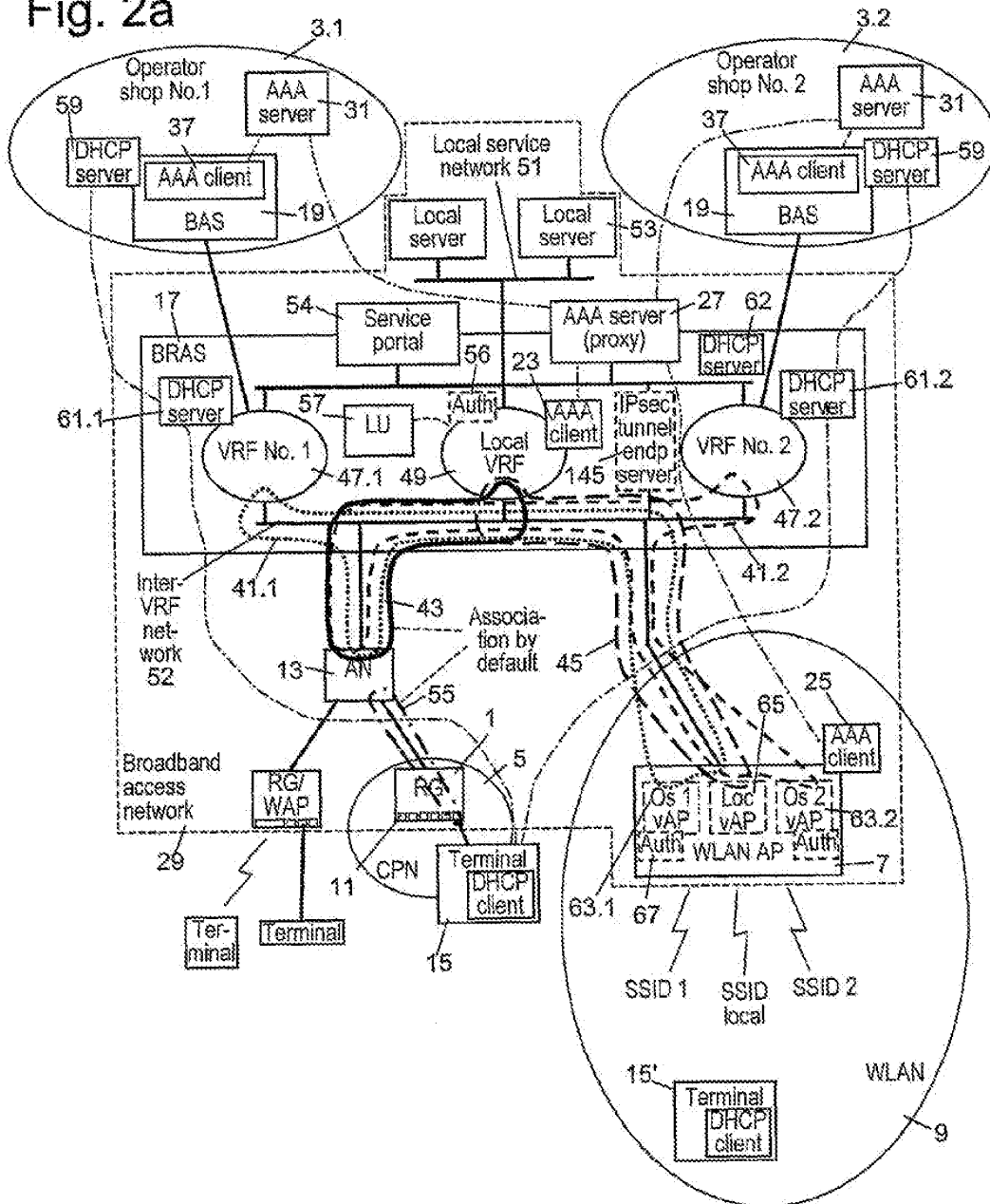
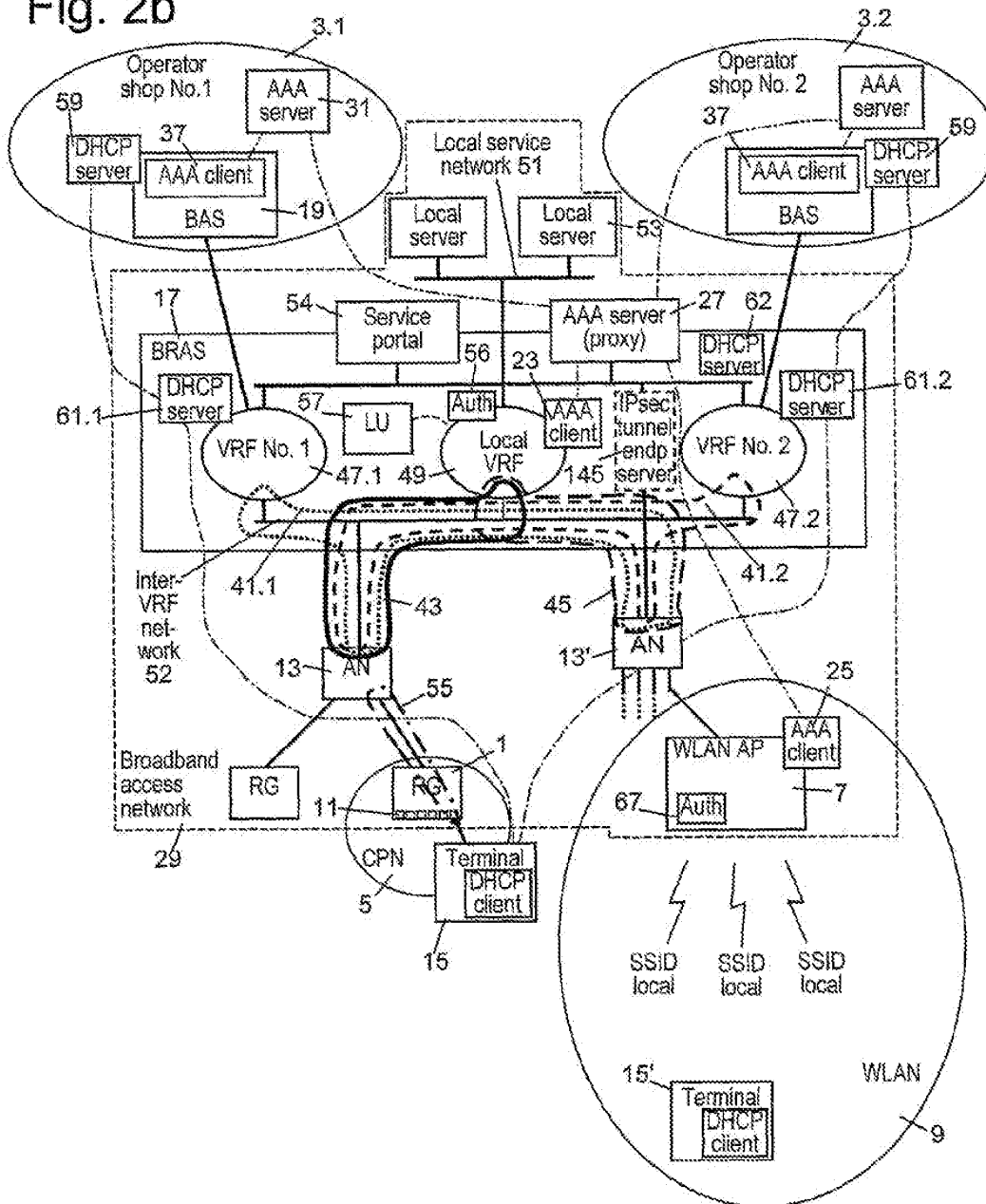


Fig. 2a



- VLAN No. 1 41.1
- VLAN No. 2 41.2
- Local default VLAN 43
- RG port VLAN 55
- Local WLAN AP VLAN 45

Fig. 2b



- VLAN No. 1 41.1
- VLAN No. 2 41.2
- Local default VLAN 43
- - - - RG port VLAN 55
- - - - Local WLAN AP VLAN 45

Fig. 2c

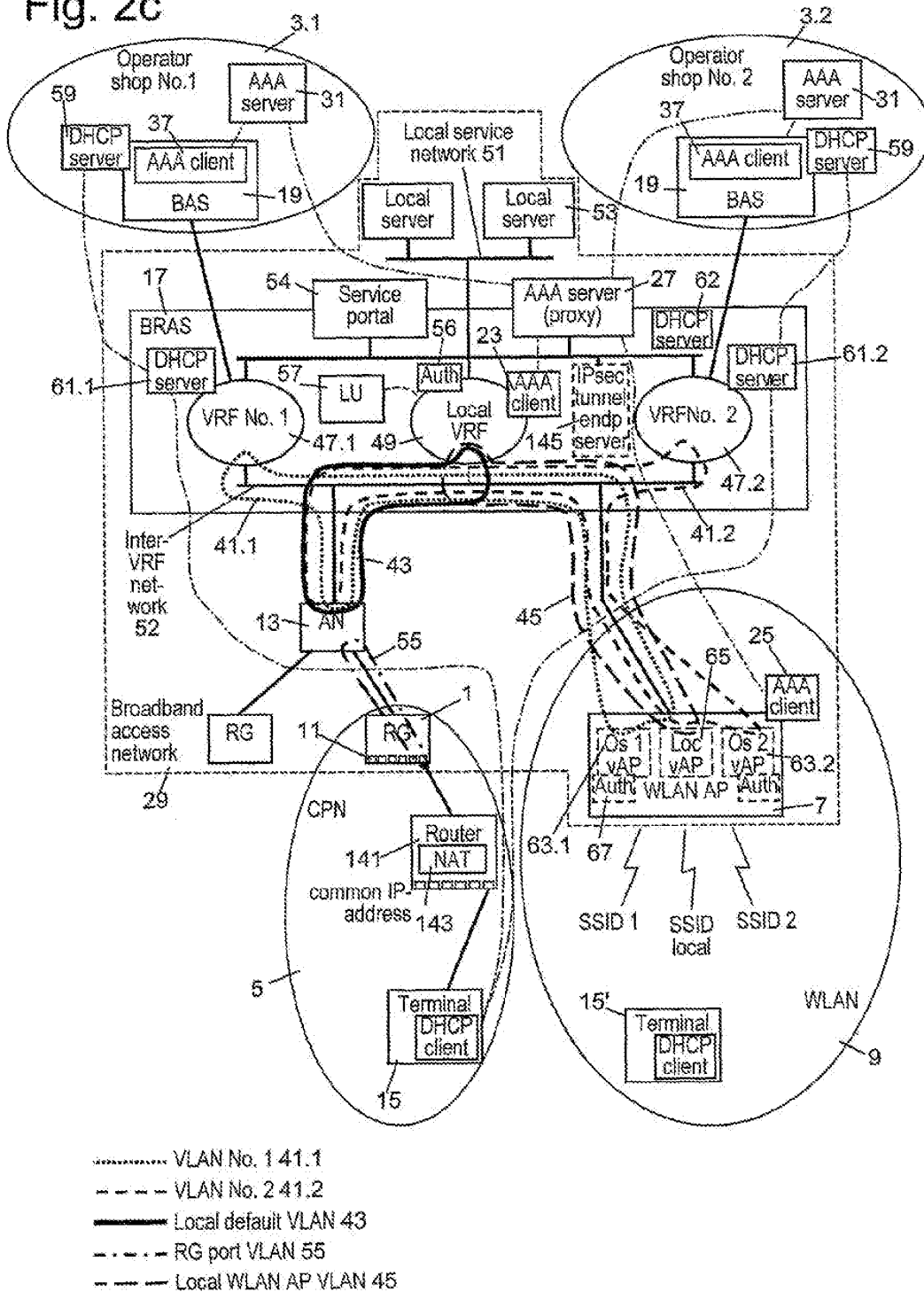


Fig. 2d

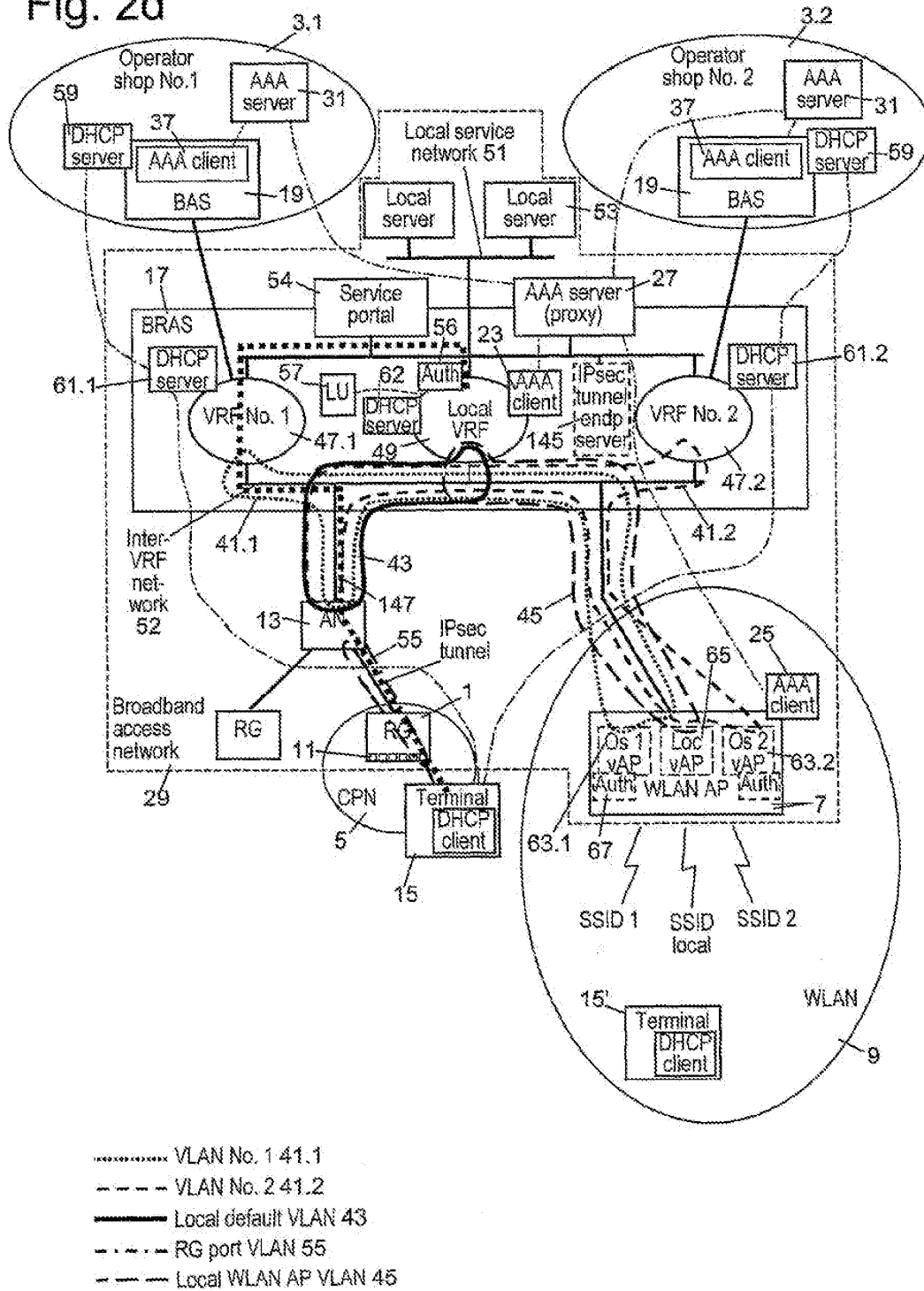
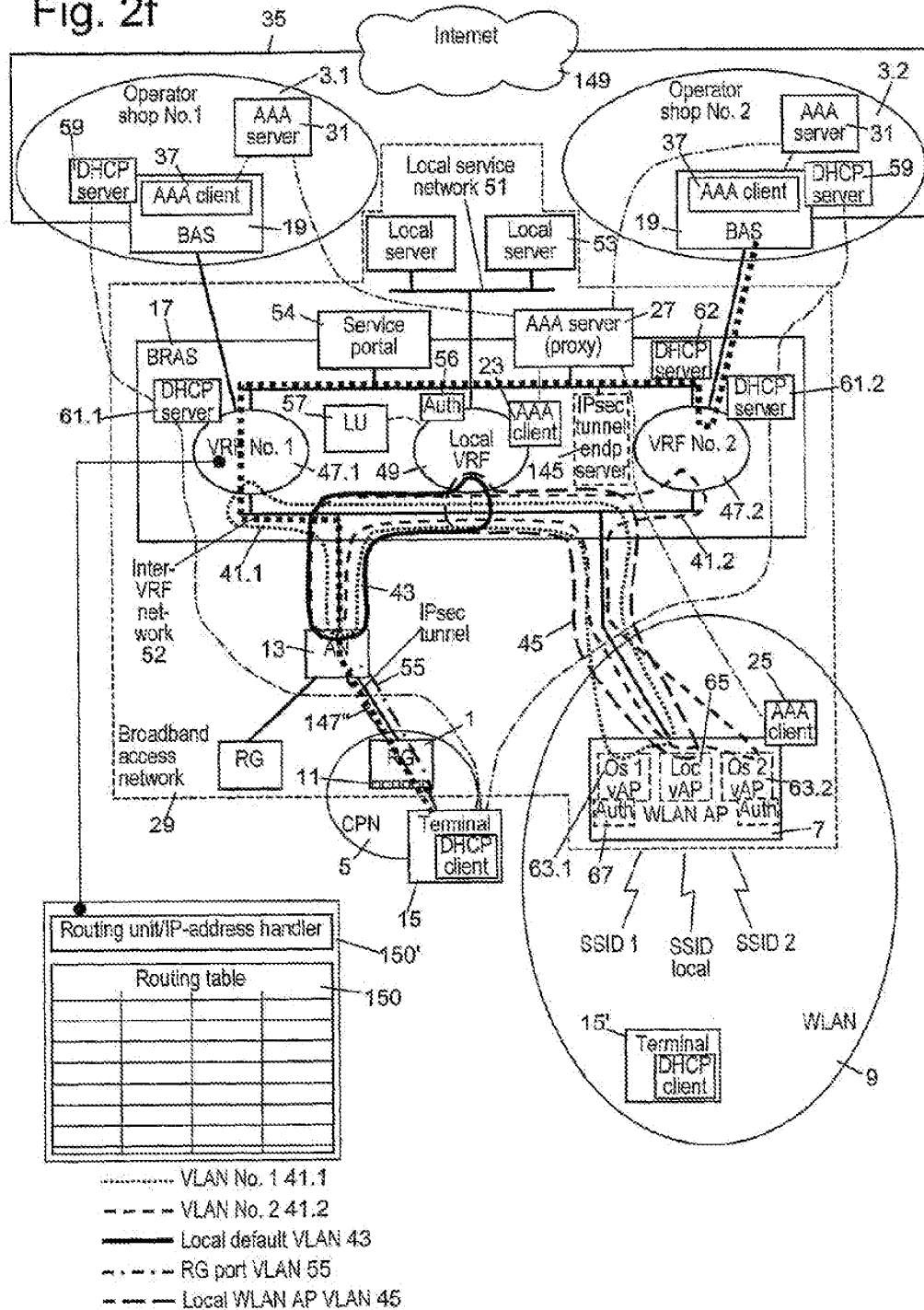


Fig. 2e



Fig. 2f



```

..... VLAN No. 1 41.1
- - - - VLAN No. 2 41.2
===== Local default VLAN 43
- . . . . RG port VLAN 55
- - - - Local WLAN AP VLAN 45

```

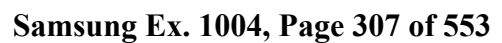


Fig. 2h

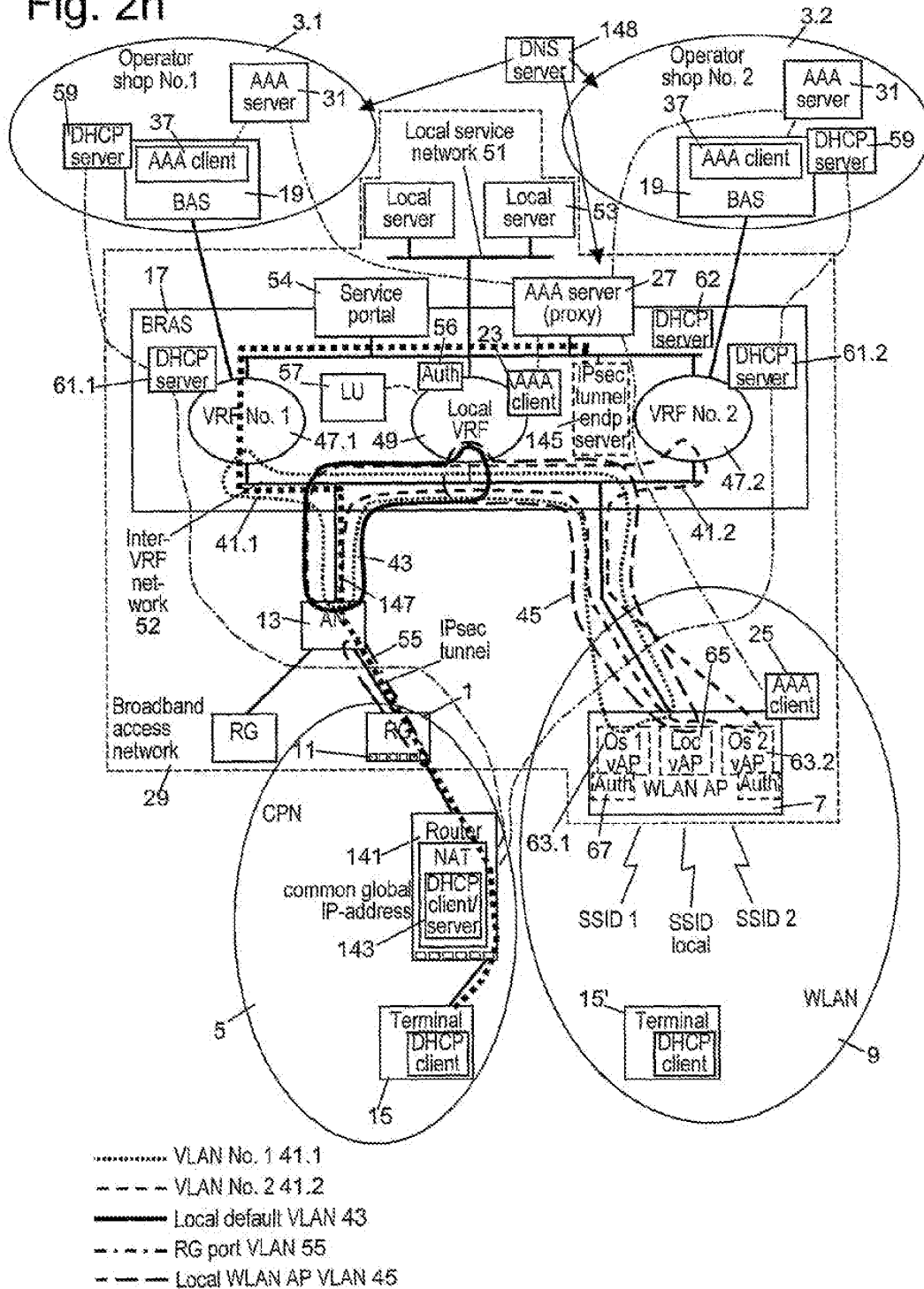


Fig. 2j

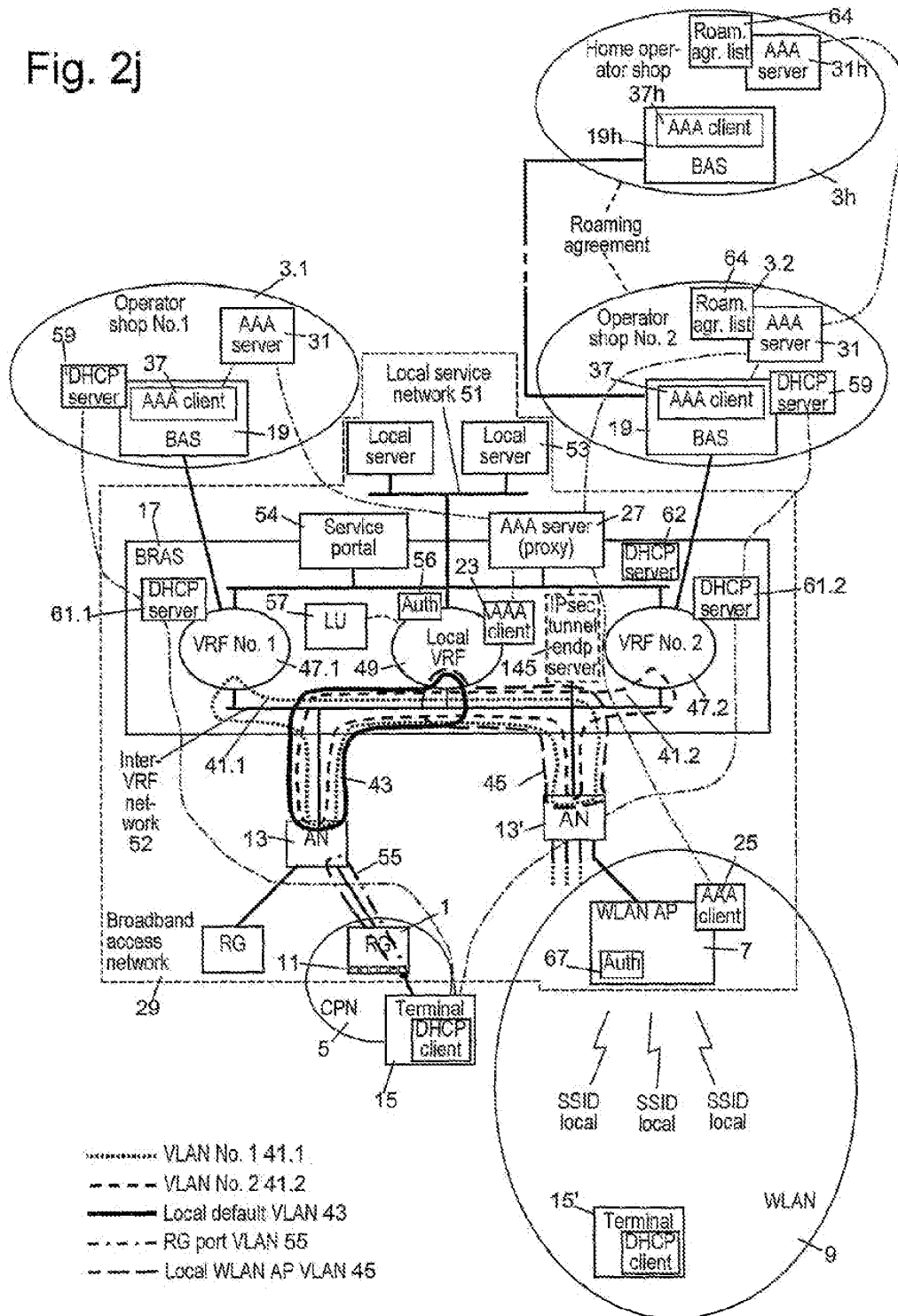
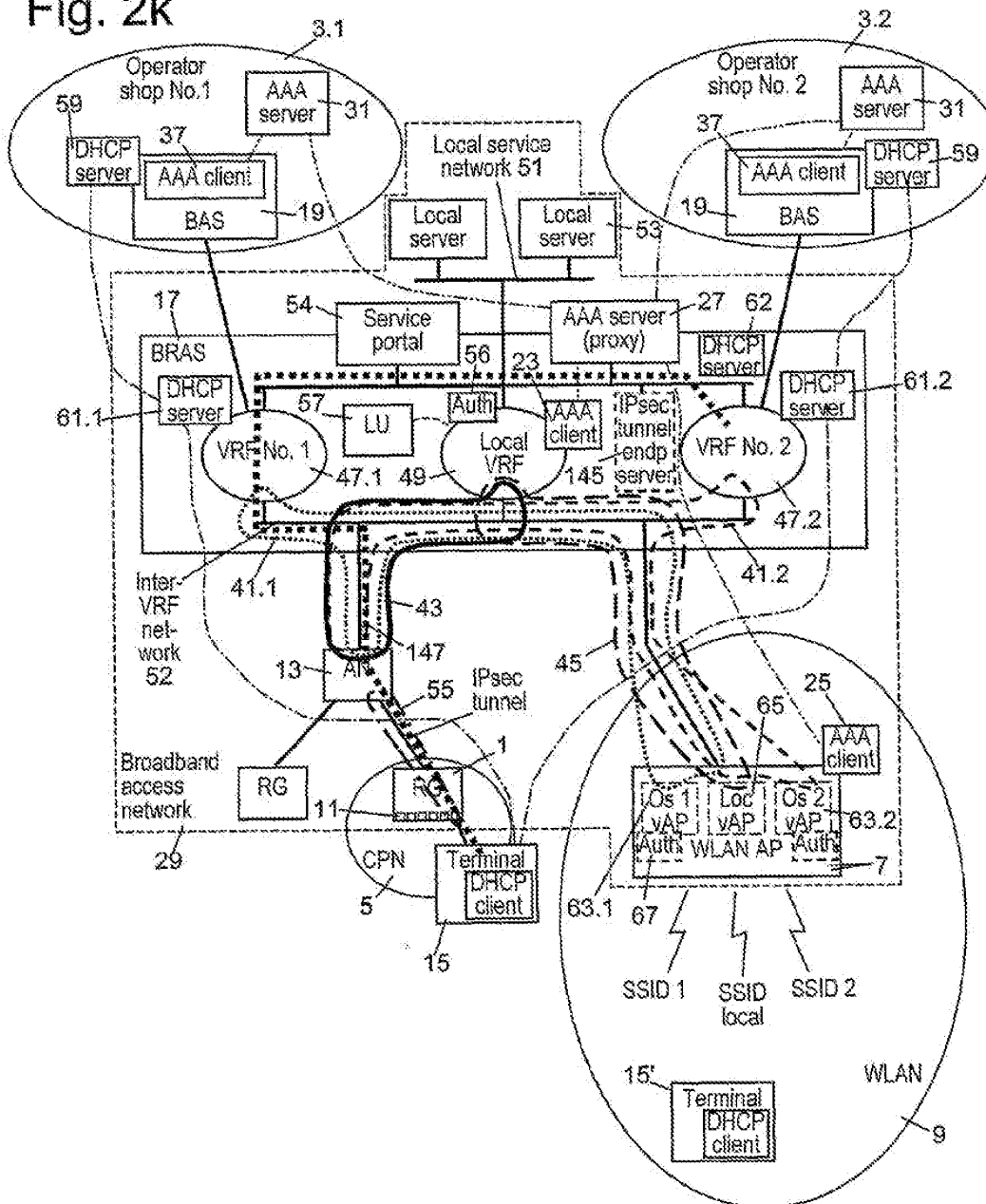


Fig. 2k



..... VLAN No. 1 41.1
 - - - - - VLAN No. 2 41.2
 ——— Local default VLAN 43
 - RG port VLAN 55
 - - - - - Local WLAN AP VLAN 45

Fig. 3a

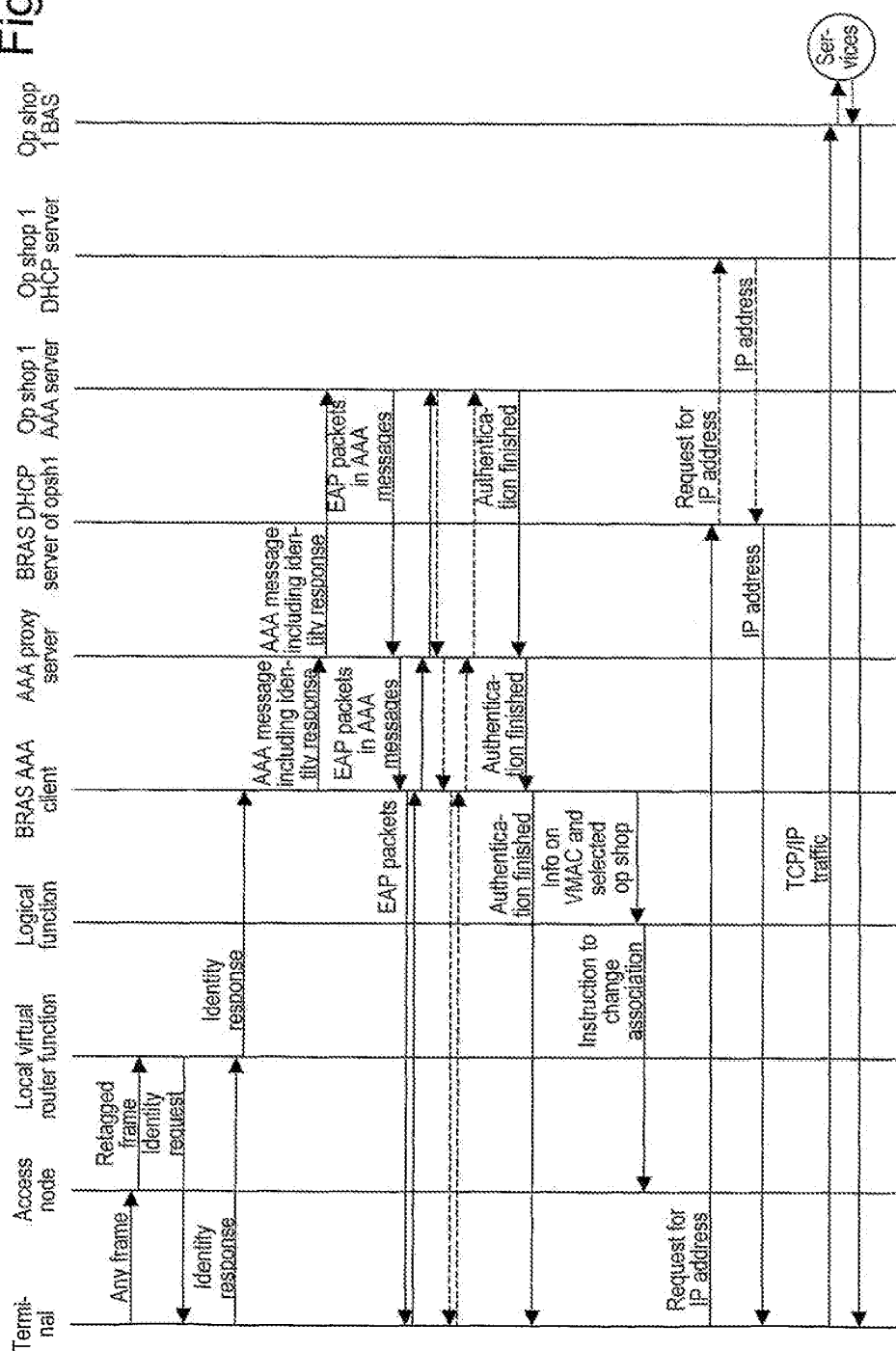


Fig. 3b

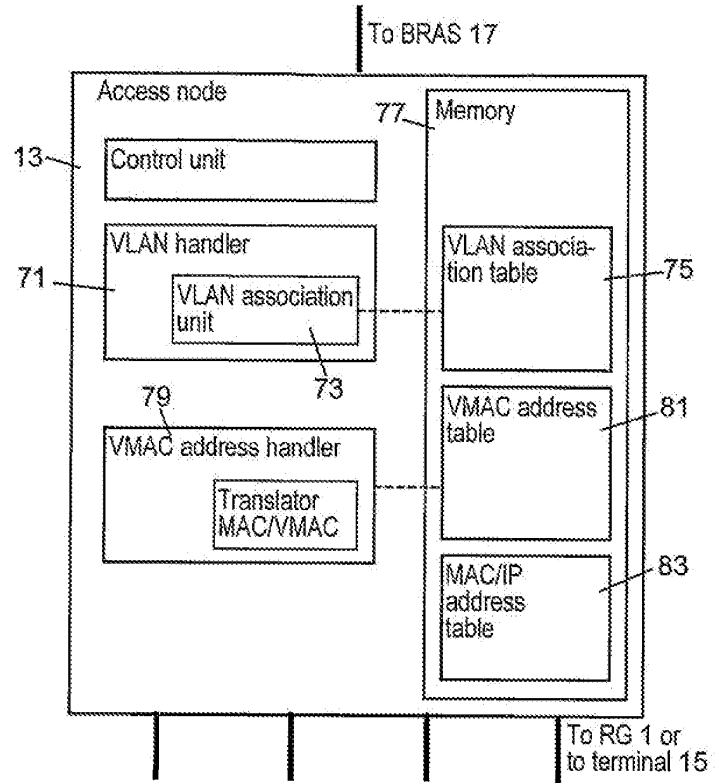


Fig. 6b

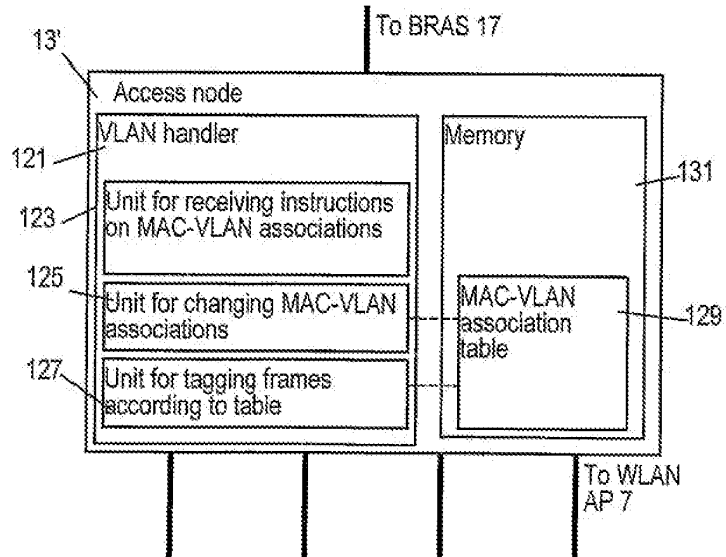


Fig. 4a

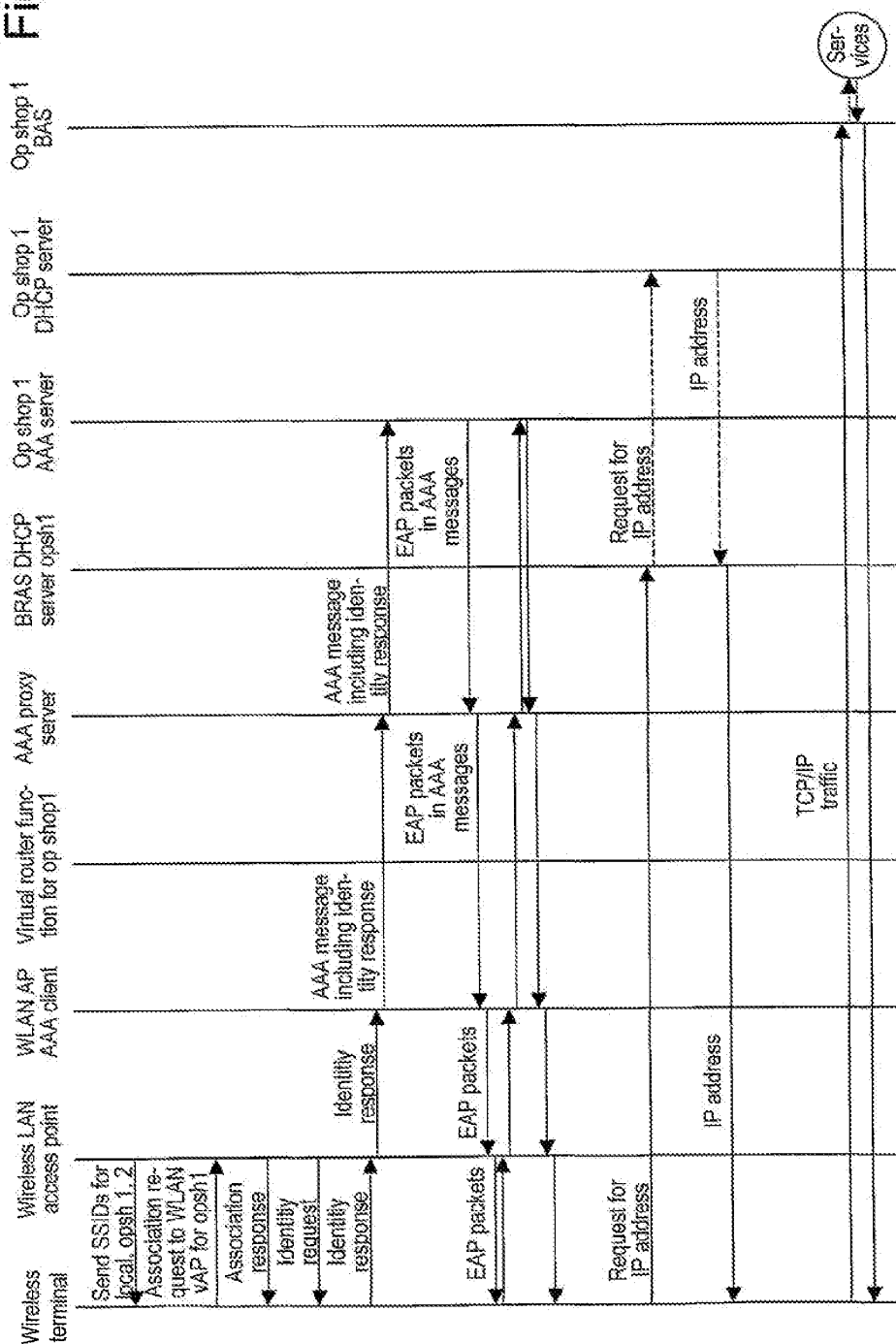


Fig. 4b

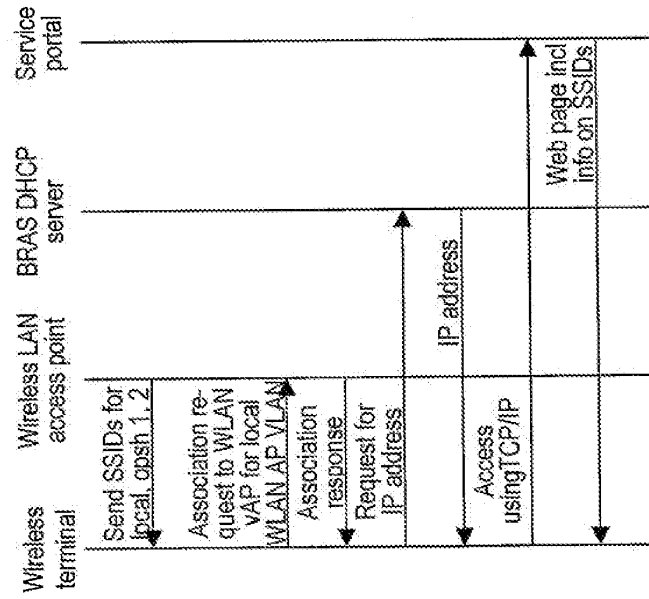


Fig. 4c

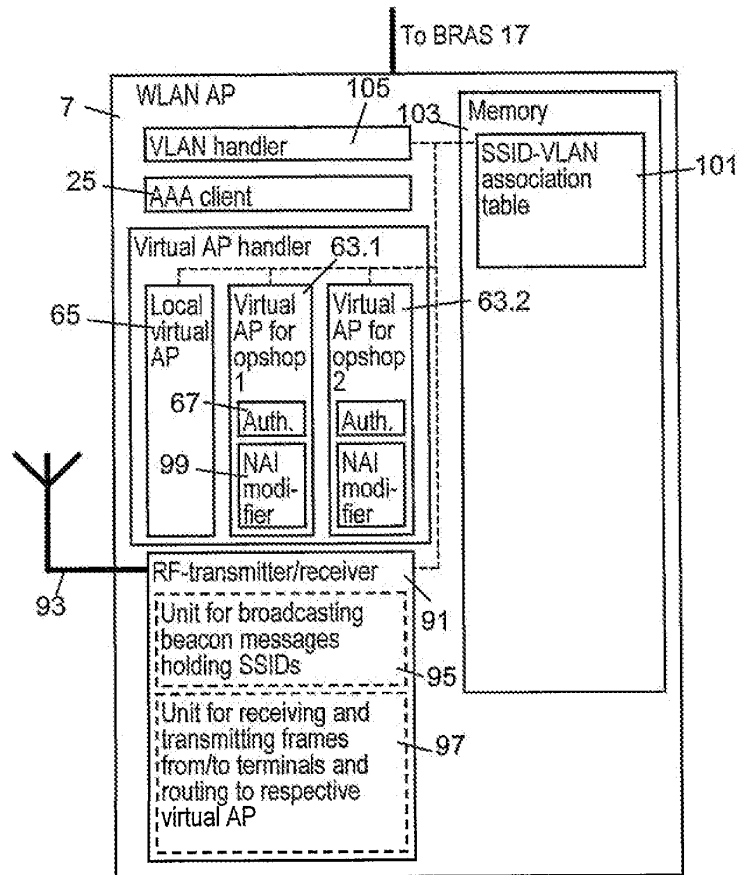


Fig. 4d Fig. 4e

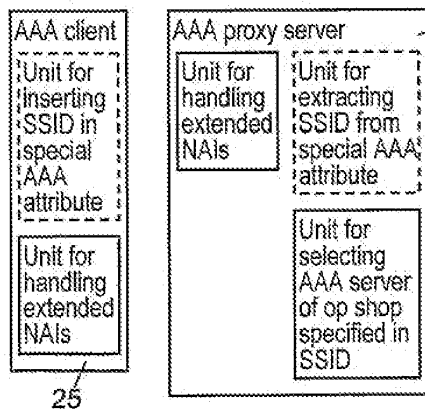


Fig. 4f

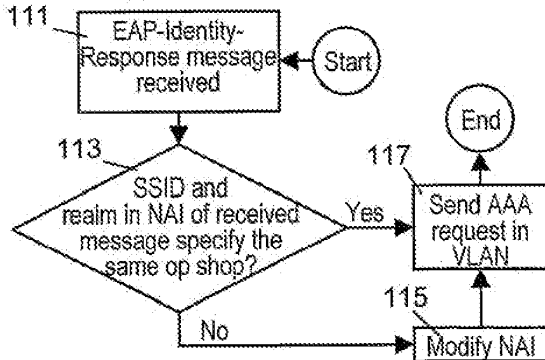


Fig. 5

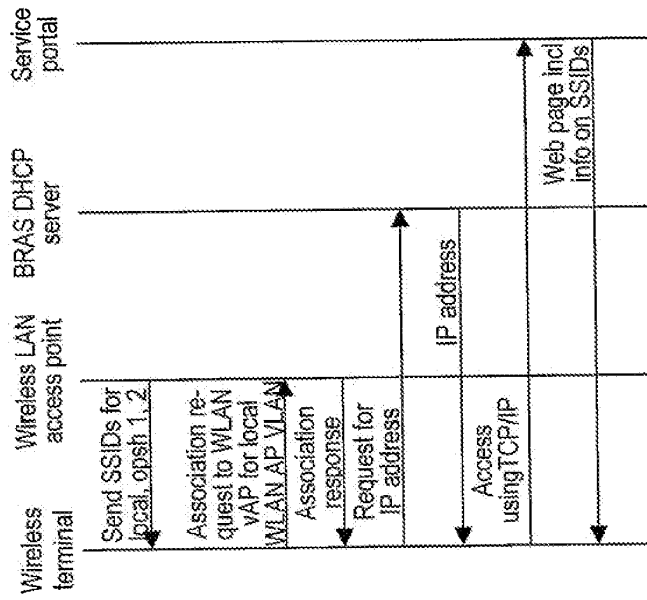


Fig. 6a

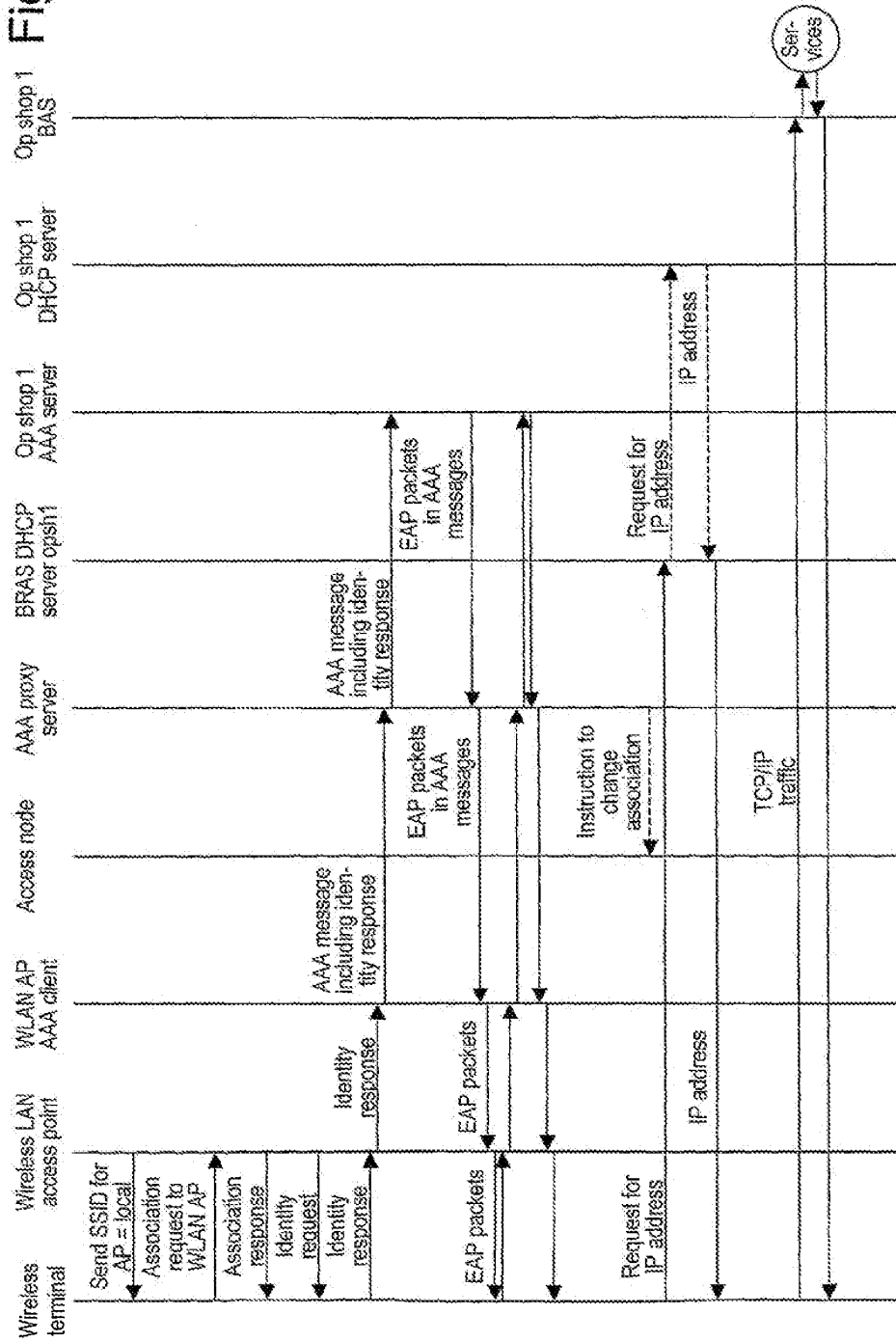


Fig. 7a

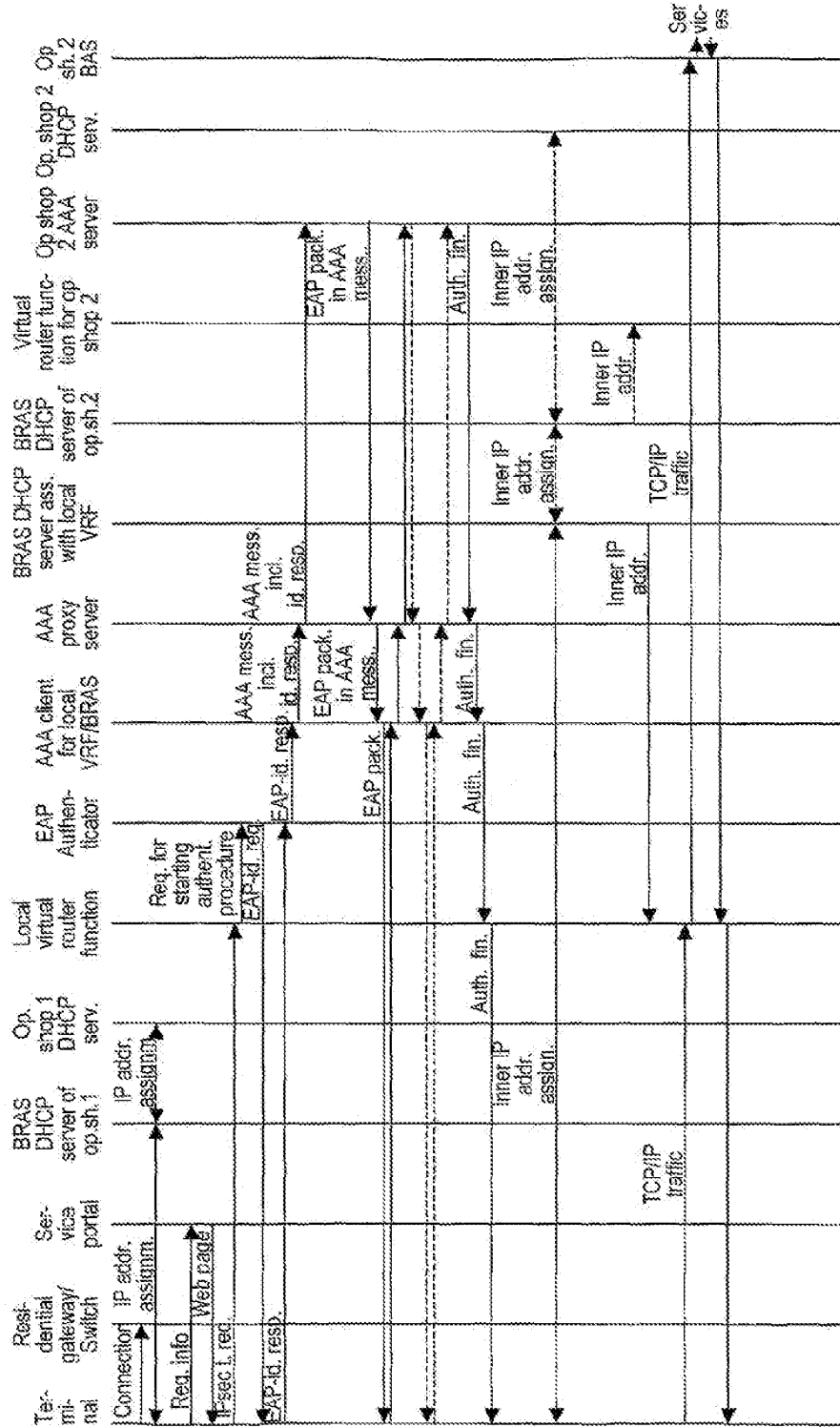
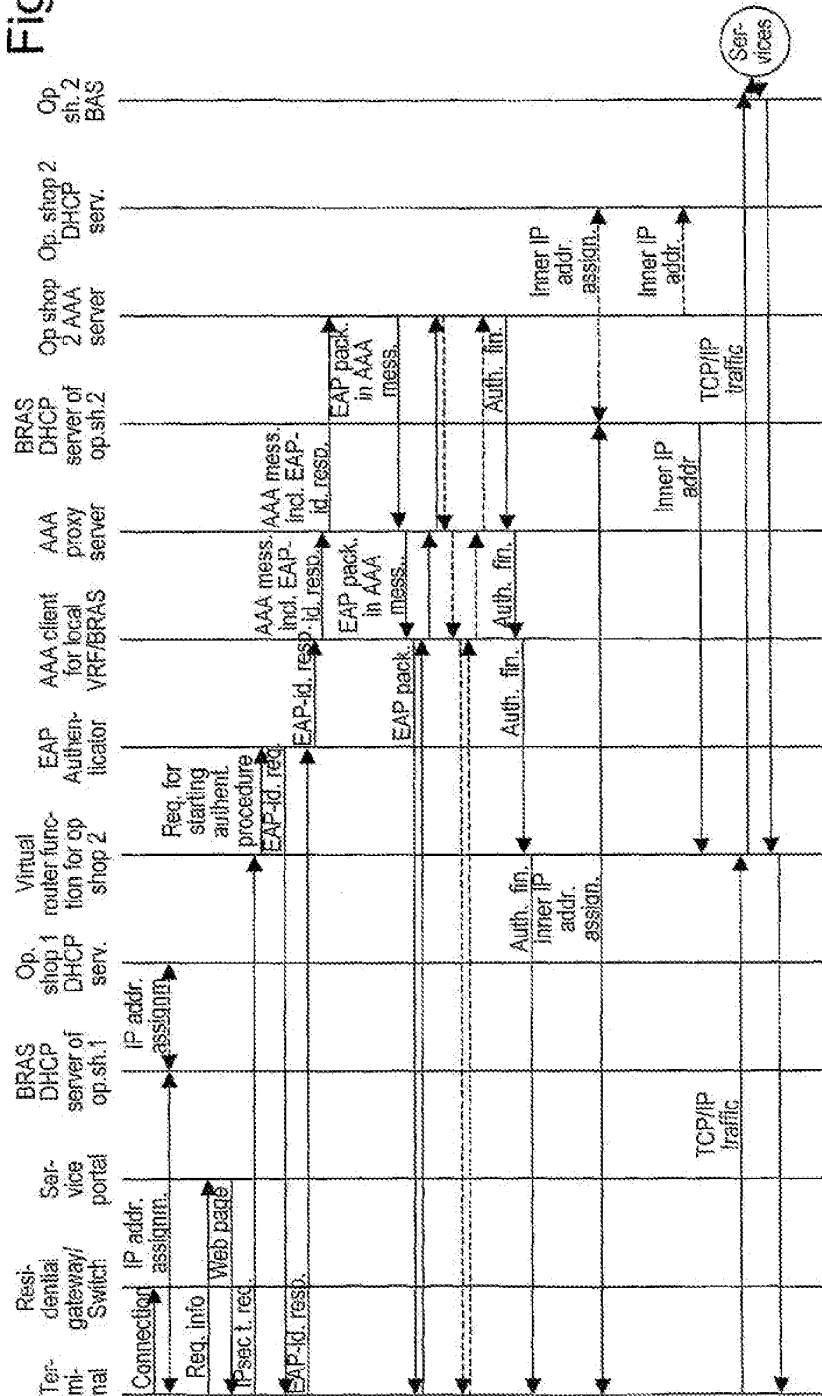


Fig. 7b



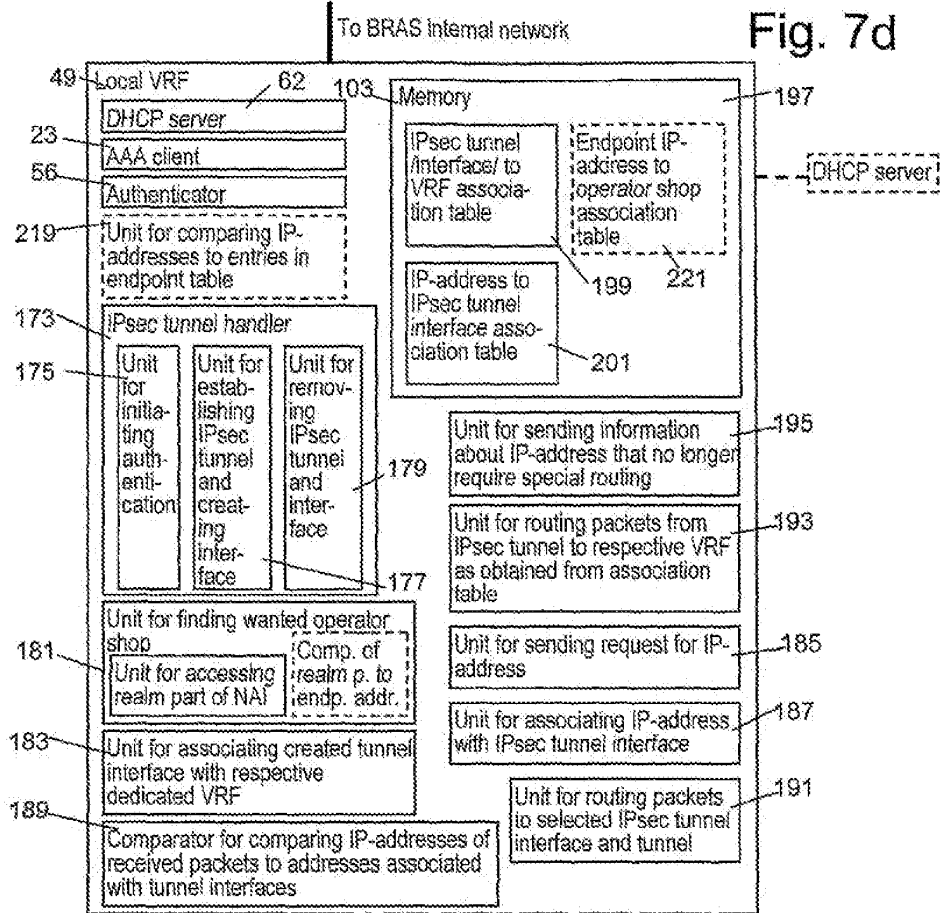


Fig. 7c

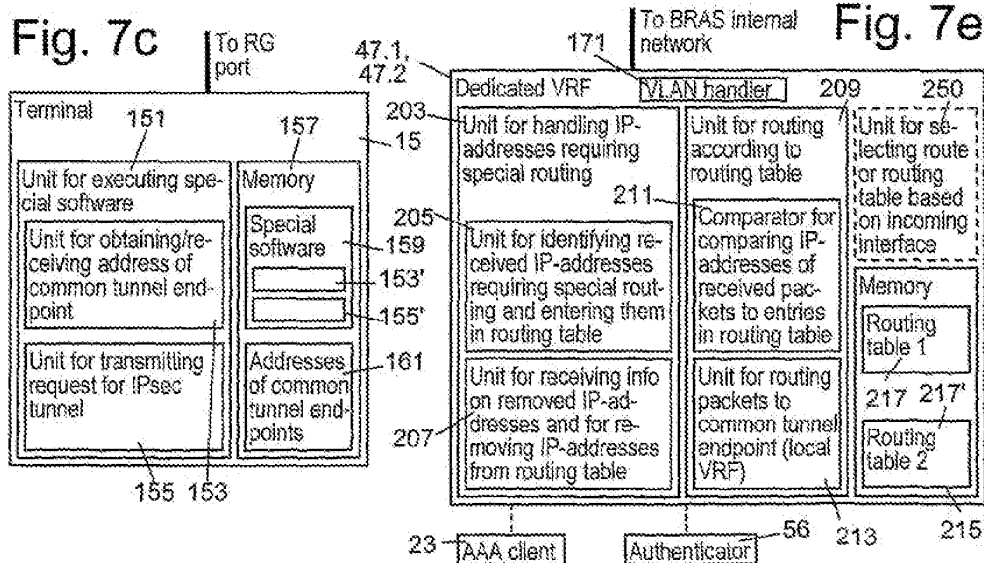


Fig. 7e

Fig. 7f

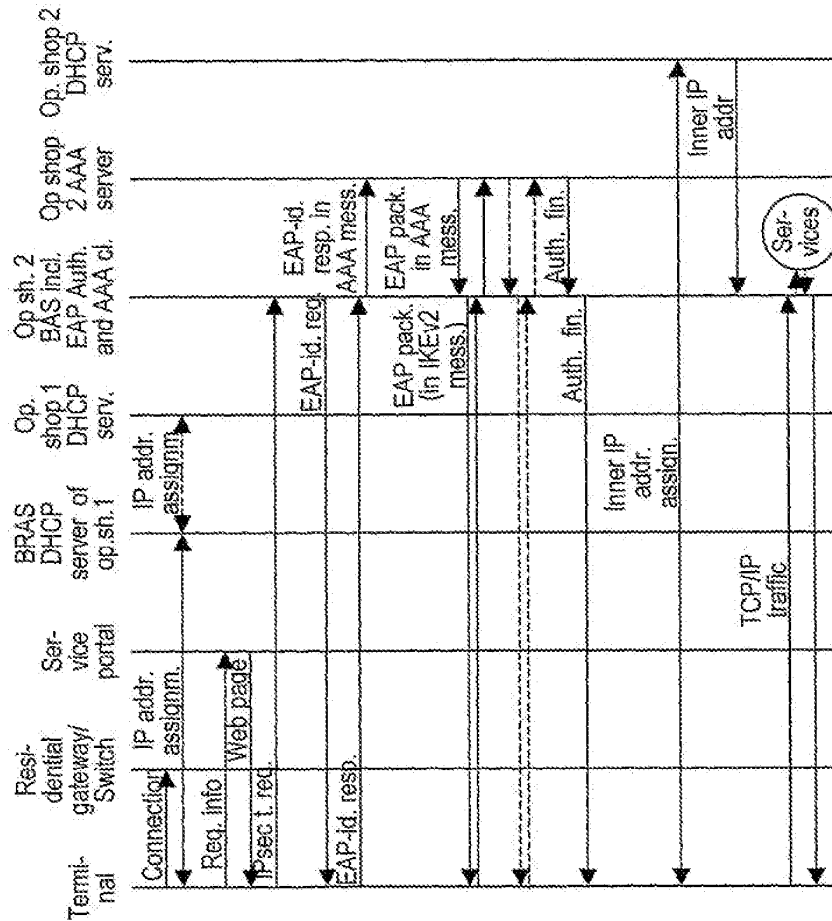


Fig. 79

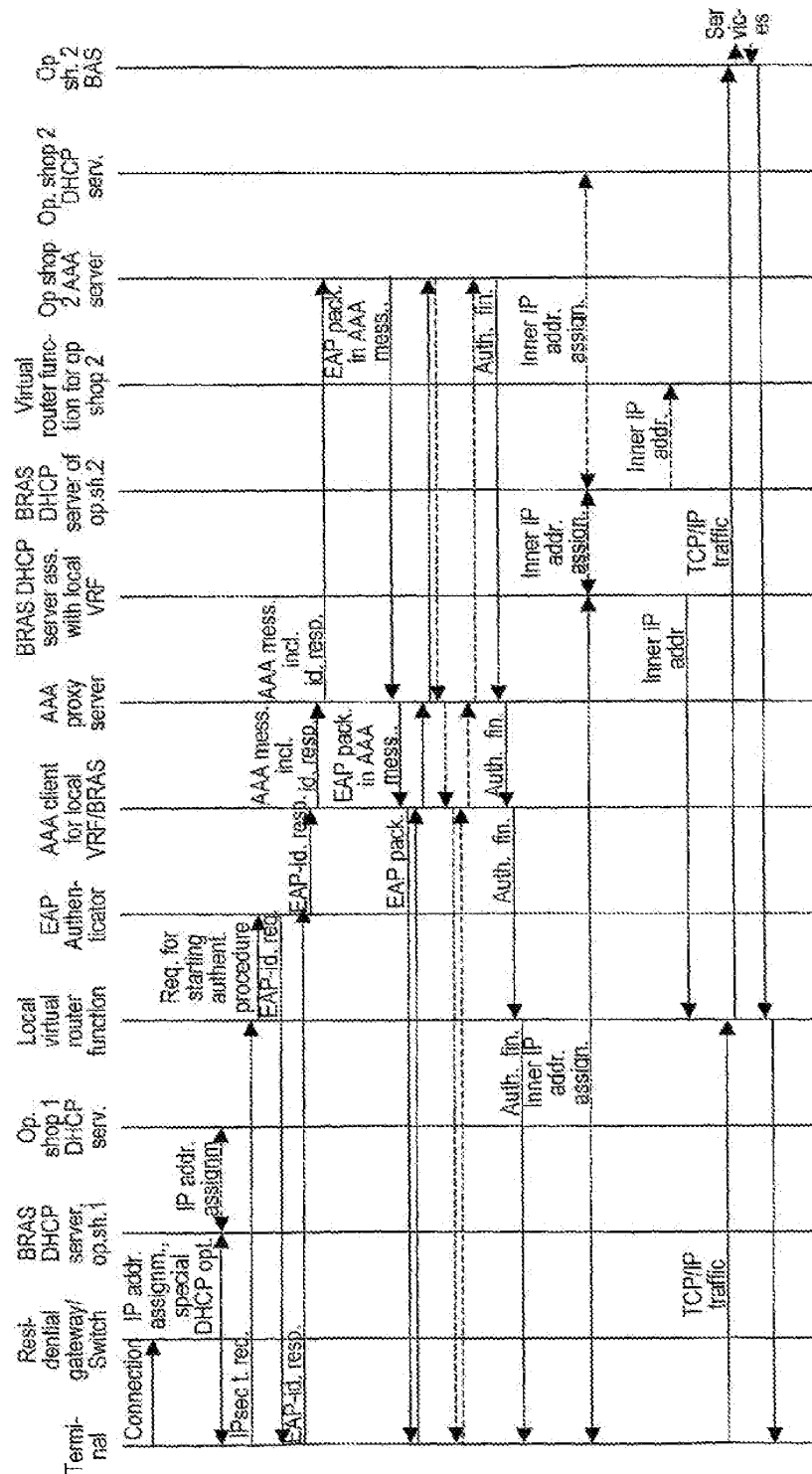


Fig. 17.

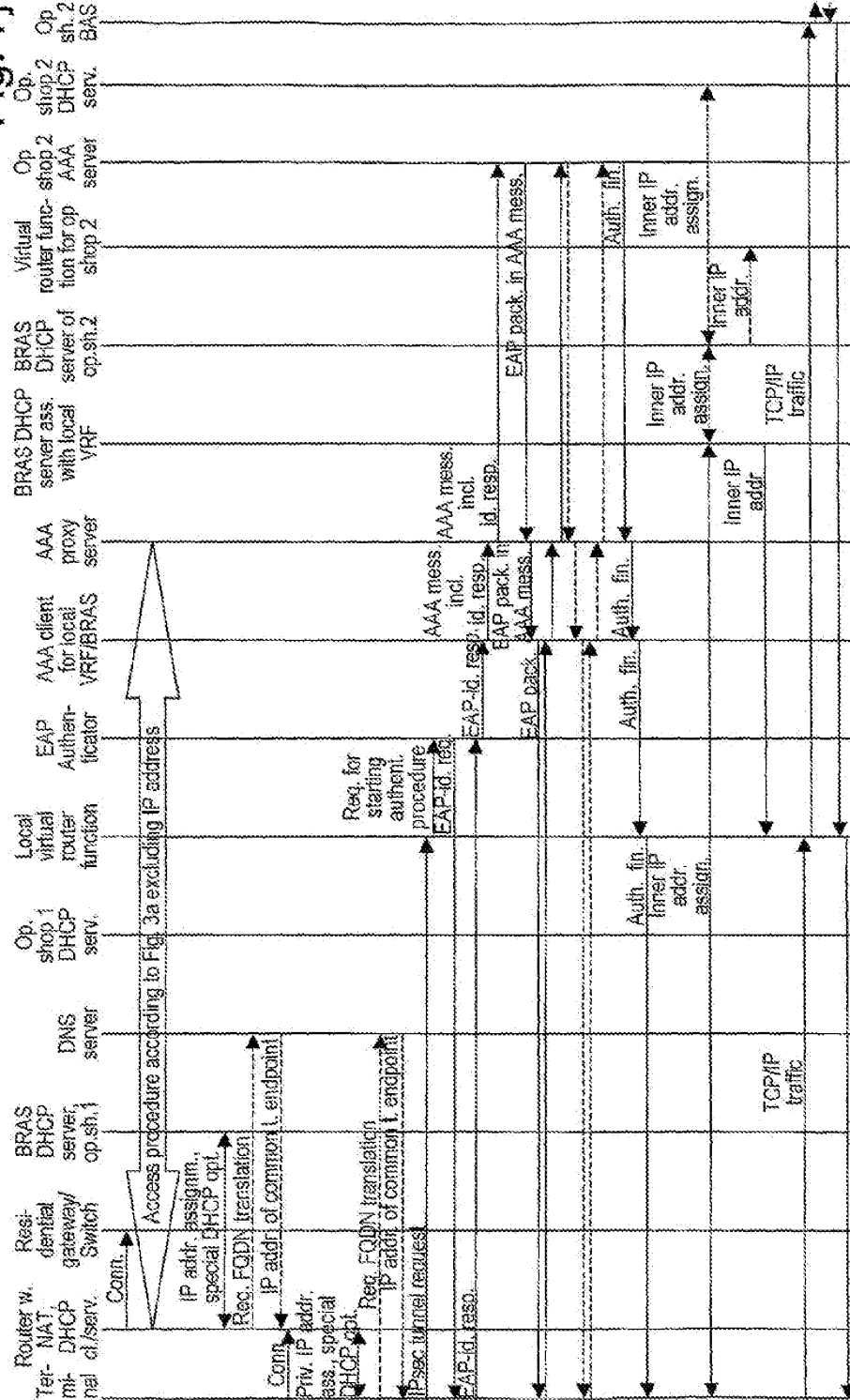


Fig. 8a

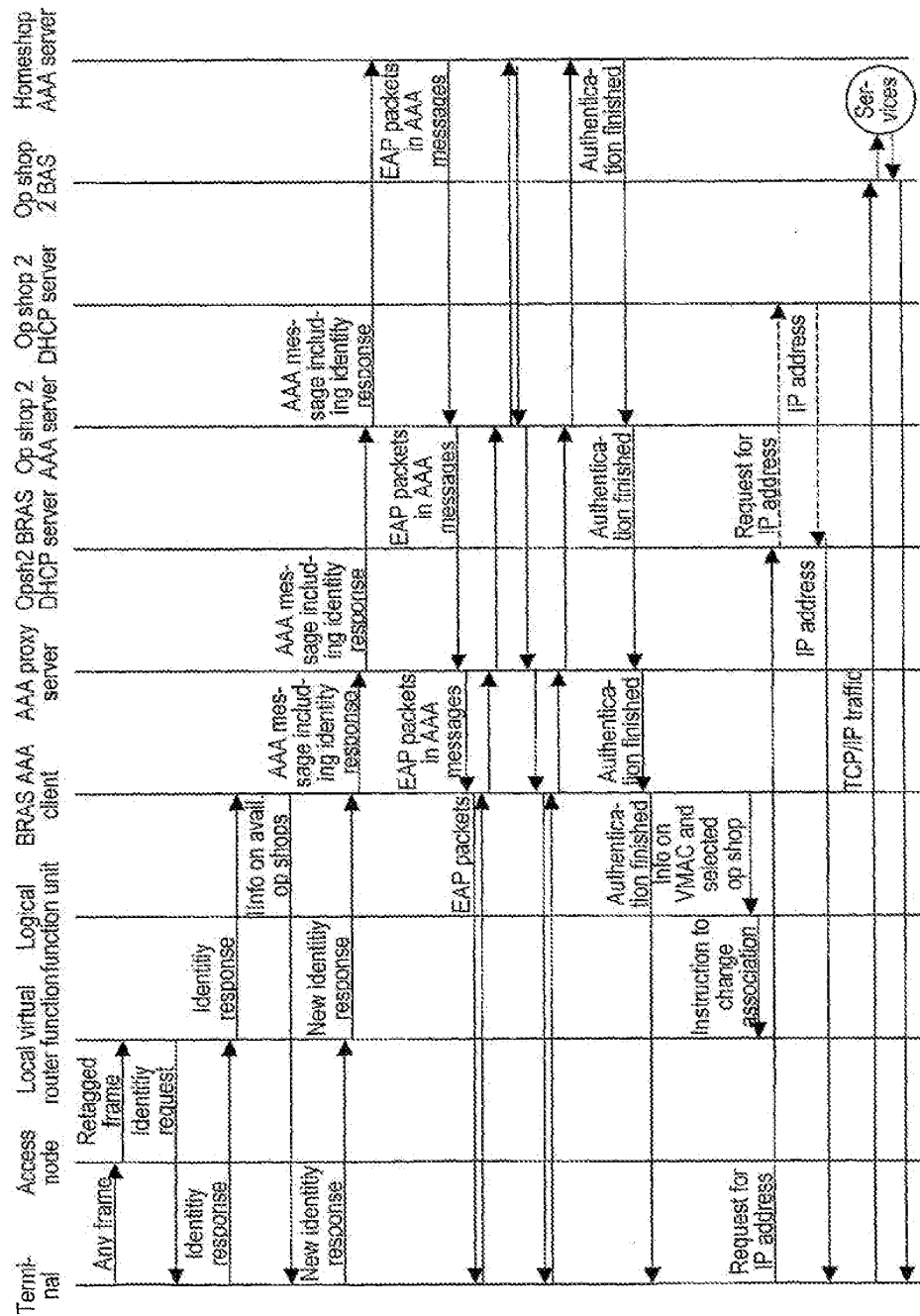


Fig. 8b

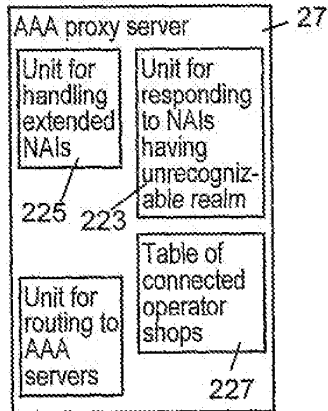


Fig. 8c

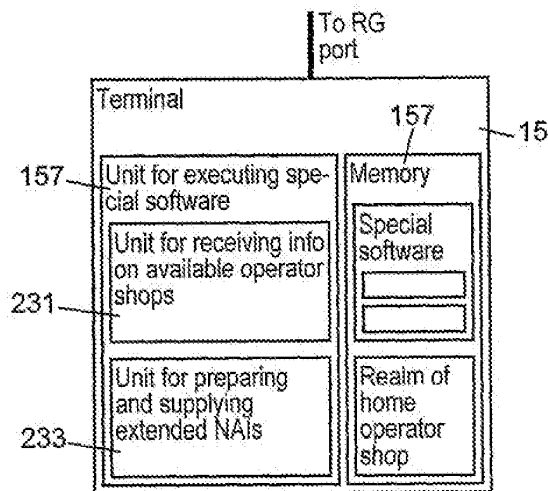
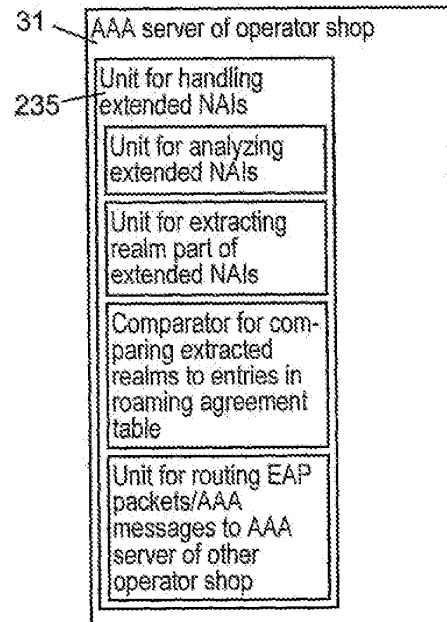
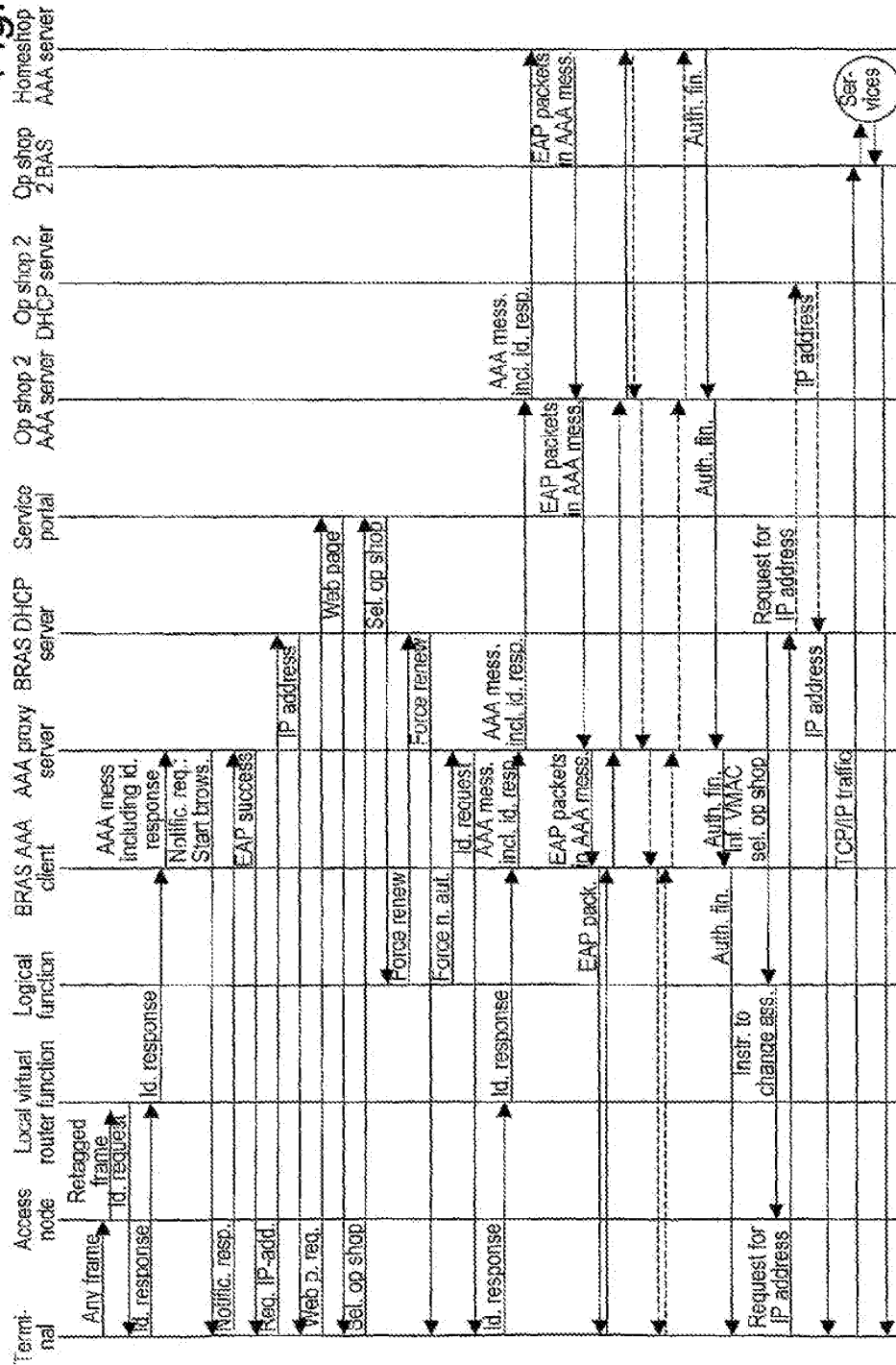


Fig. 8d



Page 96



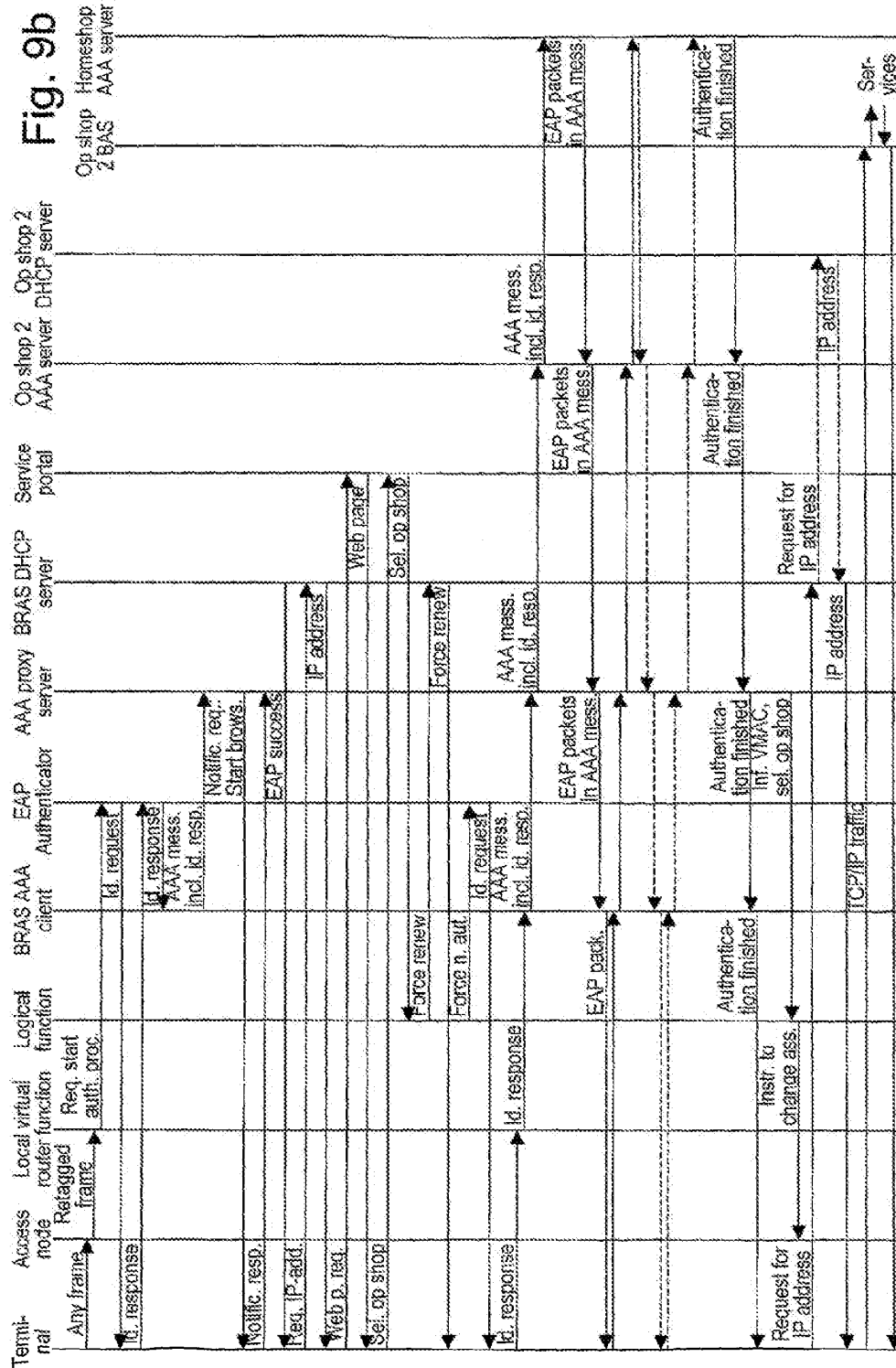


Fig. 9c

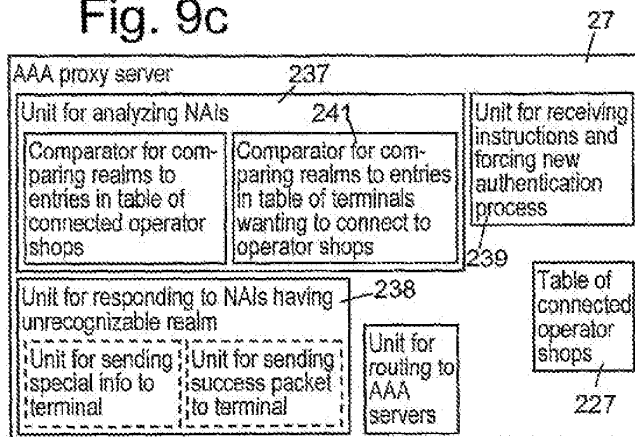


Fig. 9e

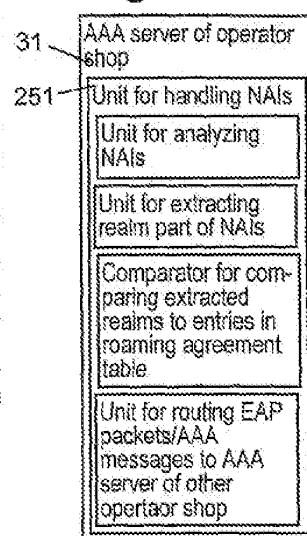


Fig. 9d

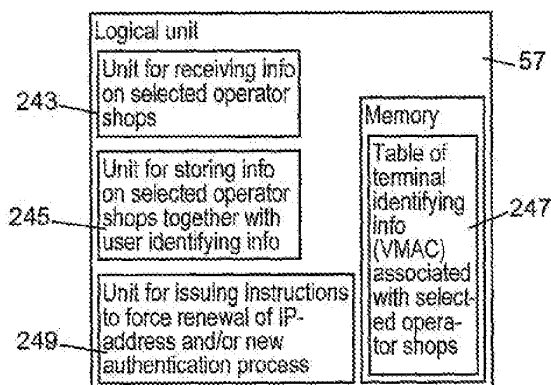


Fig. 9f

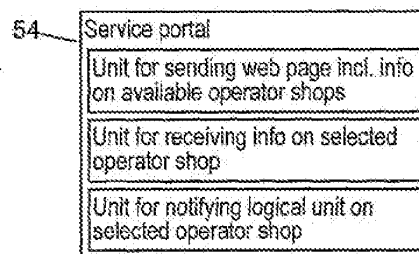
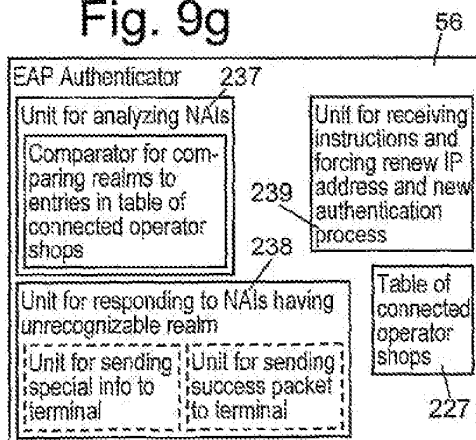


Fig. 9g



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2005060208 A [0037]
- US 2004066756 A [0047]
- US 2003117954 A [0048]
- US 2003037163 A [0049]
- WO 2006038843 A [0202] [0230]
- WO 2006038844 A [0202] [0213] [0230] [0243]

Non-patent literature cited in the description

- **B. ABOBA ; M. BEADLES.** The Network Access Identifier. RFC, January 1999, 2486 [0060]
- **B. ABOBA et al.** The Network Access Identifier. RFC, December 2005, 4282 [0060]
- **L. BLUNK ; J. VOLLBRECHT.** PPP Extensible Authentication Protocol (EAP). RFC, March 1998, 2284 [0060]
- **L. BLUNK et al.** Extensible Authentication Protocol (EAP). RFC, June 2004, 3748 [0060]
- **MAC-Forced Forwarding: A Method for Traffic Separation on an Ethernet Access Network. T. MELSEN ; S. BLAKE.** <draft-melsen-mac-forcedfwd-03.txt>, Personal Internet-Draft. IETF, August 2004 [0061]
- **MICHAEL BEGLEY.** The Public Ethernet - The next-generation broadband access network. *Ericsson Review*, 2004 [0061]
- **Medium Access Control (MAC) Security Enhancements**, 2004 [0063]
- **C. RIGNEY et al.** Remote Authentication Dial In User Service (RADIUS). RFC, June 2000, 2865 [0069]
- **B. ABOBA ; P. CALHOUN.** RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). RFC, September 2003, 3579 [0069]
- **P. CALHOUN ; J. LOUGHNEY ; E. GUTTMAN ; G. ZORN ; J. ARKKO.** Diameter Base Protocol. RFC, September 2003, 3588 [0069]
- **Diameter Extensible Authentication Protocol (EAP) Application.** Internet draft <draft-ietf-aaa-eap-03.txt>. IETF, October 2003 [0069]
- **D. MCPHERSON ; B. DYKES.** VLAN Aggregation for Efficient IP Address Allocation. RFC, February 2001, 3069 [0077]
- **L. MAMAKOS et al.** A Method for Transmitting PPP over Ethernet (PPPoE). RFC, February 1999, 2516 [0081]
- **D. HARRINGTON et al.** An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. RFC, December 2002, 3411 [0083]
- **Internet draft, <draft-adrangi-eap-network-Discovery-and-Selection-01.txt>.** Mediating Network Discovery and Selection [0241]

(19)



(11)

EP 2 713 670 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

02.04.2014 Bulletin 2014/14

(51) Int Cl.:

H04W 76/00 (2009.01)

(21) Application number: **12186237.9**

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

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

Designated Extension States:

BA ME

(71) Applicant: **BlackBerry Limited**

Waterloo, ON N2K 0A7 (CA)

(72) Inventors:

- **Smadi, Mohammed Nawaf**
Waterloo
Ontario N2L 3W8 (CA)

• **Montemurro, Michael Peter§**

Mississauga
Ontario L4W 0B5 (CA)

(74) Representative: **Hibbert, Juliet Jane Grace et al**

Kilburn & Strode LLP
Electronics
20 Red Lion Street
London WC1R 4PJ (GB)

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

(57) Techniques for use in a wireless device which is configured to operate as a group owner (GO) in a peer-to-peer (P2P) network are described. The group owner sends a first multicast message to one or more first P2P devices in the P2P network. The first multicast message includes first notice of absence (NoA) data. The group owner also sends a second multicast message to one or

more second P2P devices in the P2P network. The second multicast message includes second NoA data. Partitioning in the P2P network in this fashion may be set based on the different types of communications established with the P2P devices (e.g. different traffic classes or Quality of Service (QoS) types).

EP 2 713 670 A1

Description

BACKGROUND

Field Of The Technology

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

Description Of The Related Art

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

FIG. 1 is an illustrative representation of a communication system which includes wireless communication networks (e.g. WLANs) with which a wireless communication device may communicate;

FIG. 2 is an example of a schematic block diagram of the wireless device of FIG. 1;

FIGs. 3 and 4 are some examples of different types of wireless devices of the present disclosure, which include a smartphone (FIG. 3) and a tablet computer (FIG. 4);

FIG. 5 is an illustrative representation of a part of the communication system of FIG. 1 which may involve different types of wireless networks and communications;

FIG. 6 is an illustrative representation of a portion of memory of the wireless device, where the memory has a plurality of profiles stored therein, where each profile is associated with a first type of wireless connection (e.g. a client station type) or a second type of wireless connection (e.g. a peer-to-peer type);

FIG. 7 is a block diagram for illustrating concurrent operations of the wireless device which may operate as a group owner (GO) in a P2P network;

FIG. 8 is an illustration of the format of a message

which may be utilized for multicast addressing for communicating different Notice of Absence (NoA) data to different multicast groups;

FIG. 9 is a flowchart for describing a method for use in communicating in a P2P network;

FIG. 10 is a timing diagram of communications involving the wireless device operating as a group owner in a P2P network, scheduling absences in the P2P network by communicating NoA data without use of the technique of FIG. 9;

FIG. 11 is another timing diagram of communications involving the wireless device operating as a group owner in a P2P network, scheduling absences in the P2P network by communicating different NoA data to different multicast groups using the technique of FIG. 9; and

FIG. 12 is a close-up of a portion of the timing diagram of FIG. 11, showing the differences in doze periods of the different multicast groups based on the different NoA data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

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

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

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

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

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

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

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

[0011] Such wireless networks (e.g. infrastructure WLANs) may provide or allow access to various data and communication services to its terminals. For example, the wireless networks may provide for communication

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[0025] In some example embodiments, the orientation subsystem 249 may include other orientation sensors 251, instead of or in addition to accelerometers. For example, in various example embodiments, the orientation

subsystem 249 may include a gravity sensor, a gyroscope, a tilt sensor, an electronic compass or other suitable sensor, or combinations thereof. In some example embodiments, the device orientation subsystem 249 may include two or more orientation sensors 251 such as an accelerometer and an electronic compass.

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

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

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

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

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

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

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

[0032] Wireless device 201 also includes a battery 238 as a power source, which is typically one or more rechargeable batteries that may be charged for example, through charging circuitry coupled to a battery interface 236 such as the data port 252. The battery 238 provides electrical power to at least some of the electrical circuitry in wireless device 201, and the battery interface 236 provides a mechanical and electrical connection for the bat-

tery 238. The battery interface 236 is coupled to a regulator (not shown) which provides a regulated voltage V to the circuitry for powering wireless device 201.

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

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

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

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

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

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

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

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

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

RAM 246 for execution by the processor 240 at runtime.

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

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

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

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

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

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

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

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

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

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

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

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

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

[0053] The example tablet computer 300 also includes a microphone 258. In the example illustrated, the microphone 258 is vertically disposed below the display 304

when the tablet computer is held in the landscape orientation illustrated in FIG. 4. The microphone 258 may be located in other locations in other example embodiments.

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

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

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

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

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

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

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

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

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

[0062] Each one of profiles 602 is associated with a particular WLAN infrastructure network, and includes a

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

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

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

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

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

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

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

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

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

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

[0071] To accommodate for such various use cases, profiles associated with the various application/services utilizing Wi-Fi P2P networks are created and stored on

the wireless device. These profiles are enabled when needed, such as enabled in response to an activation of an application associated therewith. Further, the profiles may be enabled concurrently.

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

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

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

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

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

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

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

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

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

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

[0081] Note that a traffic class may be a conversational or voice traffic class, a streaming traffic class, an interactive traffic class, or a background traffic class. A conversational or voice traffic class is associated with traditional voice communications, which are usually two-way and sensitive to delay, delay variation, and data loss. A streaming traffic class is typically associated with one-way communications which are less sensitive to delay and data loss, but are sensitive to delay variations and typically require a high bandwidth. An example of streaming traffic class is a video player application. On the other hand, an interactive traffic class is typically associated with two-way "busty" types of communications. These communications can tolerate moderate delay and data loss and have variable bandwidth requirements. On-line

video game and web-surfing (browser) applications are examples of the interactive traffic class. Finally, a background traffic class is typically associated with communications which are highly tolerant of delay and data loss and may have variable bandwidth requirements. Examples of these applications include e-mail and file transfer applications.

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

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

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

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

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

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

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

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

[0089] Multicast addressing is now discussed with reference back to FIG. 8, which is an illustration of a format of a message including an address field 800 which may be populated with an address for multicast messaging. The address may be referred to as a MAC address or a layer-2 address. MAC is used for access to the physical layer from the data link layer according to the ISO/OSI model. Address field 800 may include an indication which indicates whether the address is a unicast address or a multicast address. The indication may be a bit indication in address field 800 (e.g. the least significant bit of the most significant octet of the address). If the least significant bit of the most significant octet of the address is set to zero ("0"), the frame is intended to reach only a single receiving device. This type of communication or addressing may be referred to as unicast communication or addressing. Here, a unicast frame is transmitted to all nodes within the collision domain, which typically ends at the nearest network switch or router. Only the node with the matching hardware MAC address will accept the frame, and network frames with non-matching MAC addresses are ignored. On the other hand, if the least significant bit of the most significant octet of the address is set to one ("1"), the frame will still be sent only once; however, devices may accept the frame based on different criteria than a matching MAC address. For example, devices may accept the frame based on a configurable list of accepted multicast MAC addresses. This type of communication or addressing may be referred to as multicast

communication or addressing.

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

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

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

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

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

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

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

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

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

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

[0097] In this example, the first multicast group may be of the voice or conversational traffic class and/or or

have a relatively low minimum bandwidth requirement, whereas the second multicast group may be of the streaming traffic class and/or have a relatively high minimum bandwidth requirement.

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

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

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

Claims

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

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

- multicast message including first notice of absence (NoA) data; and
 sending a second multicast message to one or more second P2P devices in the P2P network, the second multicast message including second NoA data.
2. The method of claim 1, wherein the first NoA data includes a first time period of absence for communicating with the first P2P devices, and the second NoA data includes a second time period of absence for communicating with the second P2P devices, the method further comprising:
- identifying that the one or more first P2P devices are associated with a first type of communications;
 identifying that the one or more second P2P devices are associated with a second type of communications; and
 calculating the first and the second time periods of absences based on the first and the second types of communications.
3. The method of claim 1, wherein communications of the one or more first P2P devices are associated with a first traffic class or first Quality of Service (QoS) criteria, and communications of the one or more second P2P devices are associated with a second traffic class or second first QoS criteria.
4. The method of claim 3, further comprising:
- identifying that the communications of the one or more first P2P devices are associated with the first traffic class or the first QoS criteria; and
 identifying that the communications of the one or more second P2P devices are associated with the second traffic class or the second QoS criteria.
5. The method of claim 4, further comprising:
- calculating the first NoA data for the one or more first P2P devices in response to identifying their association with the first traffic class or the first QoS criteria; and
 calculating the second NoA data for the one or more second P2P devices in response to identifying their association with the second traffic class or second QoS criteria.
6. The method of claim 1, wherein at least the first multicast message is included in a beacon frame.
7. The method of claim 1, wherein the first NoA data is indicative of a first period of absence for communicating with the first P2P devices, and the second
- NoA data is indicative of a second period of absence for communicating with the second P2P devices, the method further comprising:
- communicating with the one or more first P2P devices outside of the first period of absence indicated in the first NoA data; and
 communicating with the one or more second P2P devices outside of the second period of absence indicated in the first NoA data.
8. The method of claim 6, wherein the first NoA data comprises a first NoA attribute which includes a first start time, a first interval, a first duration, and a first count field, and wherein the second NoA data comprises a second NoA attribute which includes a second start time, a second interval, a second duration, and a second count field.
9. A wireless communication device, comprising:
- one or more processors;
 a radio frequency (RF) transceiver (RF) coupled to the one or more processors; and
 the one or more processors being configured to operate the wireless communication device as a group owner (GO) in a peer-to-peer (P2P) network by performing the method of any one of claims 1-8.
10. A method in a wireless peer-to-peer (P2P) device which is configured to communicate in a P2P network having a group owner (GO), the method comprising:
- receiving from the group owner a multicast message which includes notice of absence (NoA) data, the NoA data including a time period of absence from the P2P network; and
 refraining from communicating with the group owner during the time period of absence indicated in the NoA data of the multicast message.
11. The method of claim 10, further comprising:
- entering into a doze state during the time period of absence indicated in the NoA data of the multicast message.
12. The method of claim 10, further comprising:
- communicating with the group owner outside of the time period of absence indicated in the NoA data of the multicast message.
13. The method of claim 10, further comprising:
- wherein the time period of absence is set in ac-

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

5

10

14. A wireless communication device, comprising:

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

15

20

25

30

35

40

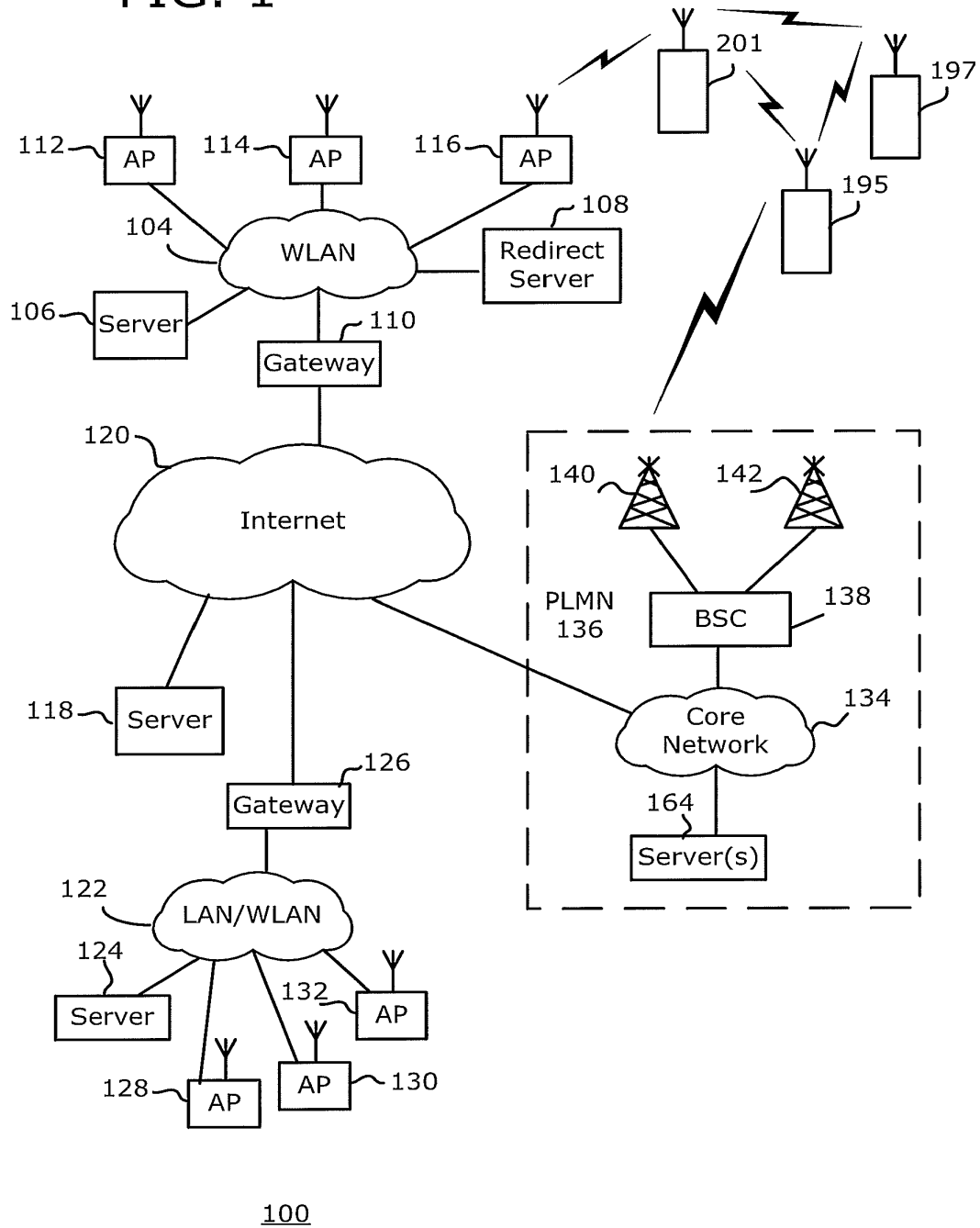
45

50

55

15

FIG. 1



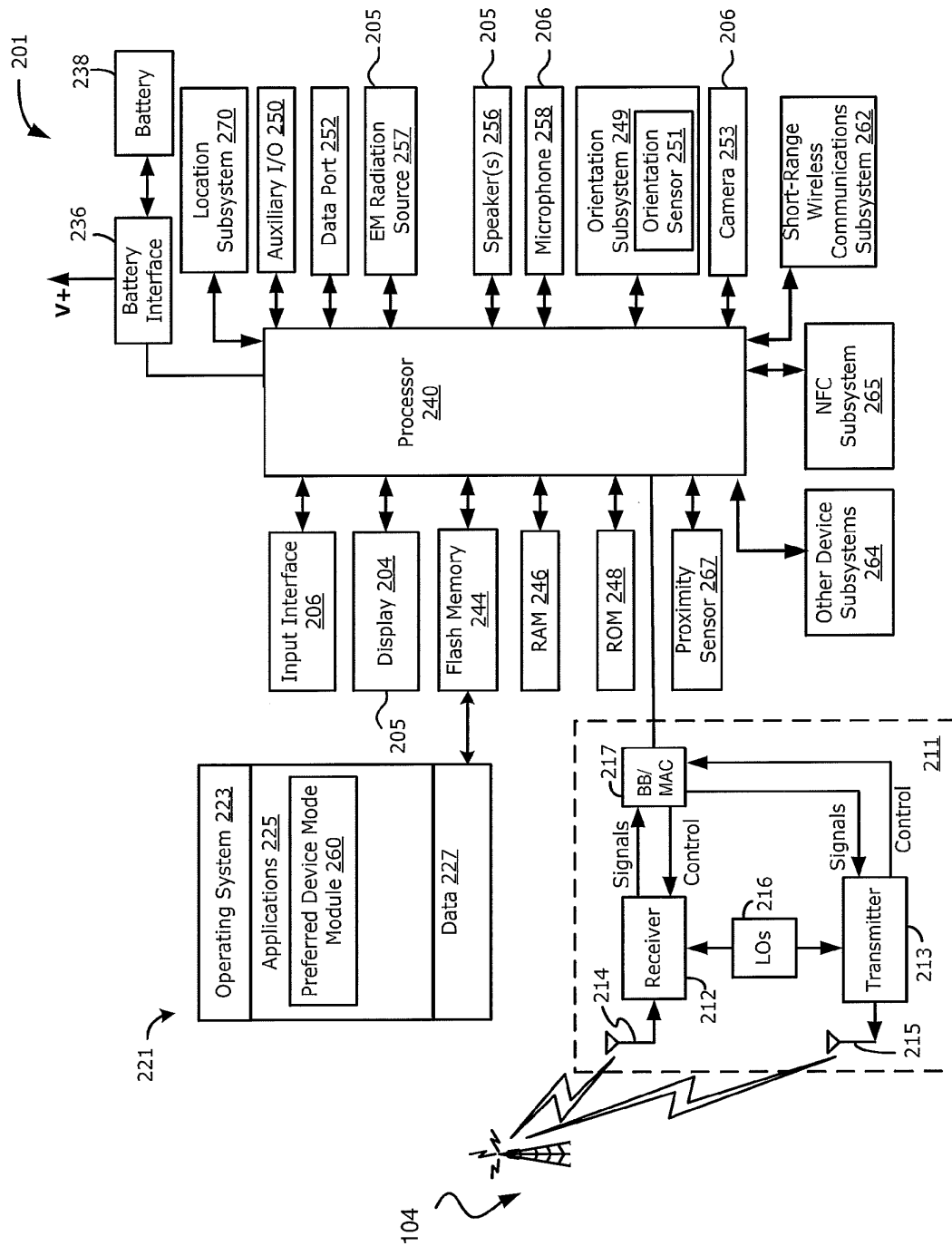


FIG. 2

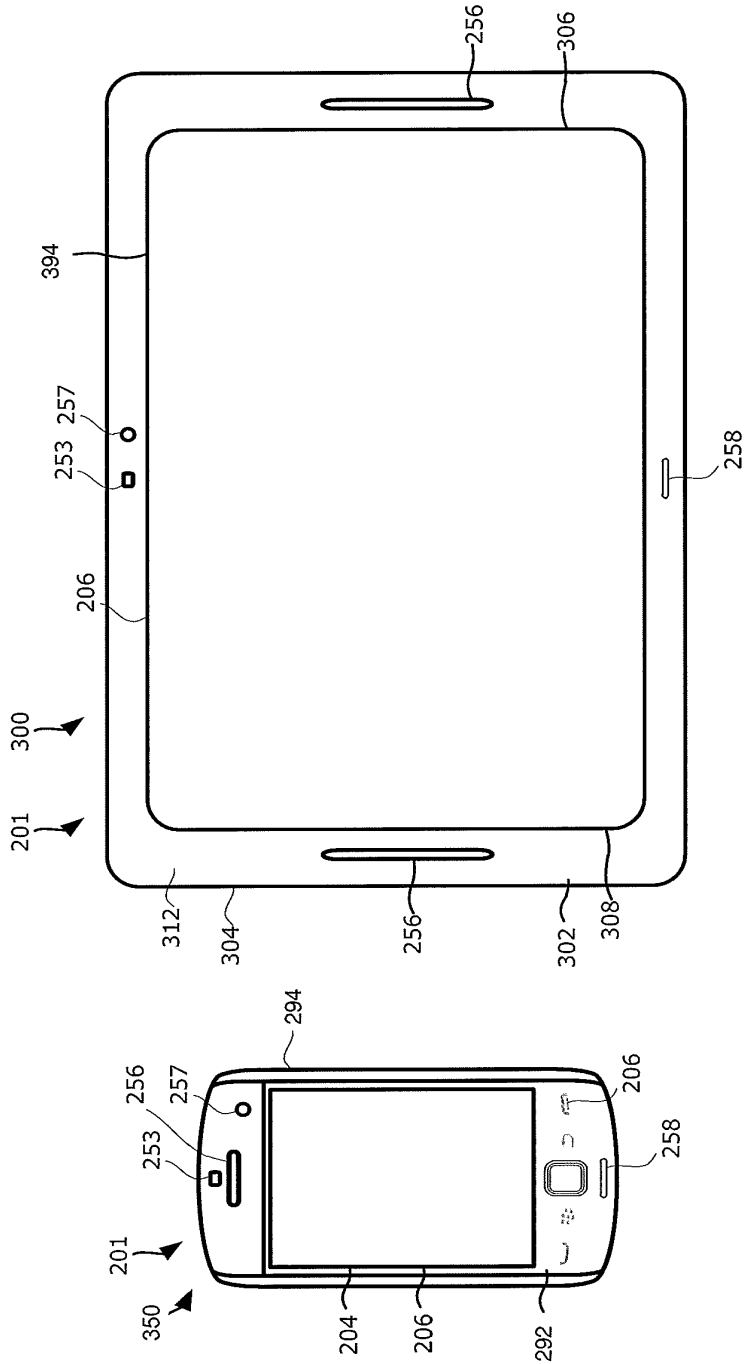


FIG. 4

FIG. 3

FIG. 5

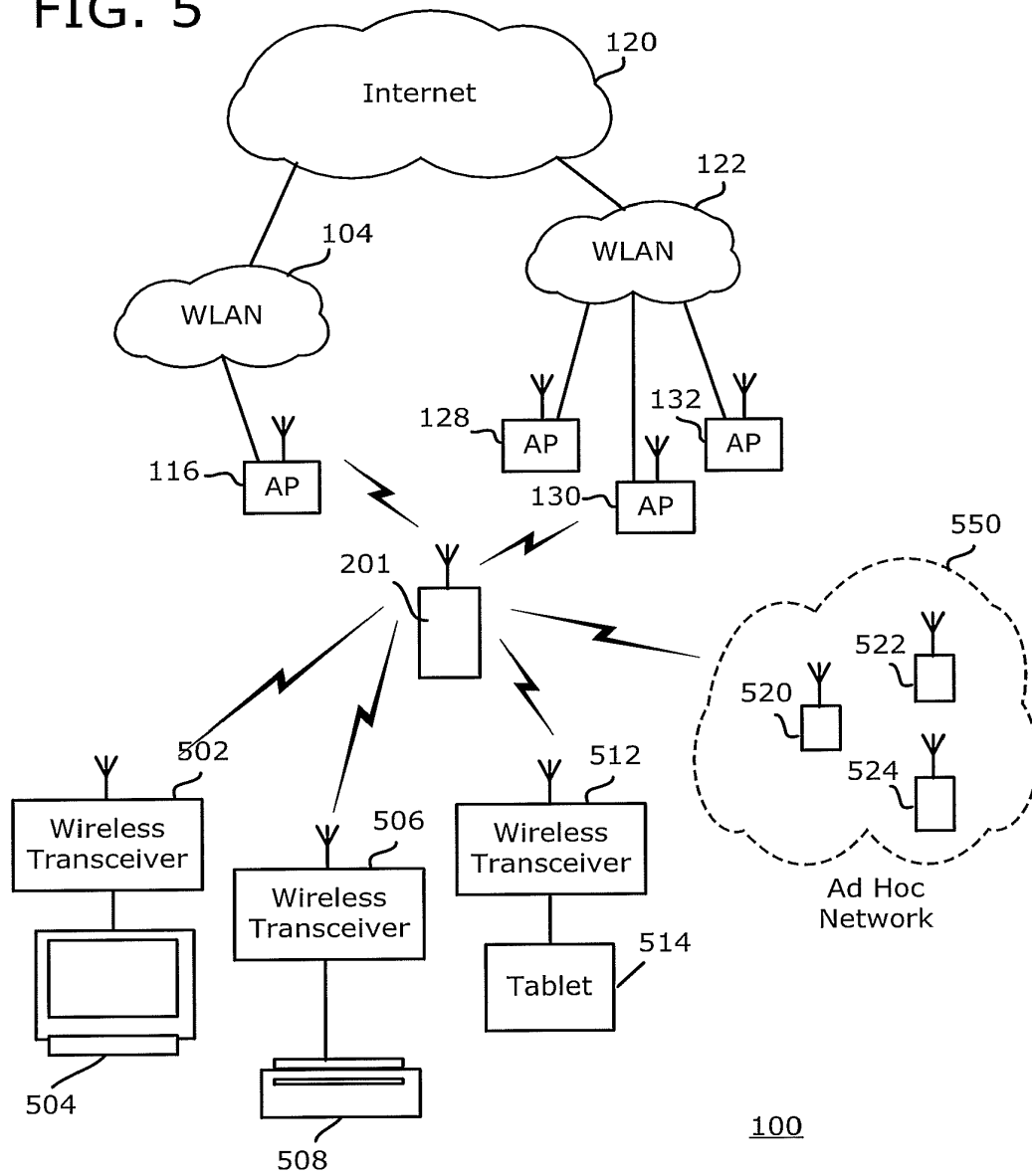


FIG. 6

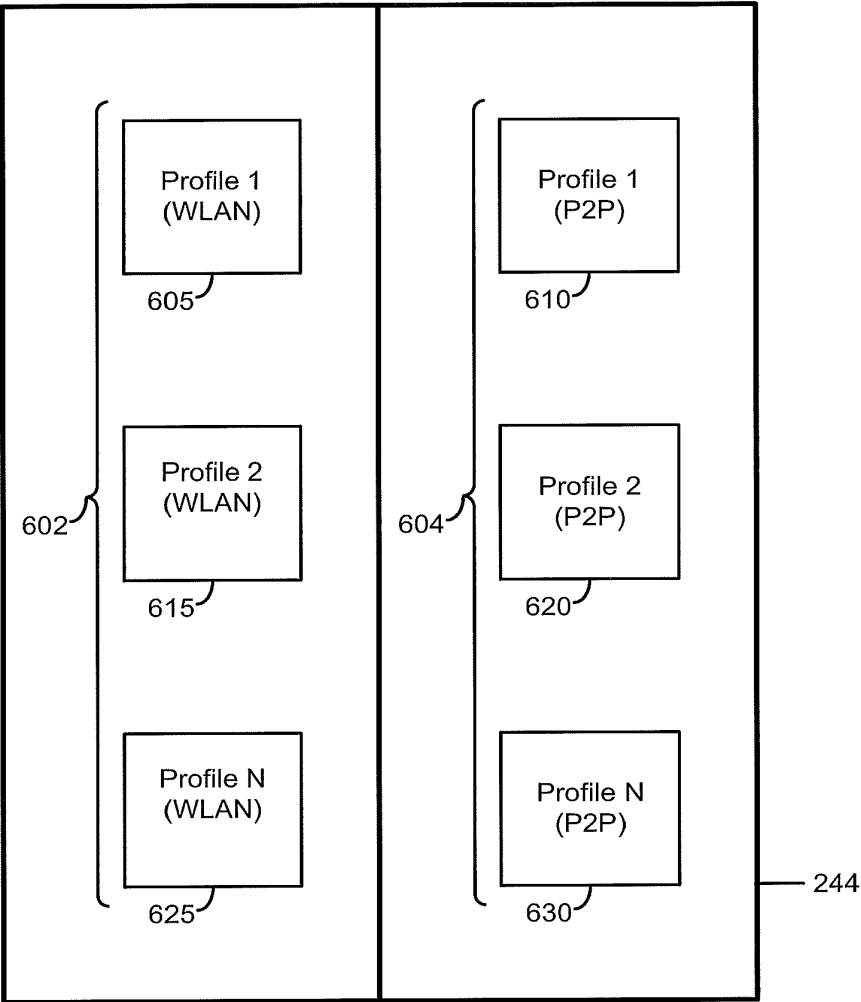
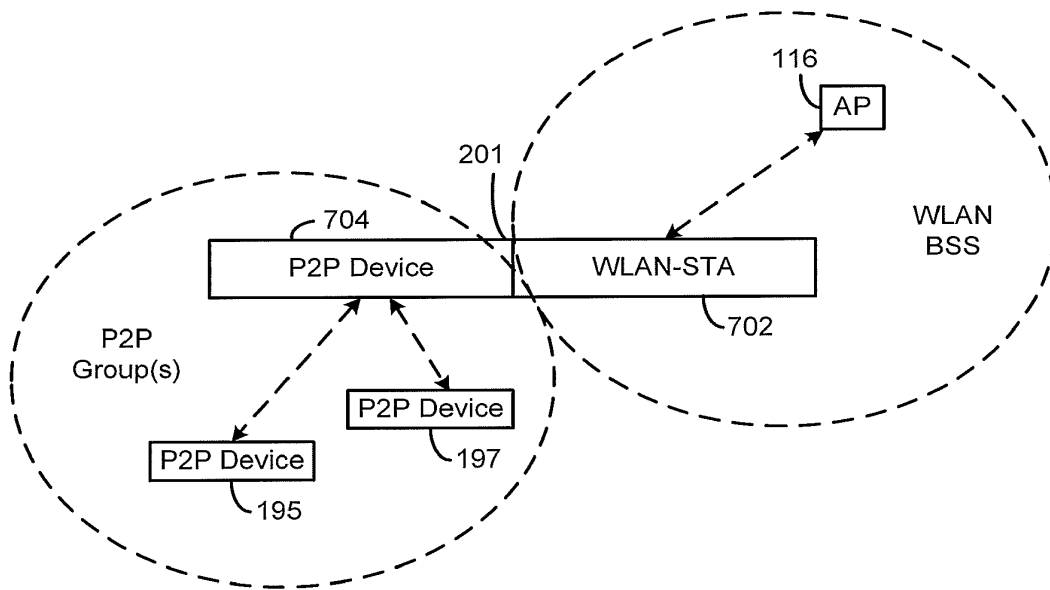


FIG. 7



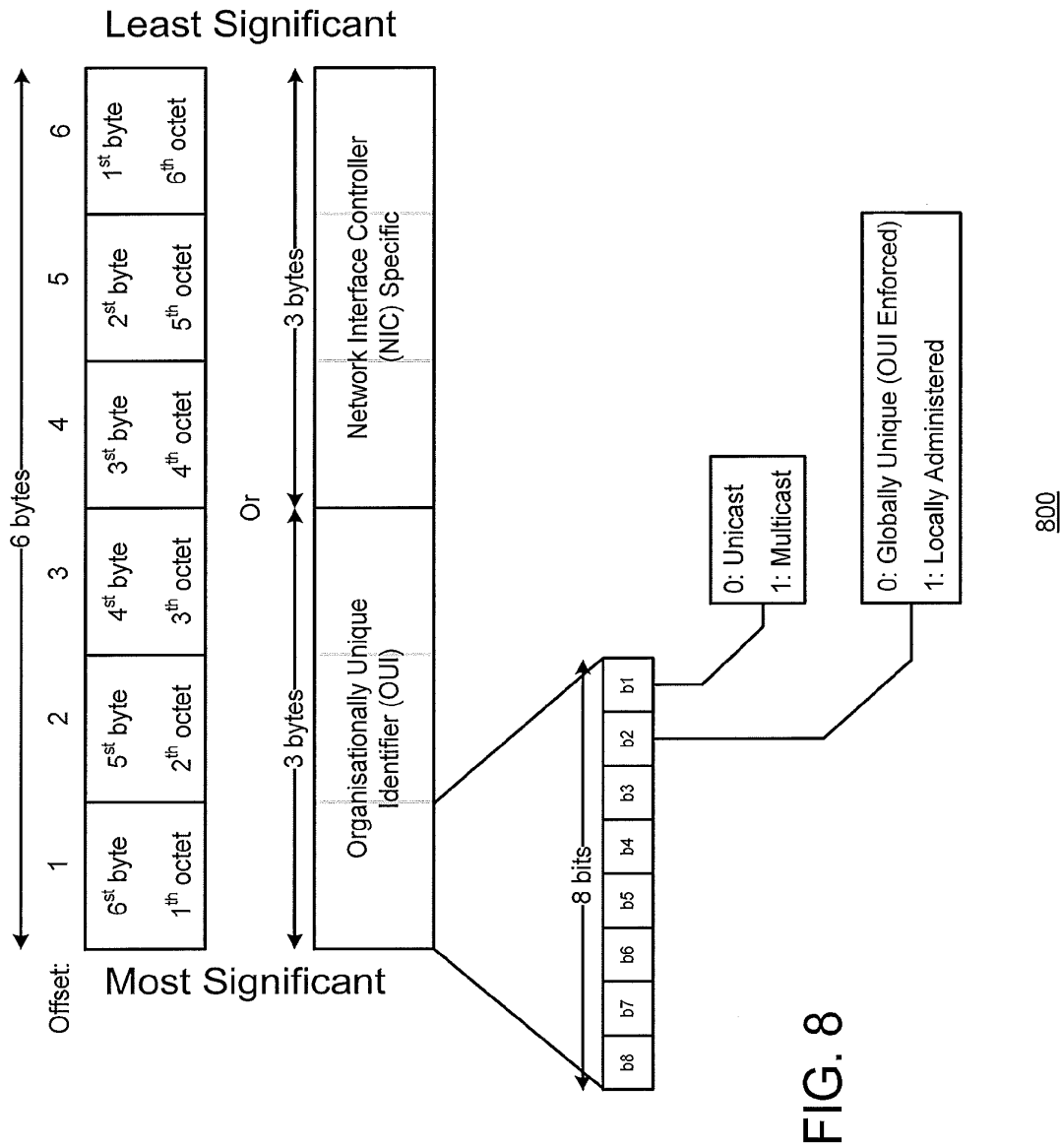
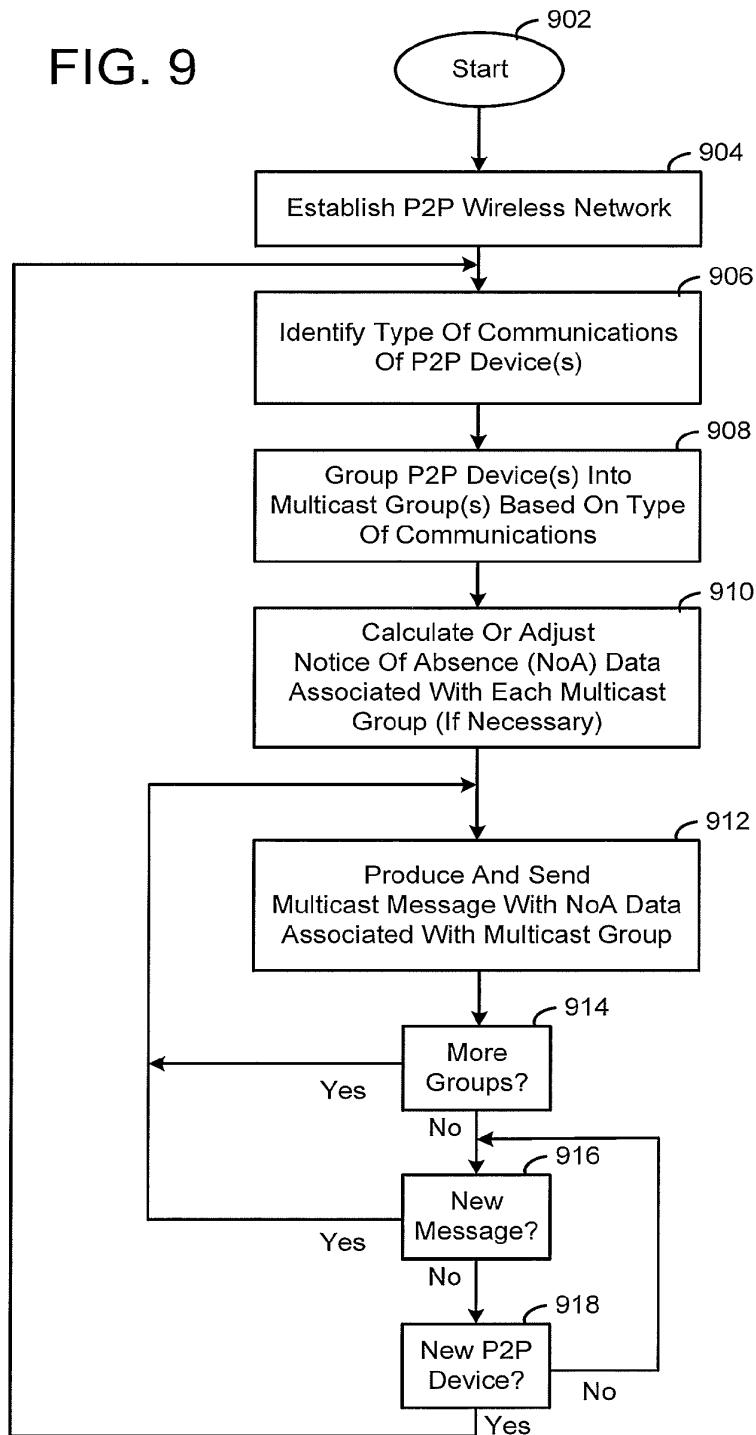


FIG. 9



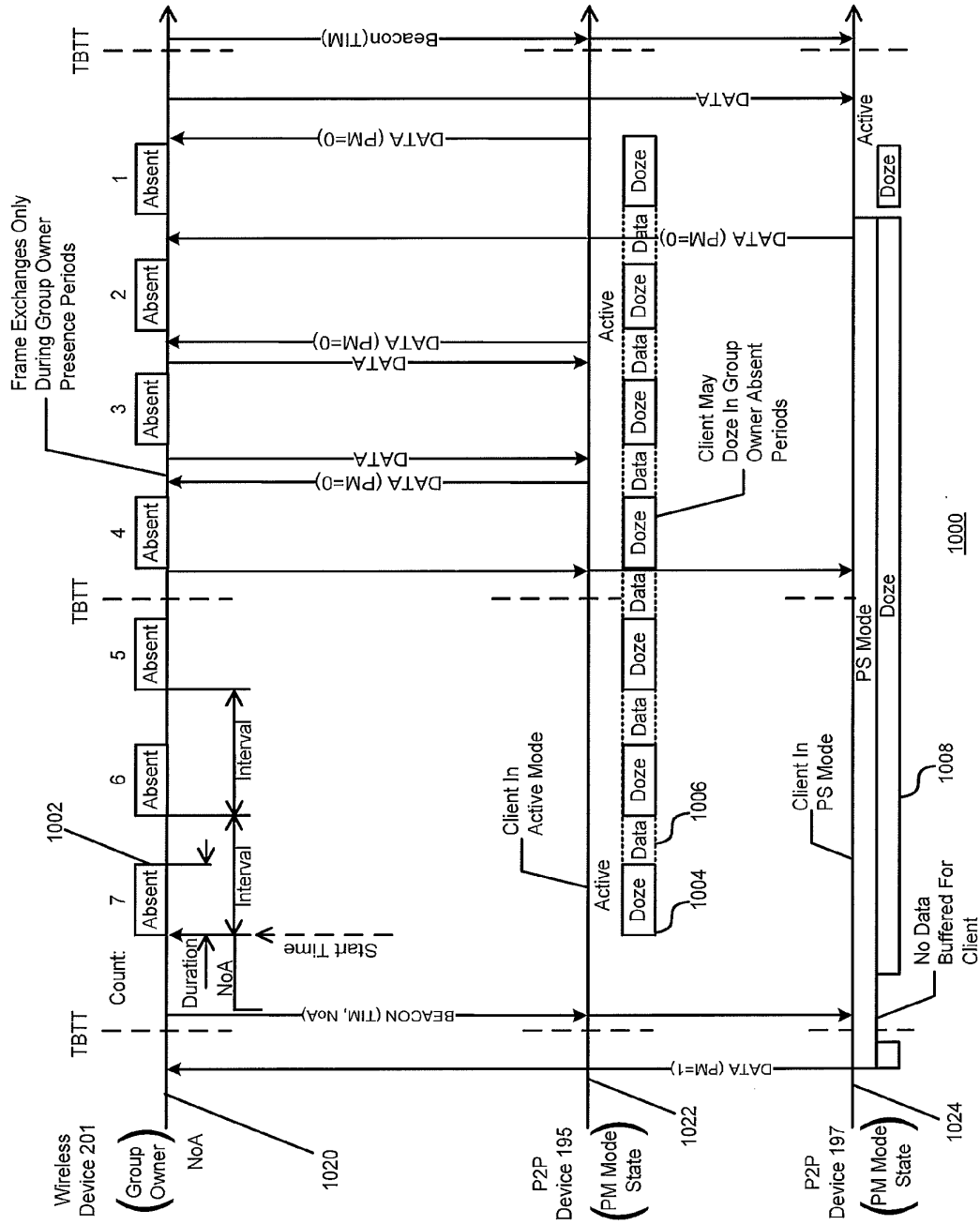


FIG. 10

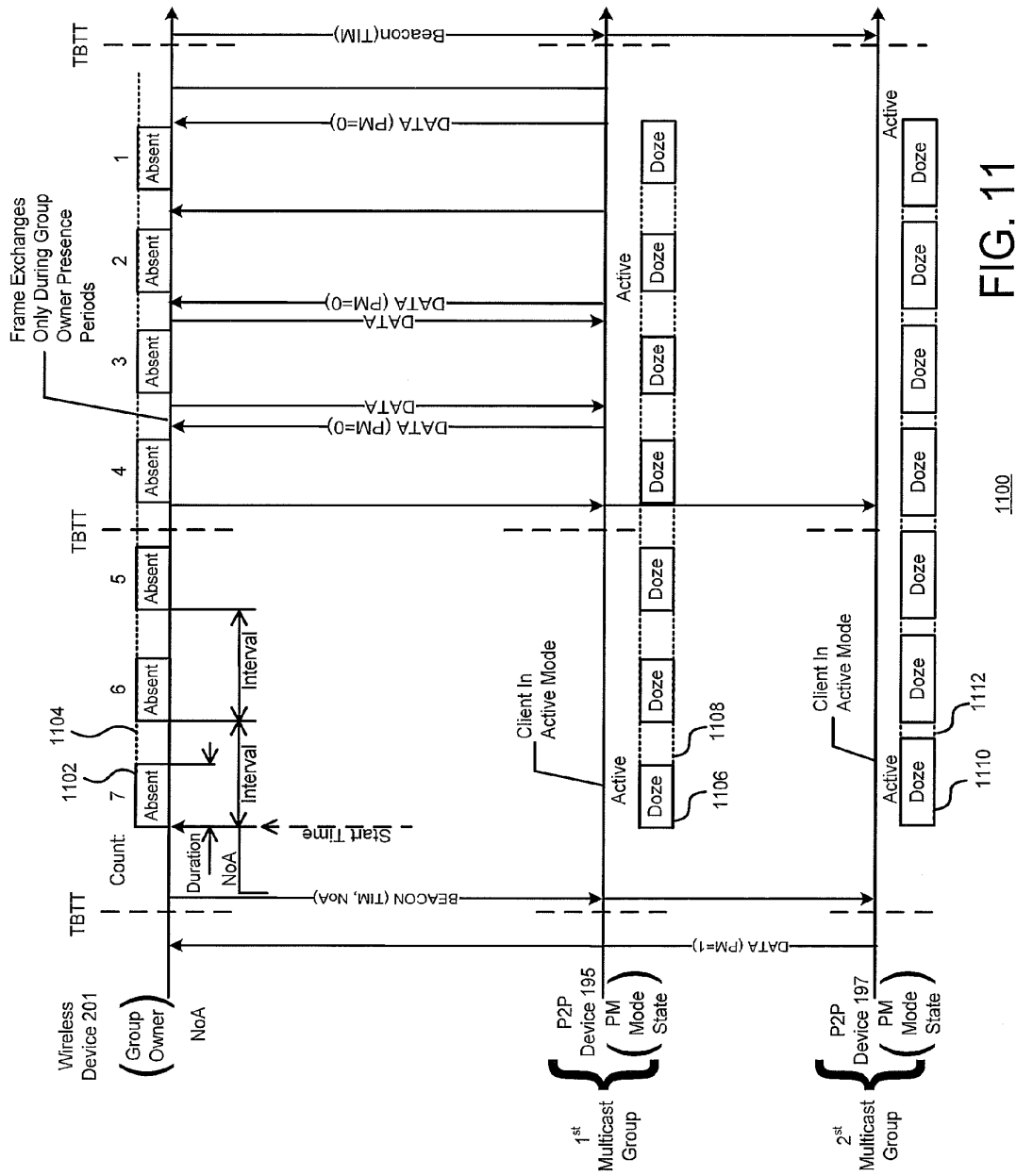


FIG. 11

1100

1102

1104

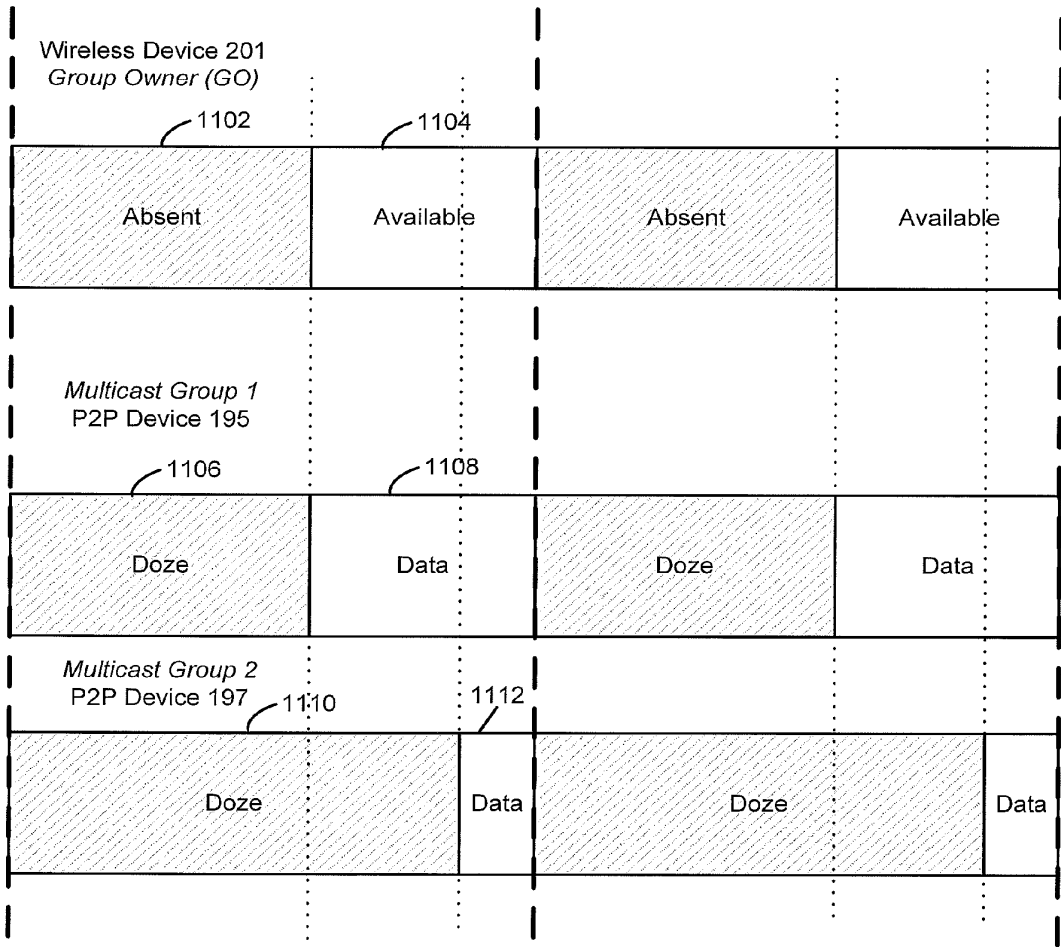
1106

1108

1110

1112

FIG. 12



1200



EUROPEAN SEARCH REPORT

Application Number
EP 12 18 6237

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WI-FI ALLIANCE: "Wi-Fi Peer-to-Peer (P2P) Specification v1.1", WI-FI ALLIANCE SPECIFICATION,, 1 January 2010 (2010-01-01), pages 1-159, XP009163866,	10-12,14	INV. H04W76/00
Y	* sections 3.2.6, 3.3.3.2 *	1-9,13	
Y	US 2006/268873 A1 (TONJES RALF [DE] ET AL TOENJES RALF [DE] ET AL) 30 November 2006 (2006-11-30) * paragraphs [0011], [0035] - [0040], [0059] *	1-9,13	
A	Wi-Fi Alliance: "Wi-Fi CERTIFIED Wi-Fi Direct", 1 October 2010 (2010-10-01), pages 1-14, XP055041124, Retrieved from the Internet: URL:http://www.wi-fi.org/knowledge-center/ white-papers/wi-fi-certified-wi-fi-direct% E2%84%A2-personal-portable-wi-fi%C2%AE-con nect-devices [retrieved on 2012-10-16] * tables 1, 2 *	1-14	TECHNICAL FIELDS SEARCHED (IPC) H04W
A	WO 2011/046703 A2 (INTEL CORP [US]; YUAN HAO [CN]) 21 April 2011 (2011-04-21) * the whole document *	1-14	
A	US 2012/106381 A1 (VEDANTHAM RAMANUJA [US] ET AL) 3 May 2012 (2012-05-03) * the whole document *	1-14	
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 19 February 2013	Examiner Saffell, Christine
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

3
EPO FORM 1503 03 02 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 12 18 6237

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

19-02-2013

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

EPO FORM P0459

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 18/448,281
Confirmation No.: 1540
First-Named Inventor: Sai C. Manapragada
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

INFORMATION DISCLOSURE STATEMENT TRANSMITTAL

1. List of All Patents, Publications, U.S. Applications, or Other Information

Pursuant to the provisions of 37 C.F.R. §§ 1.56, 1.97, and 1.98, applicant requests consideration of the references listed on the attached PTO/SB/08 form(s) [commonly referred to as a PTO-1449 form] and/or the additional information identified below.

2. Enclosed Legible Copies

2a. A legible copy of each foreign patent document and publication listed on the PTO/SB/08 form is enclosed:

- ☐ i. except, pursuant to MPEP 609.02, a copy is not provided for each reference previously cited by or submitted to the Patent Office in prior US Patent Application No(s). _____, filed _____ from which the present application claims priority under 35 U.S.C. § 120.
- ☐ ii. except, a copy is not provided for each cumulative reference and enclosed reference identified below:

☐ 2b. A copy of the specification and drawings for each cited unpublished U.S. application.

☐ 2c. A copy of a Search Report or Written Opinion from a foreign patent office is also enclosed.

- ☐ 2d. Consideration of the enclosed additional and/or below discussed information is requested.

3. Concise Explanation of Relevance for Non-English Language Information

For each non-English language reference listed on the attached PTO/SB/08 form(s), reference is made to:

- ☒ 3a. an English language translation submitted herewith,
- ☐ 3b. a foreign patent office Search Report (in the English language) submitted herewith,
- ☐ 3c. an English language translation of a foreign patent office Search Report submitted herewith,
- ☐ 3d. the concise explanation contained in the present application at page(s) _____,
- ☐ 3e. the concise explanation set forth in the attached English language abstract,
- ☐ 3f. a copy of a related patent publication (in the English language) cited herewith,

Foreign Patent Document	Corresponding English Language Patent Document

- ☐ 3g. the following concise explanation: _____.

4. Time for Filing

- ☒ 4a. This Information Disclosure Statement is submitted:
- ☒ i. for U.S. national applications or national stage PCT applications (not including CPAs and RCEs), within three months of filing or entry into national stage;
- ☒ ii. for U.S. national applications, national stage PCT applications, CPAs, or RCEs before the first Office Action on the merits;
and/or
- ☐ iii. before the mailing of an Office Action on the merits after the filing of a Request for Continued Examination (RCE) under § 1.114,

and thus no certification and/or fee is required.

- ☐ 4b. This information Disclosure Statement is submitted after three months from the filing date and after the first Office Action on the merits but prior to the mailing date of a final Office Action or Notice of Allowance, and thus:
 - ☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below, or
 - ☐ ii. the fee set forth in 37 C.F.R. § 1.17(p) is enclosed.
- ☐ 4c. This Information Disclosure Statement is submitted after the mailing date of a final Office Action or Notice of Allowance and prior to payment of the issue fee, and thus:
 - ☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below and the fee set forth in 37 C.F.R. § 1.17(p) is enclosed, or
 - ☐ ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.
- ☐ 4d. This Information Disclosure Statement is submitted after payment of the issue fee, and thus:
 - i. a Petition to Withdraw from Issue pursuant to 37 C.F.R. § 1.313(c)(2) has been filed, and
 - ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.

5. Certification- Statement Under 37 C.F.R. 1.97(e)

- ☐ 5a. It is hereby certified that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.
- ☐ 5b. It is hereby certified that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

The filing of this Information Disclosure Statement shall not be construed as an admission that the information cited is, or is considered to be, material to patentability as defined

in § 1.56(b). It is believed that no additional fees are required. Should any other fee be required, however, please charge such fee to Deposit Account No. 23-3030, but not to include any payment of issue fees.

Respectfully submitted,

By /Blake R. Hartz, Reg. No. 73453/
Blake R. Hartz, Reg. No. 73453
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
Telephone: (317) 634-3456 Fax: (317) 637-7561
Email: bhartz@uspatent.com



- (51) **International Patent Classification:**
H04L 29/12 (2006.01) *H04W 76/02* (2009.01)
- (21) **International Application Number:**
PCT/IB2013/001660
- (22) **International Filing Date:**
30 July 2013 (30.07.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/677,079 30 July 2012 (30.07.2012) US
- (71) **Applicant:** TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; S-164 83 Stockholm (SE).
- (72) **Inventors:** HUANG, Kaiyuan; 603 March Road, Kanata, Ontario K2K 2M5 (CA). RAYMENT, Stephen; 1604-95 Bronson Avenue, Ottawa, Ontario K1R 1E2 (CA). ROELAND, Dinand; Skinnarasvagen 39, S-19275 Sollentuna (SE). ROMMER, Stefan; Skogstrydsgatan 7, S-42674 Vastra Frolunda (CA).
- (74) **Agent:** BAUER, Richard, P.; Katten Muchin Rosenman LLP, 2900 K Street NW, Suite 200, North Tower, Washington, DC 20007-5118 (US).

- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

[Continued on next page]

- (54)
- Title:**
- METHOD AND SYSTEM FOR PROVIDING MULTIPLE SERVICES OVER WLAN

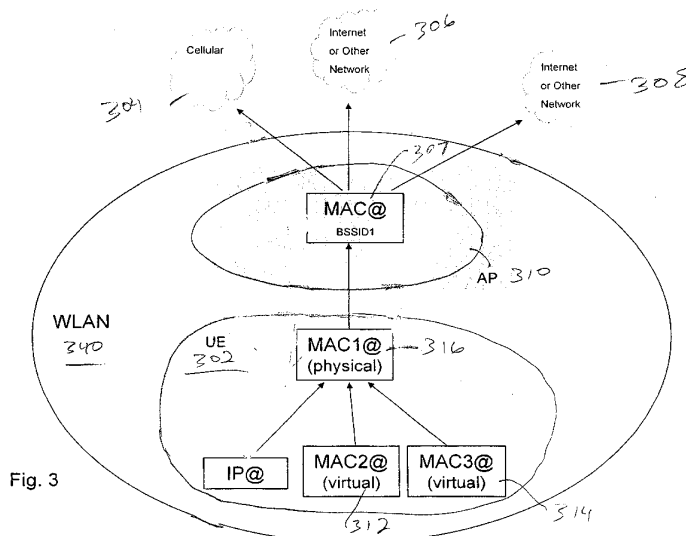


Fig. 3

- (57) **Abstract:** A system and method of providing, to a client, access to multiple packet data networks (PDNs), each PDN providing a dedicated PDN connection is disclosed. The client is provided with a number of virtual MAC addresses. Each of the virtual MAC addresses is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the packet data networks. One of the virtual MAC addresses is then delivered via a 4 address MAC frame when the client is communicating with the associated data service. The client may be a Wi-Fi client communicating with the associated data service over a cellular data network.



-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND SYSTEM FOR PROVIDING MULTIPLE SERVICES OVER WLAN

[0001] This application claims priority to U.S. Provisional Patent Appln. No. 61/677,079, filed July 30, 2012, the contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present application relates generally to WLAN access to a cellular network, more specifically, to providing multiple virtual services over a WLAN interface.

BACKGROUND OF THE INVENTION

[0003] A need exists to provide multiple concurrent services over WLAN (Wireless Local Area Network). For example when WLAN is used to provide access to cellular data networks, it is desirable to provide access to multiple PDNs (Packet Data Networks). This capability is currently done on 3G/4G networks where, e.g., IMS (IP Multimedia Subsystem) and Internet access can be simultaneously provided. Each of these services is identified via their APNs (Access Point Name). It is the name of a network, where a network in 3GPP terminology is called Packet Data Network (PDN). In the 3GPP core network, there is a gateway called PGW (Packet Data Network Gateway). This is a PDN GW; i.e. a gateway towards one or more PDNs. Between the UE (User Equipment; e.g., Wi-Fi client) and PGW(s) one or more “PDN connections” are setup. Each PDN connection is a virtual point-to-point link from a UE to a PDN. A UE initiates the setup of a PDN connection. When it does that, it may include an APN. Each PDN connection has one IP address. As each PDN may have its own IP address range, it can occur that two PDN connections to different PDNs get the same IP address. Herein, the term “PDN” may be used for a “PDN connection.” Thus, the IP address spaces for each of the different services may overlap, making IP address resolution of the services impossible. What is needed is a means to provide multiple virtual point-to-point links between the device and one or more PDNs.

[0004] Other approaches have been proposed to solve this problem, including running VLANs (Virtual Local Area Networks, e.g., IEEE 802.1Q) over WLAN, and performing tunneling over WLAN (using e.g. GRE - Generic Routing Encapsulation). The approach described below is potentially simpler to implement than the alternatives, reducing device cost and power consumption and the basic frame structure is already implemented in some existing devices.

SUMMARY OF THE INVENTION

[0005] The present invention is directed to alleviating the problems of the prior art. In particular, the present invention proposes to use the IEEE 802.11 WDS (Wireless Distribution System) four-address frame format to segregate multiple virtual services over a single WLAN interface.

[0006] According to one aspect of the present invention, a method provides to a client access to multiple packet data network (PDN) connections – preferably over WLAN, each PDN providing a dedicated PDN connection (e.g., Skype, Netflix, etc.), a single PDN capable of providing multiple services. The client (e.g., User Equipment (UE) such as a cell phone) is provided with a number of virtual MAC (Media Access Control) addresses. Each of the virtual MAC addresses is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the PDNs. One of the virtual MAC addresses is then provided via a 4 address MAC frame for the client to communicate with the associated data service. When communicating with a data service via a PDN connection, the virtual MAC address associated with the PDN connection is then included in a 4 address MAC frame.

[0007] In a preferred embodiment, the client is a Wi-Fi client, and the Wi-Fi client is communicating with the associated data service over a cellular data network.

[0008] According to another aspect of the present invention, apparatus providing to a client, access to a plurality of PDNs, each PDN providing a dedicated PDN connection, includes an

Access Point (AP) configured to communicate with (i) the client and (ii) the plurality of PDNs. The AP may be configured to provide the client a plurality of virtual MAC addresses, and to assign each of the virtual MAC addresses to a dedicated PDN connection, where each dedicated PDN connection is associated with one of the PDNs. The AP is further configured to provide one of the virtual MAC addresses via a 4 address MAC frame for the client to communicate with the associated data service. In alternative embodiments, the virtual MAC addresses may be (i) pre-loaded onto the UE (User Equipment, e.g., a cell phone) as pre-configured global MACs (e.g., for each data service), (ii) administered by the network (fixed or 3GPP (3rd Generation Partnership Project) AAA (Authentication, Authorization and Accounting protocol)) and sent to UE at authentication, and/or (iii) negotiated dynamically when the UE needs it (e.g. based on ARP (Address Resolution Protocol)). In alternatives (ii) and (iii), the virtual MAC addresses may be supplied to the UE through the AP.

[0009] According to a further aspect of the present invention, at least one computer-readable, non-transitory medium is provided, which contains program code which, when loaded into one or more processors of an AP, causes the one or more processors to provide to a client access to a plurality of PDNs, where each PDN provides a dedicated PDN connection. The program code causes the one or more processors to provide the client a plurality of virtual Media Access Control (MAC) addresses; where each of the virtual MAC addresses corresponds to a dedicated PDN connection, each dedicated PDN connection being associated with one of the PDNs; and deliver one of the virtual MAC addresses via a 4 address MAC frame for the client to use when the client is communicating with the associated data service.

[0010] Other aspects and features of the present invention will become apparent to those of ordinary skill in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1a is a diagram illustrating the general 802.11 frame format;

[0012] Fig. 1b is a diagram illustrating the 802.11 frame format in accordance with the preferred embodiments;

[0013] Fig. 2 is a diagram illustrating a typical use of the known 802.11 address format frame in a wireless bridge;

[0014] Fig. 3 is a block diagram illustrating links between a UE and a Trusted WLAN Access Gateway (TWAG) according to an embodiment of the invention;

[0015] Fig. 4 is a schematic block diagram of the structure according to the preferred embodiments;

[0016] Fig. 5 is a functional flow chart illustrating how the four-address MAC header is used for communication between a UE and a PDN;

[0017] Fig. 6 is a flow chart of a preferred process according to the present invention;

[0018] Fig. 7 is a process diagram of an initial attachment in WLAN on GTP (GPRS Tunneling Protocol) S2a;

[0019] Fig. 8 is a process diagram of UE-Initiated connectivity to additional PDN in WLAN on GTP S2a;

[0020] Fig. 9 is a process diagram of a handover procedure between 3GPP access and WLAN on S2a;

[0021] Fig. 10 is a process diagram of a handover from WLAN on GTP S2a to 3GPP access;

[0022] Fig. 11 is a process diagram of a UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN;

[0023] Fig. 12 is a process diagram of a PDN GW Initiated Bearer Deactivation with GTP on S2a.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0024] In order to lighten the following description, the following acronyms will be used herein:

Table 1

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting protocol
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AP	Access Point
APN	Access Point Network
ARP	Address Resolution Protocol
BNG	Broadband Network Gateway
BSSID	Basic Service Set Identifier
DA	Destination Address
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol

EPC	Evolved Packet Core
EPS	Evolved Packet System
FFS	For Further Study
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
hPCRF	Home network Policy Control and Charging Rules Function
HPLMN	Home Public Land Mobile Network
IMSI	International Mobile Subscriber Identity
IP-CAN	IP Connectivity Access Network
LBO	Local Breakout
MAC	Media Access Control
NSWO	Non Seamless WLAN Offload
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PMIPv6	Proxy Mobile IP version 6
QoS	Quality of Service
RA	Receiver Address
S2a	Trusted non-3GPP interface to EPC
SA	Source Address
SaMOG	S2a-based Mobility over GTP

SDO	Standard Development Organization
TA	Transmitter Address
TEID	Tunnel Endpoint ID
TWAG	Trusted WLAN Access Gateway
UE	User Equipment
vPCRF	Visited network Policy Control and Charging Rules Function
VPLMN	Visited Public Land Mobile Network
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network
WLCP	WLAN Control Protocol

[0025] In overview, the present invention proposes a solution for SaMOG (S2a-based Mobility over GTP) phase 2. For the first PDN connection, additional information elements are proposed to be added to EAP-AKA (Extendible Authentication Protocol - Authentication and Key Agreement). These information elements may carry e.g. handover indicator or APN. For additional PDN connections, traffic may be separated on a per-PDN connection basis using four MAC addresses in the 802.11 frame. A control protocol may be used to setup and teardown additional PDN connections.

[0026] Typically, the first PDN/NSWO (Non Seamless WLAN Offload) connection over WLAN uses the per-UE point-to-point link as defined in TS 23.402 clause 16. Standard IEEE 802.11 messaging is used over the Wi-Fi air link. As defined in IEEE 802.11-2007 section 7.2.2, a normal data frame uses three address fields. E.g. for an uplink frame (To DS=1 and From DS=0 in table 7-7 of IEEE 802.11-2007):

Address #1 is the receiving address (RA) and equals the BSSID of the AP;

Address #2 is the transmitting address (TA) and equals the source address (SA) which equals the MAC address of the UE;

Address #3 is the destination address (DA) and equals the MAC address of the TWAG (Trusted WLAN Access Gateway).

The MAC header also defines an address #4 which is normally not used.

[0027] To achieve a per-UE-and-PDN point-to-point link for additional PDN/NSWO connections, all four address fields in the MAC data frame header are used in accordance with the present invention. Frames are sent/received with header fields To DS=1 and From DS=1 as defined in table 7-7 of IEEE 802.11-2007. E.g. for an uplink frame:

Address #1 is RA and equals the BSSID of the AP;

Address #2 is TA and equals the physical MAC address of the UE;

Address #3 is DA and equals the MAC address of the TWAG;

Address #4 is SA and equals a virtual MAC address of the UE.

[0028] In the present invention, for each additional PDN connection, there is a virtual MAC address on the UE. This address is preferably unique within the scope of the UE. A virtual MAC address combined with the physical MAC address of the UE provides a globally unique identification for a PDN/NSWO connection. The TWAG and the UE can use this identification to correlate a packet to the correct PDN/NSWO connection.

[0029] Preferably, the 4-address MAC frame is used only over the Wi-Fi air link. Between the access point and TWAG, standard (wired) Ethernet frames are used. For an additional PDN connection, the UE virtual MAC address may be used between the access point and TWAG. The solution may be: (1) In the downlink, the AP preferably is able to know which physical MAC belongs to a virtual MAC. This may be a new AP requirement. It may learn this from uplink packets, though. (2) If the physical MAC is not used between AP and TWAG, but only use the virtual MAC, then the virtual MAC should be unique within the scope of a TWAG. So, some kind of MAC negotiation mechanism can be used. This could be

done with the control protocol in the next section. Alternatively, some other mechanism e.g. VLANs between AP and TWAG may be used.

[0030] WLCP (WLAN Control Protocol) is a new protocol (related to SaMOG). The details are to be defined in Wi-Fi Alliance or 3GPP. WLCP could use the 4-address field as well; e.g. a dedicated virtual MAC is used to denote WLCP packets. The WLCP packets may be defined by Wi-Fi Alliance or stage 3 in 3GPP. A WLCP packet may e.g. indicate “attach” including APN and handover indicator.

[0031] Fig. 1a, is a diagram which illustrates the general format of the 802.11 MAC frame format. The MAC frame format comprises a set of fields that occur in a fixed order in all frames. There are three address fields in the MAC frame format, four when the ad hoc or the Wireless Distribution System (WDS) mode is being used. These fields are used to indicate the basic service set identifier (BSSID), source address, destination address, transmitting station address, and receiving station address. The usage of the four address fields in each frame type is indicated by the abbreviations BSSID, Destination Address (DA), Source Address (SA), Receiver Address (RA), and Transmitter Address (TA).

[0032] Fig. 1b, is a diagram which illustrates the format of the 802.11 4-address MAC frame format according to the preferred embodiments. It is similar to Fig. 1a, but specifies that the fourth MAC address is a virtual MAC address.

[0033] In Fig. 2, a LAN 1 (200) has a Station 1 (202), a Station 2 (204), an AP 1 (206), and UE (208), which communicates with at least one of antennas (210) and (212). A second LAN 2 (220) has a Station 3 (222), a Station 4 (224), an AP 2 (226), and antennas (230) and (232). LAN 1 communicates with LAN 2 over WDS link (240), using an 802.11 4-address format frame (280) according to the ad hoc or WDS modes. LAN1 and LAN 2 operate with 802.3 Ethernet Frames (250) and (252), respectively. LAN 1 can communicate with a cellular network (260) and/or an Internet or other network (270). Each of the Stations, APs, and UEs includes one or more processors, ROM storing program code for carrying out the

functions described herein, RAM, typical interfaces, transmitters/receivers, antennas, power supplies, etc. The UE may, for example, be a hand-held portable device such as a cellular telephone, smart phone, pad device, Personal Data Assistant, laptop computer, etc.

[0034] In Fig. 2, the four-address format frame (280) may be used to direct information over the WDS link (240). In this case, the four-address format frame (280) comprises the MAC address of Station 1 (202), the MAC address of Access Point 1 (206), the MAC address of Access Point 2 (226), and the MAC address of Station 3 (222). These are included in the 802.11 frame header. The frame data of (280) is the same as the original Ethernet frame (250). Based on information in this four-address format frame (280), the original Ethernet frame (250) will be reconstructed.

[0035] In the prior art, the UE typically can have only a single connection over the WLAN. The UE will not be able to concurrently access more than one PDN connection. As indicated earlier, when the WLAN is used to provide access to cellular data networks, it is desirable to provide access to multiple PDNs (packet data networks). As will be described further below, in the preferred embodiments, the IEEE 802.11 WDS (Wireless Distribution System) four-address frame format (280) is used to segregate multiple virtual services over a single WLAN interface. A four-address format currently may be used to create wireless repeater products, where one pair of addresses defines the ultimate source and destination address, and the other pair defines the next hop address. In the preferred embodiments on the other hand, the format is modified to enable multiple virtual services to be associated with multiple virtual addresses.

[0036] Fig. 3 shows the basic architecture of a wireless distribution system that illustrates how a UE can access multiple services according to the preferred embodiments of the present invention. In Fig. 3, MAC2@ and MAC3@ each are associated with an IP@. Thus, there are a total of three IP addresses in Fig. 3. The figure illustrates how a Wi-Fi client, such as a mobile device UE (302) can connect to a Trusted WLAN Access Gateway Cellular Network

(304), or Internet or other network (306) and/or (308), via an Access Point (310) in order to obtain access to additional services through the WLAN 340.

[0037] The Wi-Fi client (302) is provided access to multiple packet data networks (PDNs) via a cellular data network (304), where each PDN provides a dedicated PDN connection. More specifically, the Wi-Fi client (302) is provided with a number of virtual MAC addresses (312) and (314). Each virtual MAC address (312) and (314) is assigned to a dedicated PDN connection and each dedicated PDN connection is associated with one of the packet data networks. The Wi-Fi client's virtual MAC address for the requested data service is then delivered via a 4 address MAC frame (inner address) when the Wi-Fi client (302) is communicating with the associated data service over the cellular data network (304).

[0038] For an upstream frame (device to network), the receiver address is the wireless access point (310) address MAC BSSAD1 (307; outer address), and the destination address is the wireless access gateway address, while the transmitter address is the device (302) physical address (316) and the source address is the device (302) virtual address (312; inner address) and/or (314; inner address). For a downstream frame (network to device), the transmitter address is the access point (310) address and the source address is the wireless access gateway, while the receiver address is the device (302) physical address (316) and the destination address is the device (302) virtual address (312) and/or (314).

[0039] Fig. 4 is a schematic block diagram of the structure according to the preferred embodiments. The UE may comprise a cellular telephone (402) having an antenna (404) which wirelessly communicates with a first antenna (454) of an AP (450). The cellular telephone (402) also has one or more CPUs (406), a ROM (408), a RAM (410), a bus (412), an antenna interface (414), a transmitter/receiver (416; which may be separate or combined circuitry), and a power supply (418). The AP has a one or more CPUs (456), a ROM (458), a RAM (460), a bus (462), a first antenna interface (456), a first transmitter/receiver (462; which may be separate or combined circuitry), and a power supply (458). The AP (450) also has a second antenna (470) for communicating with one or more dedicated Networks (480)

and (482). A second interface (472) is coupled the second antenna (470), and a second transceiver (474) is coupled to the second interface (472). A third interface (490) may, for example, be coupled to a wired network via wiring (492).

[0040] For single APN connections, only the transmitter address and the receiver address will be used on the upstream and downstream respectively. The need to use multiple PDN connections is indicated when the device initially connects to the network, or when an additional APN is needed, by using, e.g. extensions to EAP (Extensible Authentication Protocol) or DHCP (Dynamic Host Control Protocol). In this case the source and destination address fields will be used instead of transmitter and receiver.

[0041] For a first PDN connection, the normal Wi-Fi MAC address format is used. No change is necessary compared to unmodified UE. The 4-MAC address MAC format is then used between UE and AP for additional PDN connections. The 4-MAC frame in the upstream, i.e. between UE and AP will comprise:

RA (Receiver Address) = AP BSSID

TA (Transmitter Address) = UE MAC@1 (physical)

DA (Destination Address) = TWAG

SA (Source Address) = UE MAC@2 (virtual; for 2nd PDN connection).

[0042] On the downstream side, that is between the AP and UE, the 4-MAC frame format will comprise:

RA (Receiver Address) = UE MAC@1 (physical)

TA (Transmitter Address) = AP BSSID

DA (Destination Address) = UE MAC@2 (virtual)

SA (Source Address) = TWAG.

Where, e.g., MAC@1 is an abbreviation for MAC Address 1.

[0043] Now, between the AP and the TWAG, normal addressing is used; e.g. using UE MAC@2 for the 2nd PDN connection. The virtual MAC addresses may assigned to the UE by:

- Pre-configured global MACs loaded into the UE at the factory or a UE provisioning facility (e.g., wireless provider store);
- Administered by a network (fixed or 3GPP (AAA) and sent to the UE at authentication (perhaps limited to a max number of PDN connections); and/or
- Negotiated dynamically when the UE needs it (e.g. by means of the previously mentioned WLCP, or based on ARP (Address Resolution Protocol)).

[0044] Fig. 5, is a functional flow diagram illustrating how the 4-address MAC header is used in the establishment of an additional PDN connection in the preferred embodiments.

[0045] For authentication (EAP and 802.1X) and for the first PDN connection, the UE uses its first MAC address and normal Wi-Fi MAC frame for addressing. This way, an easier UE implementation can be achieved when only a single PDN connection is used.

[0046] For an additional PDN connection, the UE uses another virtual MAC address. All signaling over Wi-Fi is done using the 4-address MAC frame. For PDN connections, DHCP extensions may be used (when DHCP is the control plane protocol) to indicate handover and a non-default APN. Downlink frames are always sent L2 (Layer 2) unicast (including e.g. RA and IP multicast). The 4-address MAC frames use the same encryption over Wi-Fi as the normal MAC frames.

[0047] Fig. 6 is a flow chart of a preferred process according to the present invention. These functions are preferably carried out in the AP, using one or more processors therein, together with memory storing program code to carry out the described functions. The process provides the UE access to a plural PDNs, where each PDN provides a dedicated PDN

connection. The process begins at step (602), and at step (604) the AP allocates the UE a plurality of virtual MAC addresses. At step (606), the AP assigns each of the virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of the PDNs. At step (608), the AP delivers one of the virtual MAC addresses via a 4 address MAC frame when the UE is communicating with the associated data service.

[0048] Fig. 7 is a process diagram of an initial attachment in WLAN on GTP (GPRS Tunneling Protocol) S2a for roaming, LBO (Local Breakout), and non-roaming scenarios. The procedure is as in 3GPP TS (Technical Specification) 23.402 clause 16.2.1 with the following additions:

Step 1. Optionally, in order to optimize network selection, the network may indicate its capabilities (support for handover, support for attach to non-default APN, support for non-seamless WLAN offload, support for EPC-routed traffic, support for attach to multiple PDN connections). Preferably, it is FFS if these capabilities are specified by 3GPP or by another SDO.

Step 2. The UE indicates initial attach in EAP to the 3GPP AAA. The UE preferably indicates whether it requests EPC (Evolved Packet Core) access or non-seamless WLAN offload in EAP to the 3GPP AAA. If the UE requests EPC access, it may indicate APN. As part of step 2, the 3GPP AAA sends these indicators to the TWAN. If the UE indicates EPC access without indicating APN, then the EAP reply indicates the selected default APN. As part of step 2, the UE indicates its capabilities (support for handover, support for attach to non-default APN, support for attach to multiple PDN connections). The network indicates its capabilities (support for handover, support for attach to non-default APN, support for non-seamless WLAN offload, support for EPC-routed traffic, support for attach to multiple PDN connections) to the UE.

Step 3. If the UE indicated an APN in the previous step, the TWAN verifies that it is allowed by subscription, selects the PDN GW for the APN correspondingly, and includes the APN in the Create Session Request.

[0049] Fig. 8 is a process diagram of UE-Initiated connectivity to an additional PDN in WLAN on GTP S2a. Establishment of an additional PDN/NSWO connection over WLAN with GTP S2a is supported only for the accesses that support such feature and for the UEs that have such capability.

[0050] This procedure is related to the case when the UE has an established a PDN/NSWO connection over WLAN and wishes to establish one or more additional PDN/NSWO connections over such access. This procedure is also used to request for connectivity to an additional PDN/NSWO connection over WLAN when the UE is simultaneously connected to such access and a 3GPP access, and the UE already has active PDN/NSWO connections over both the accesses. The UE establishes a separate point-to-point link to the TWAG for each additional PDN/NSWO connection.

[0051] There can be more than one PDN connection per APN when GTP is used between the TWAN and the PDN GW. During the establishment of a new PDN connection, the TWAN allocates and sends a default S2a bearer ID to the PDN GW. The default S2a bearer ID is unique in the scope of the UE within a TWAG, i.e. the IMSI (International Mobile Subscriber Identity) and the default S2a bearer ID together identify a PDN connection within a TWAG. In order to be able to identify a specific established PDN connection, both the TWAG and the PDN GW preferably store the default S2a bearer ID. The establishment of an additional PDN/NSWO connection should not impact the first PDN/NSWO connection. As a separate point-to-point link is used for each additional PDN/NSWO connection, traffic separation can be achieved between all PDN/NSWO connections including the first.

Step 1. The UE triggers the establishment of a new PDN/NSWO connection by means of WLCP. This step establishes the setup of a new per-UE-and-PDN-connection point-to-point link to the TWAG. The UE preferably indicates whether it requests EPC access or non-seamless WLAN offload. If the UE requests EPC access, it may indicate APN. The UE preferably triggers the re-establishment of an existing PDN/NSWO connectivity by providing a handover indicator.

Step 2. Upon establishment of an additional PDN/NSWO connection, steps 9-15 as described in clause 8.2.x.2.1.1 are performed. As part of these steps, the TWAN performs PDN GW selection as described in TS 23.402. Steps 9-15 are preferably executed with PDN GW2 instead of PDN GW1. Unless non-seamless WLAN offload was selected in step 1, steps 10-14 in clause 8.2.x.2.1.1 are preferably always performed.

[0052] Fig. 9 is a process diagram of a handover procedure between 3GPP access and WLAN on S2a. The home routed roaming, LBO and non-roaming scenarios are depicted in Fig. 9. In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN (Home Public Land Mobile Network) to the PDN GW in the VPLMN (Visited Public Land Mobile Network) and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy preferably are not involved, except for the authentication and authorization in step 2.

[0053] For connectivity to multiple PDNs the following preferably applies:

If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 15 are preferably skipped and the UE preferably only perform step 16 for each PDN connection that is being transferred from 3GPP access.

If the UE is connected only to 3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 15 are preferably performed. In these steps the UE preferably provides an APN corresponding to one of the PDN connections that are being transferred from 3GPP access. The UE preferably then repeats step 16 for each of the remaining PDN connections that are being transferred from 3GPP access.

Step 17 is preferably repeated for each PDN connection that is being transferred from 3GPP access.

Step 16 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in TS 23.402 clause 8.1.

[0054] The steps in Fig. 9 are based on Fig. 8, with the following changes:

Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.

Step 2. As step 2 in Fig. 8 with the following addition: The UE preferably indicates handover via EAP to 3GPP AAA.

Steps 3 and 10. As step 2 in Fig. 8 with the following addition: The handover indication is preferably set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF (Policy and Charging Enforcement Function)-Initiated IP-CAN (IP Connectivity Access Network) Session Modification Procedure with the PCRF (Policy and Charging Rules Function).

Step 4 and 11. The PDN GW preferably executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [xx]. The Event Report indicates the change in Access Type. If the PDN GW decided to allocate a new IP address/prefix instead of preserving the old IP address/prefix, as described in TS 23.402 clause 4.1.3.2.3, the PDN GW executes an IP-CAN session Establishment Procedure with the PCRF instead of a PCEF-Initiated IP-CAN Session Modification Procedure.

Step 6 and 13. The PDN GW preferably responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID (Tunnel Endpoint ID) of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS (Evolved Packet System) Bearer Identity, EPS Bearer QoS (Quality of Service), APN-AMBR (Aggregate Maximum Bit Rate), Charging ID, Cause). The Create Session Response preferably contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access. The Charging Id provided by the PGW is preferably the Charging ID previously assigned to the default bearer of the PDN connection in the 3GPP access.

Step 16. For connectivity to multiple PDNs simultaneously or nearly-simultaneously, the UE preferably establishes connectivity to each PDN that is being transferred from 3GPP access, besides the PDN connection that was established in the

previous steps, by executing the UE-initiated Connectivity to Additional PDN procedure specified above.

Step 17. The PDN GW preferably initiates the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in TS 23.402 clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [xx], clause 5.4.4.1.

[0055] Fig. 10 is a process diagram of a handover from WLAN on GTP S2a to 3GPP access for roaming, LBO and non-roaming scenarios, according to the present invention. This procedure is preferably as in TS 23.402 clause 8.2.1.1/8.2.1.2 with the following differences:

Step 1. There is preferably a GTP tunnel between TWAN and PGW.

Step 18. The PDN GW preferably initiates resource allocation deactivation procedure in the TWAN as discussed above.

[0056] Fig. 11 is a process diagram of a UE/TWAN-initiated PDN disconnection procedure with GTP S2a in WLAN. If the UE has a single PDN/NSWO connection established over WLAN, this procedure is preferably the same as TS 23.402 clause 16.3.1.1. If the UE has multiple PDN/NSWO connections established over WLAN, this clause preferably applies to UE/TWAN-requested PDN disconnection procedure. For multiple PDN/NSWO connectivity, this disconnection procedure is preferably repeated for each PDN/NSWO connection.

[0057] The procedure outlined in Fig. 11 preferably applies to the Non-Roaming, Home Routed Roaming, and Local Breakout cases. In the Local Breakout case, the vPCRF preferably forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy preferably serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is preferably not involved.

[0058] If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF preferably do not occur. Instead, the PDN GW may employ static configured policies.

Step 1. The UE may initiate disconnection of the PDN/NSWO connection by means of WLCP.

Step 2. The TWAN preferably releases the PDN connection and sends a Delete Session Request (Linked EPS Bearer ID) message for this PDN connection to the PDN GW. In case of a NSWO connection, the TWAN preferably releases this connection and the subsequent steps preferably do not apply.

Step 3. The PDN GW preferably informs the 3GPP AAA Server of the PDN disconnection.

Step 4. The PDN GW preferably deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [x].

Step 5. The PDN GW preferably acknowledges with a Delete Session Response (Cause) message.

[0059] Fig. 12 is a process diagram of a PDN GW Initiated Bearer Resource Allocation Deactivation in WLAN with GTP on S2a. The procedure of Fig. 12 is preferably as in TS 23.402, clause 16.4.1 with the following difference: If all TWAN resources related to a PDN/NSWO connection are released, then in step 3 the UE is preferably informed of the PDN/NSWO release using WLCP.

[0060] The present invention can be realized in hardware, or a combination of hardware and software. Any kind of computing system, or other apparatus adapted for carrying out the methods described herein, is suited to perform the functions described herein. A typical combination of hardware and software could be a specialized computer system, e.g., a router, having one or more processing elements and a computer program stored on a storage medium that, when loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer

program product, which comprises all the features enabling the implementation of the methods described herein, and which, when loaded in a computing system is able to carry out these methods. Storage medium refers to any volatile or non-volatile storage device.

[0061] Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form. Computer readable medium means any non-transitory medium capable of storing program code which, when loaded into one or more processors, causes functions to be performed as described herein.

[0062] Thus, one embodiment is a computer readable medium containing computer readable instruction that, when executed by a processor, cause the processor to perform functions for maintaining clock synchronization between a first and a second radio.

[0063] All documents, specifications, clauses, etc. discussed herein are hereby incorporated into this disclosure by reference.

[0064] In addition, unless mention was made above to the contrary, it should be noted that all of the accompanying drawings are not to scale. It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described herein above. A variety of modifications and variations are possible in light of the above teachings without departing from the scope and spirit of the invention, which is limited only by the following claims.

What is Claimed Is:

1. A method of providing, to a client, access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, comprising the steps of:

assigning said client a plurality of virtual Media Access Control (MAC) addresses;

assigning each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and

providing to said client at least one of said virtual MAC addresses via a 4 address MAC frame for said client to communicate with the associated data service.

2. The method according to claim 1, wherein said client comprises a Wi-Fi client, and wherein said Wi-Fi client communicates with the associated data service over a cellular data network using the provided 4 address MAC frame.

3. The method according to claim 2, wherein the Wi-Fi client communicates with plural associated data services at the same time.

4. The method according to claim 2, wherein the communicating comprises providing an upstream 4 address MAC frame comprising:

a Receiver Address corresponding to an Access Point (AP) Basic Service Set Identifier (BSSID);

a Transmitter Address corresponding to a User Equipment (UE) MAC address1;

a Destination Address corresponding to a Trusted WLAN Access Gateway; and

a Source Address corresponding to a UE MAC address2.

5. The method according to claim 4, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

6. The method according to claim 2, wherein the communicating comprises providing a downstream 4 address MAC frame comprising:

- a Receiver Address corresponding to a UE MAC address1;
- a Transmitter Address corresponding to an AP BSSID;
- a Destination Address corresponding to a UE MAC address2; and
- a Source Address corresponding to a Trusted WLAN Access Gateway.

7. The method according to claim 6, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

8. The method according to claim 2, further comprising a second step of the client communicating with a second associated data service over the cellular data network using a second one of said virtual MAC addresses via a second 4 address MAC frame, and wherein the second step of communicating comprises providing an upstream 4 address MAC frame comprising:

- a Receiver Address corresponding to an AP BSSID;
- a Transmitter Address corresponding to a UE MAC address1;
- a Destination Address corresponding to a Trusted WLAN Access Gateway;

and

- a Source Address corresponding to a UE MAC address3.

9. The method according to claim 8, wherein the client has a first connection to a PDN, and wherein the UE MAC address3 comprises a virtual address corresponding to another PDN connection.

10. The method according to claim 9, wherein the second step of communicating comprises providing a downstream 4 address MAC frame comprising:

- a Receiver Address corresponding to a UE MAC address1;
- a Transmitter Address corresponding to an AP BSSID;
- a Destination Address corresponding to a UE MAC address3; and
- a Source Address corresponding to a Trusted WLAN Access Gateway.

11. The method according to claim 10, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to another PDN connection.

12. The method according to claim 1, wherein said Wi-Fi client comprises a cellular telephone.

13. The method according to claim 1, wherein said Wi-Fi client comprises a pad device.

14. The method according to claim 1, wherein the virtual MAC addresses are provided to the client prior to said client contacting an access point.

15. The method according to claim 1, wherein the virtual MAC addresses are provided to the client after said client contacts an access point.

16. The method according to claim 1, wherein the virtual MAC addresses are provided to the client by a network during an authentication process.

17. The method according to claim 1, wherein the virtual MAC addresses are provided to the client by a negotiation during an address resolution negotiation.

18. The method according to claim 1, wherein the virtual MAC addresses provided to the client are stored in a client memory.

19. Apparatus providing to a client, access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, comprising:
an Access Point (AP) configured to communicate with (i) the client and (ii) the plurality of PDNs, the AP further configured to:
assign said client a plurality of virtual Media Access Control (MAC) addresses;
assign each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and
provide to said client at least one of said virtual MAC addresses via a 4 address MAC frame for said client to communicate with the associated data service.

20. The apparatus according to claim 19, wherein said client comprises a Wi-Fi client, and wherein said Wi-Fi client communicates with the associated data service over a cellular data network using the provided 4 address MAC frame.

21. The apparatus according to claim 20, wherein the AP is further configured to provide the client an upstream 4 address MAC frame comprising:
a Receiver Address corresponding to an Access Point (AP) Basic Service Set Identifier (BSSID);
a Transmitter Address corresponding to a User Equipment (UE) MAC address1;
a Destination Address corresponding to a Trusted WLAN Access Gateway;
and
a Source Address corresponding to a UE MAC address2.

22. The apparatus according to claim 21, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

23. The apparatus according to claim 21, wherein the AP is further configured to provide the client a downstream 4 address MAC frame comprising:

- a Receiver Address corresponding to a UE MAC address1;
- a Transmitter Address corresponding to an AP BSSID;
- a Destination Address corresponding to a UE MAC address2; and
- a Source Address corresponding to a Trusted WLAN Access Gateway.

24. The apparatus according to claim 23, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to a second PDN connection.

25. The apparatus according to claim 19, wherein the AP is further configured to provide the client with a second one of said virtual MAC addresses via a second 4 address MAC frame for the client to communicate with another associated data service, and wherein the AP is further configured to provide to the client an upstream 4 address MAC frame comprising:

- a Receiver Address corresponding to an AP BSSID;
- a Transmitter Address corresponding to a UE MAC address1;
- a Destination Address corresponding to a Trusted WLAN Access Gateway;

and

- a Source Address corresponding to a UE MAC address3.

26. The apparatus according to claim 25, wherein the client has a first connection to a PDN, and wherein the UE MAC address3 comprises a virtual address corresponding to another PDN connection.

27. The apparatus according to claim 26, wherein the AP is further configured to provide to the client a downstream 4 address MAC frame comprising:

- a Receiver Address corresponding to a UE MAC address1;
- a Transmitter Address corresponding to an AP BSSID;
- a Destination Address corresponding to a UE MAC address3; and
- a Source Address corresponding to a Trusted WLAN Access Gateway.

28. The apparatus according to claim 27, wherein the client has a first connection to a PDN, and wherein the UE MAC address2 comprises a virtual address corresponding to another PDN connection.

29. The apparatus according to claim 19, further comprising the Wi-Fi client, which comprises a cellular telephone.

30. At least one computer-readable, non-transitory medium containing program code which, when loaded into one or more processors of an Access Point (AP) causes said one or more processors to provide to a client access to a plurality of Packet Data Networks (PDNs), each PDN providing a dedicated PDN connection, said program code also causing said one or more processors to:

- assign to said client a plurality of virtual Media Access Control (MAC) addresses;
- assign each of said virtual MAC addresses to a dedicated PDN connection, each dedicated PDN connection being associated with one of said PDNs; and
- provide to the client at least one of said virtual MAC addresses via a 4 address MAC frame when said client is communicating with the associated data service.

31. A cellular telephone, comprising:
transmitter and receiver structure configured to communicate with an access point;

a memory storing a plurality of virtual Media Access Control (MAC) addresses, each corresponding to a dedicated PDN connection; and

at least one processor configured to communicate with said access point, through said transmitter and receiver structure, using at least one of the stored virtual MAC addresses in a 4 address MAC frame.

802.11 frame: addressing

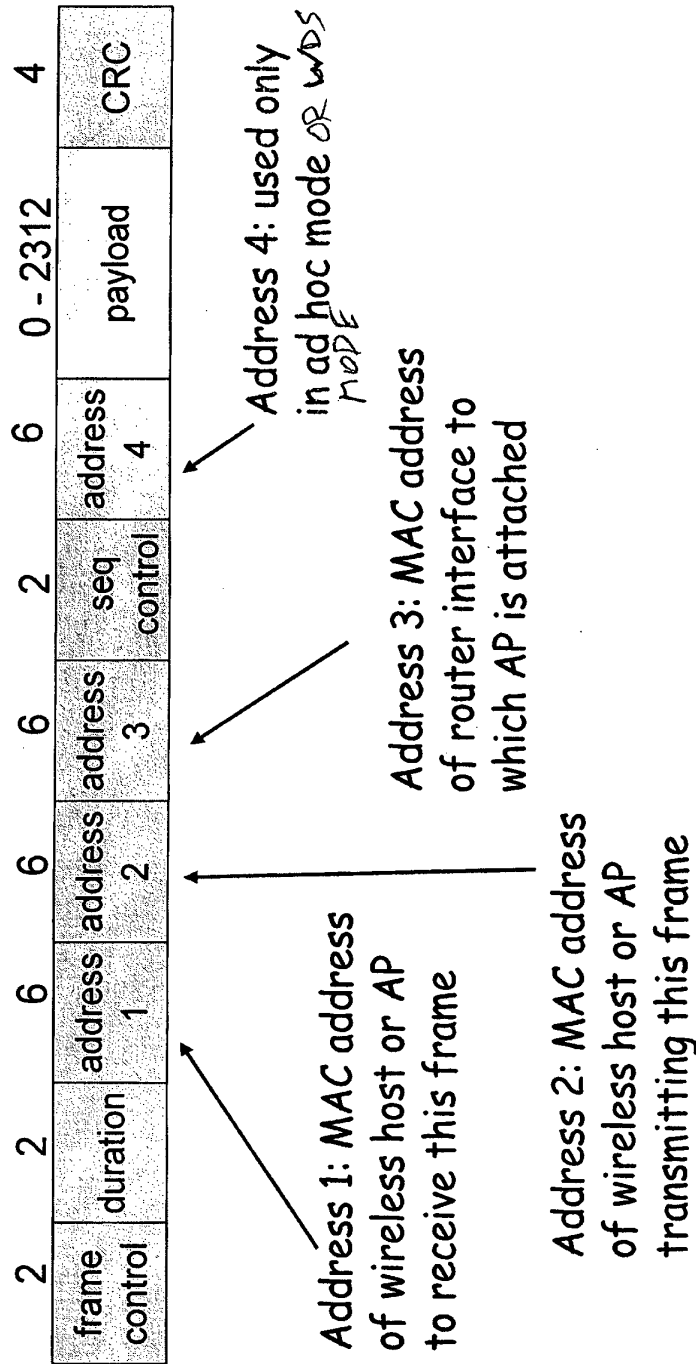


Fig. 1a

802.11 frame: addressing

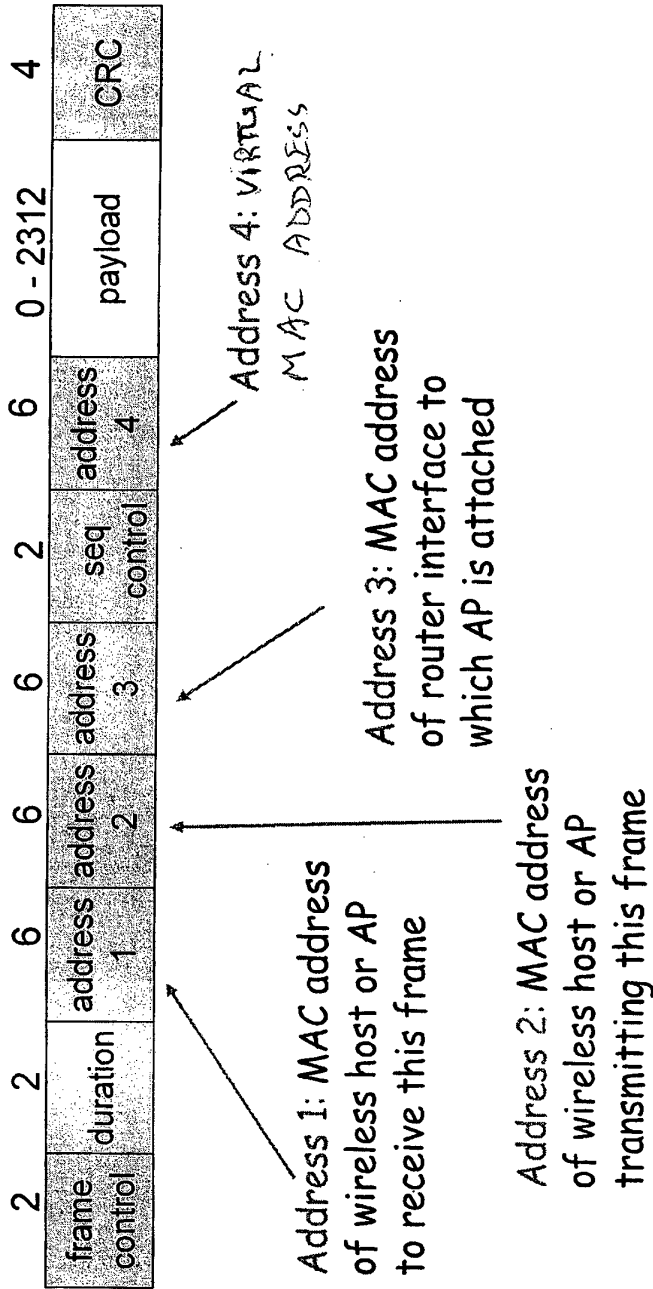


Fig. 1b

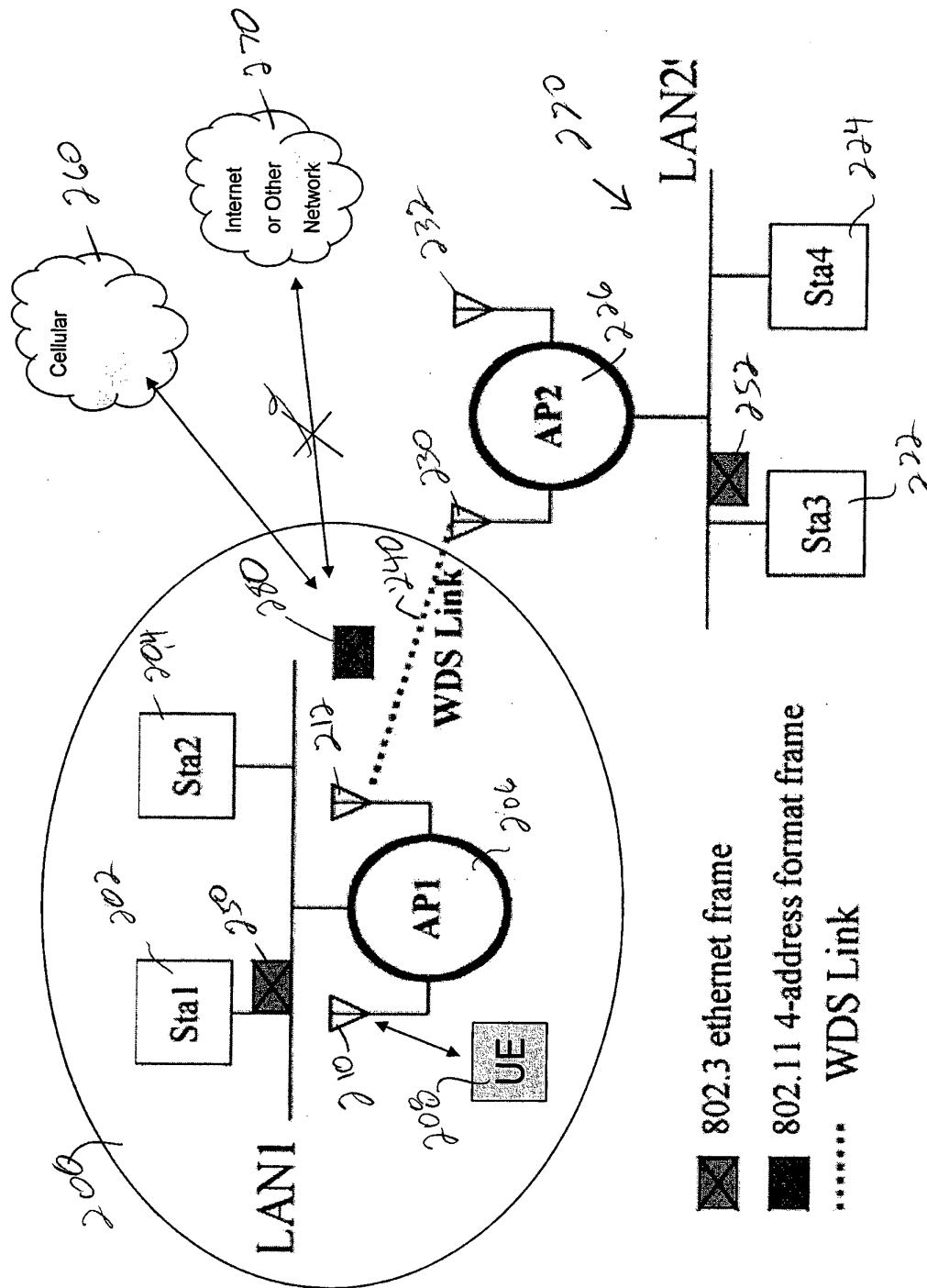


Fig. 2 PRIOR ART

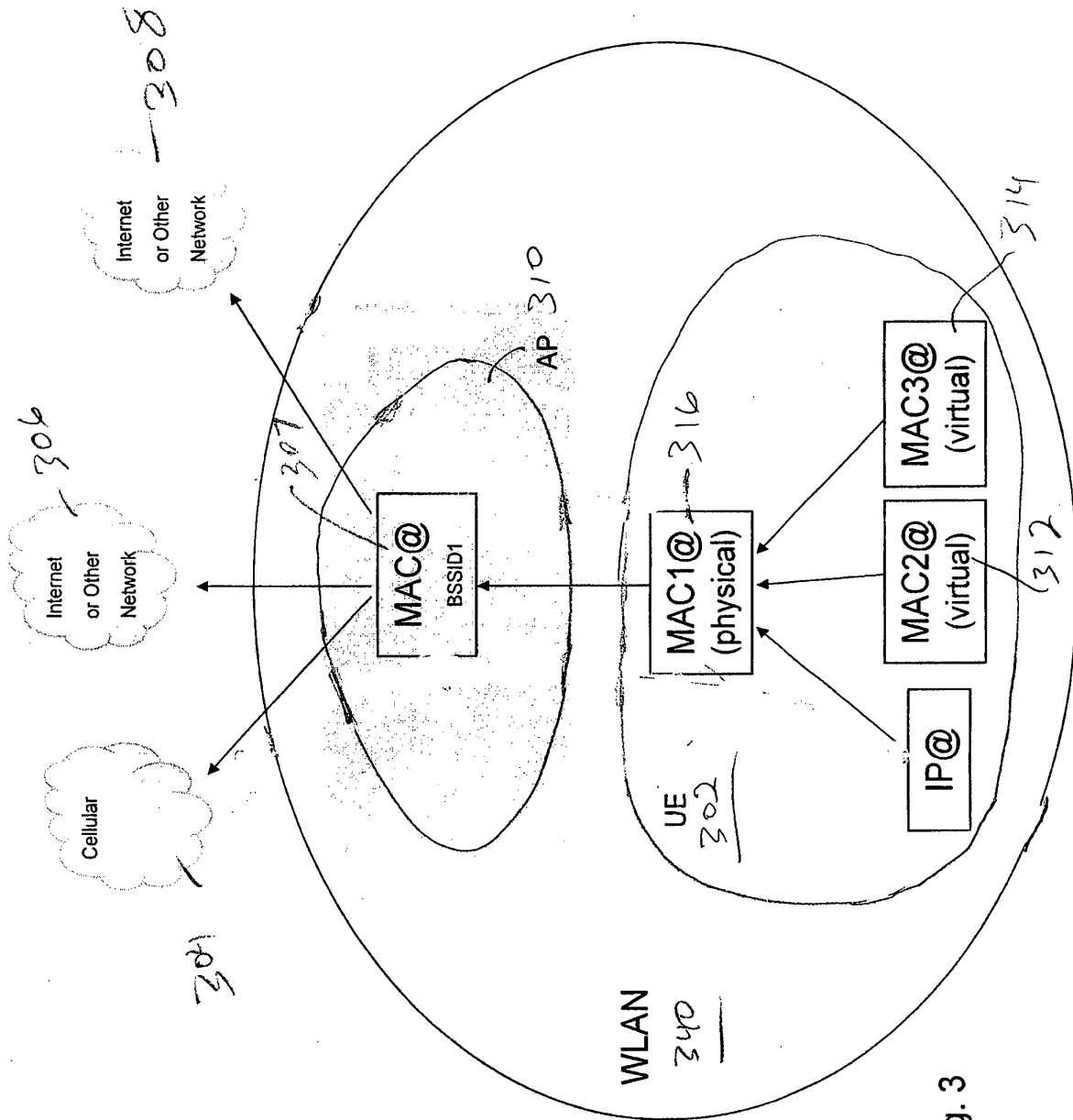


Fig. 3

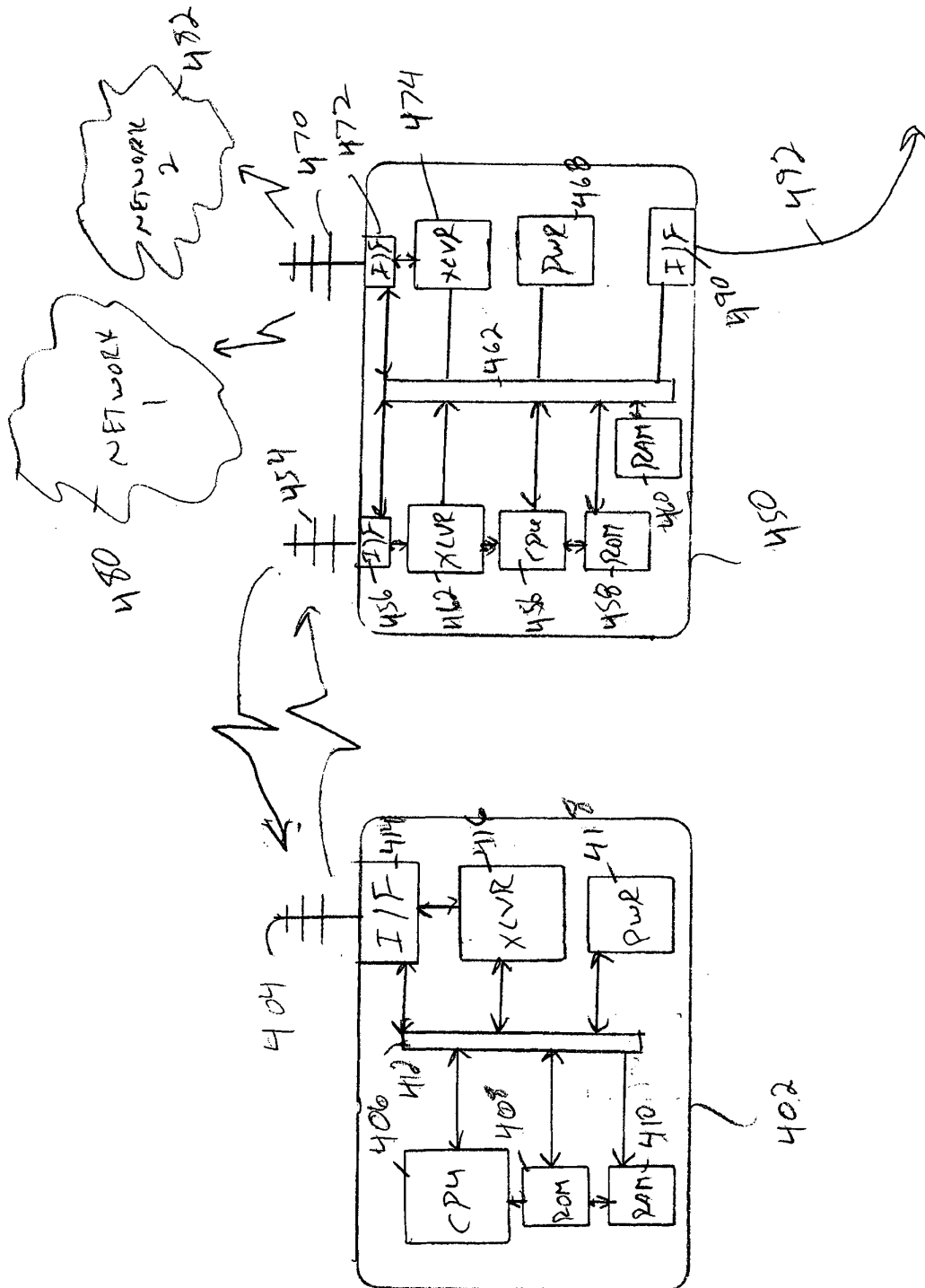


Fig. 4

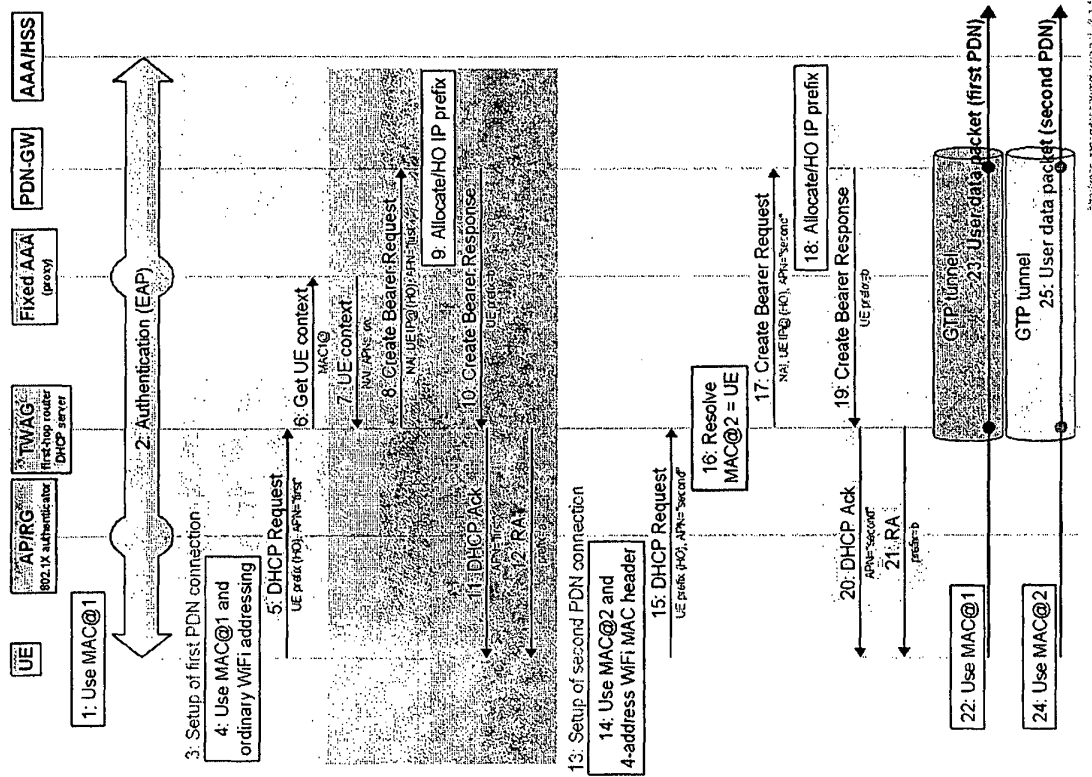


Fig. 5

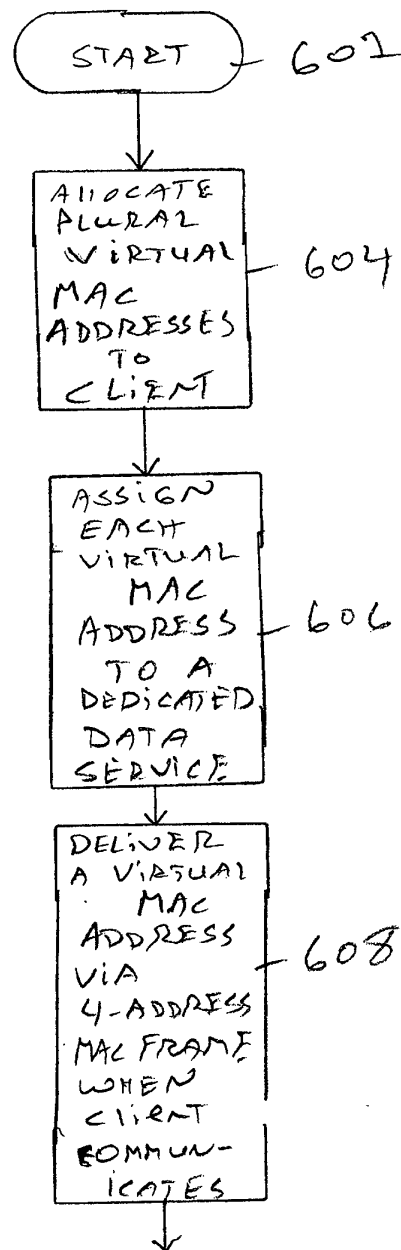


FIG. 6

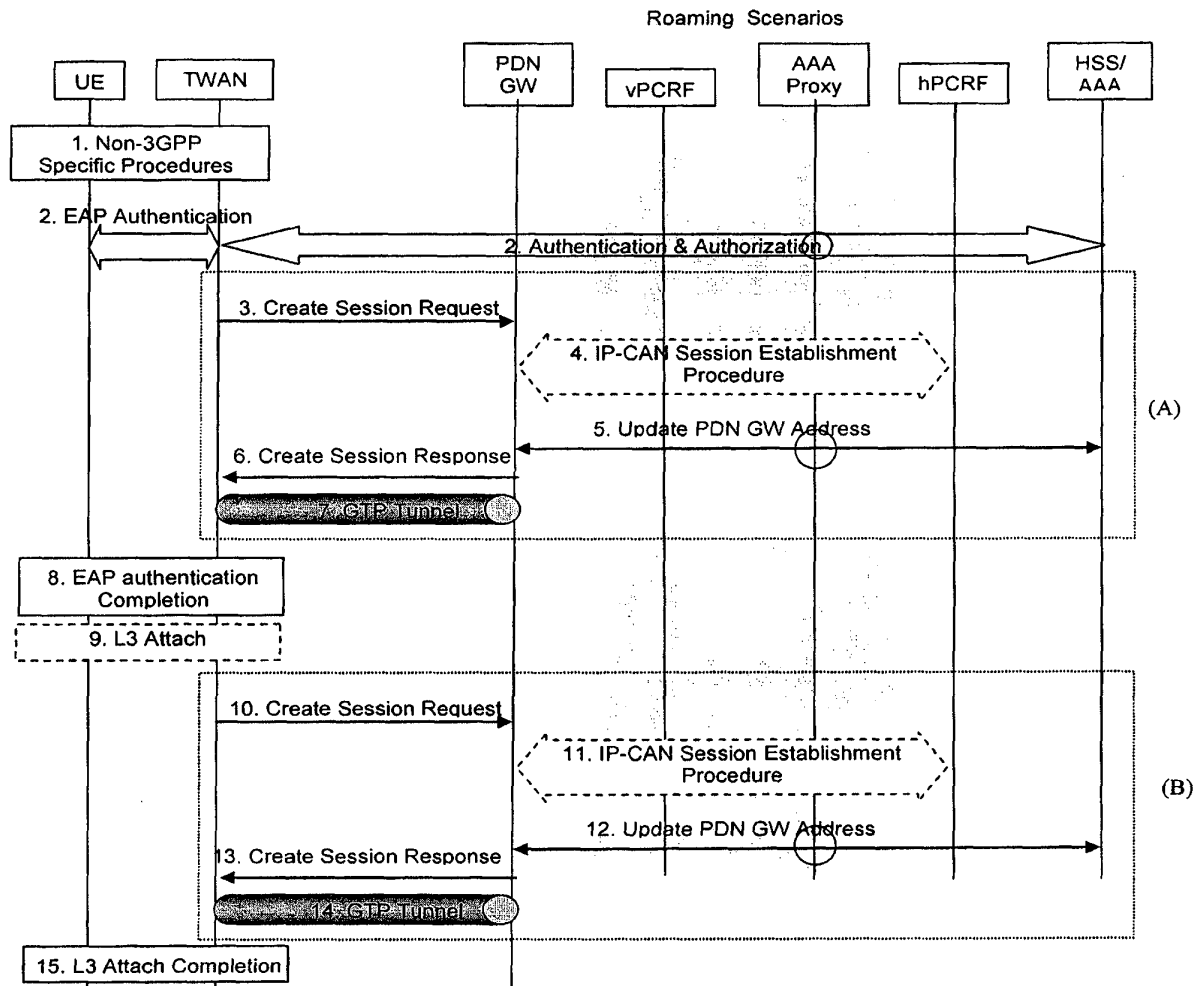


Fig. 7

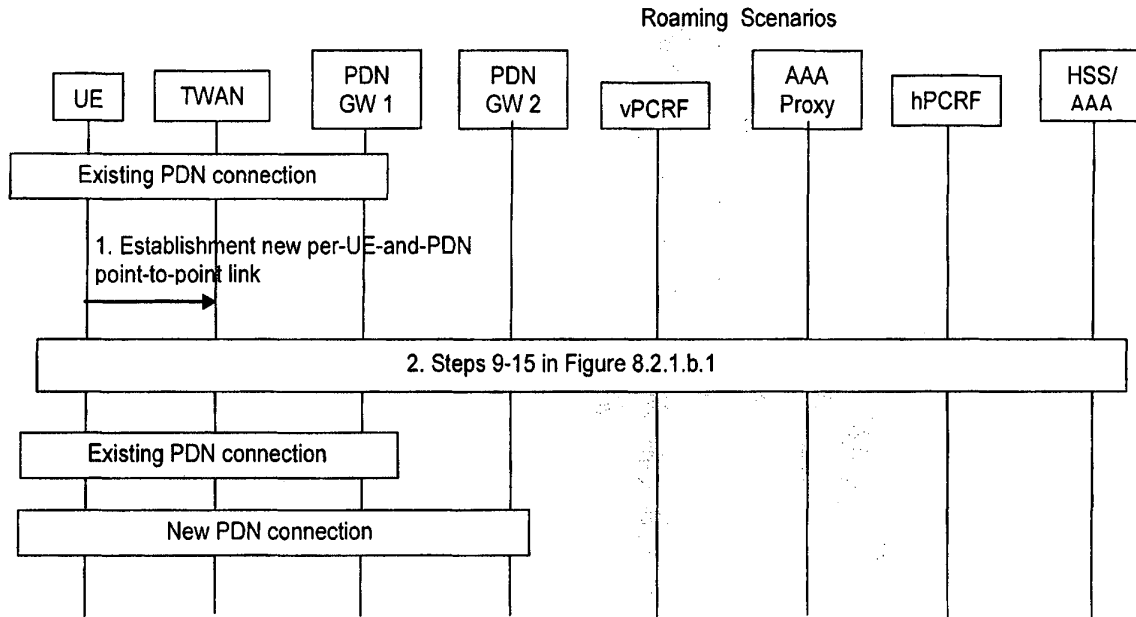


Fig. 8

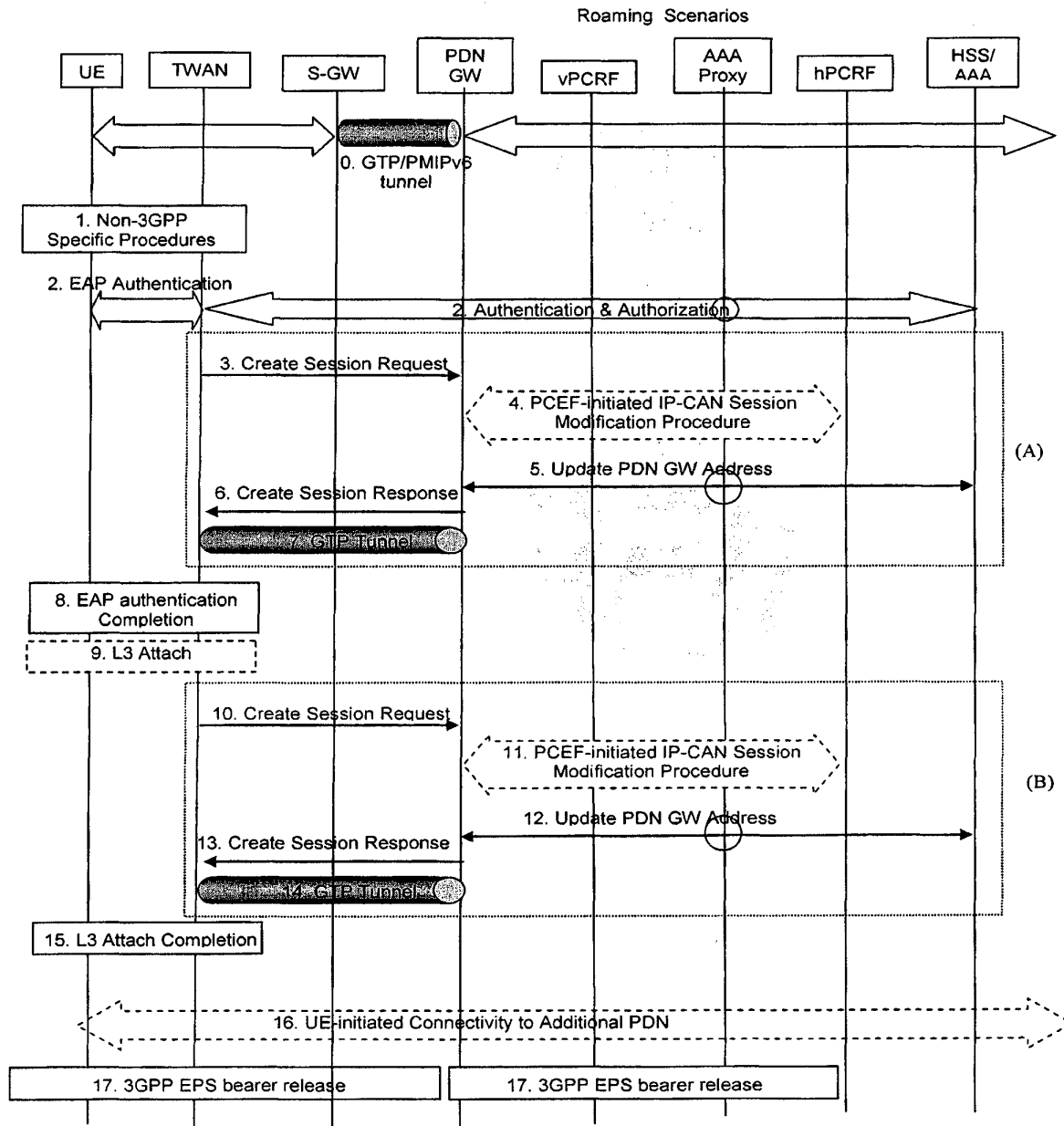


Fig. 9

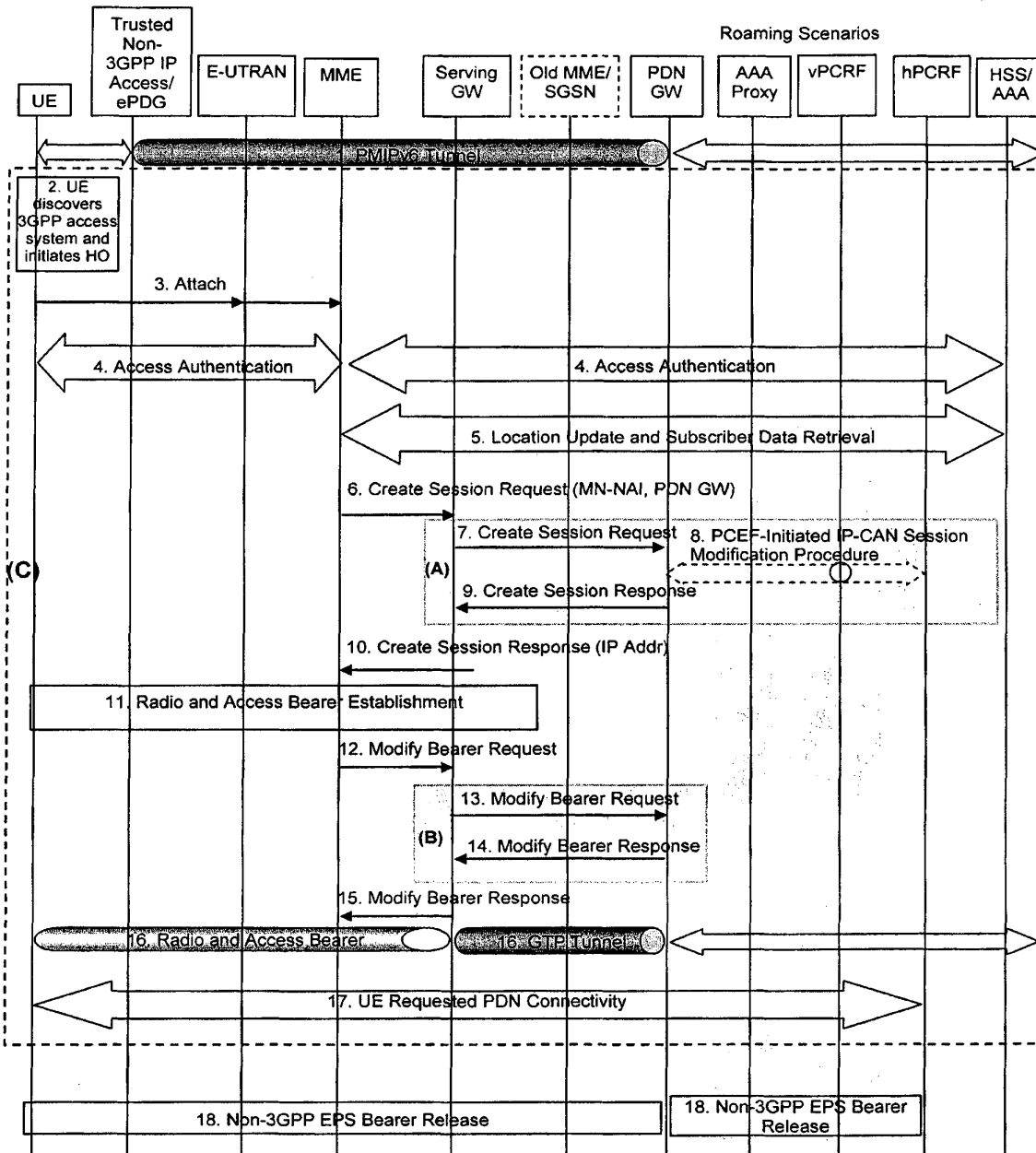


Fig. 10

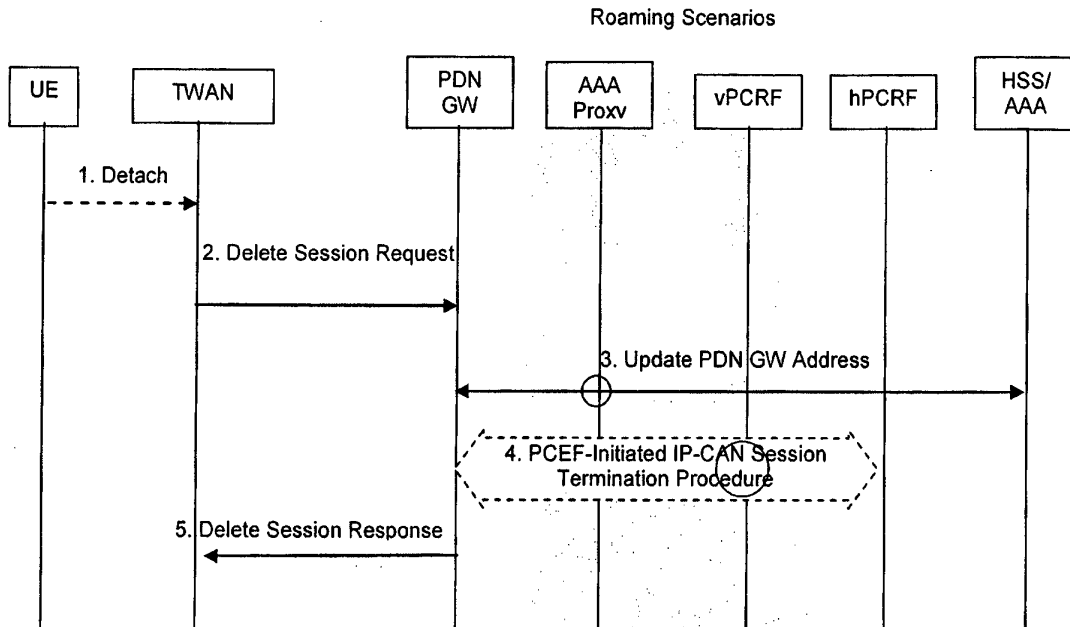
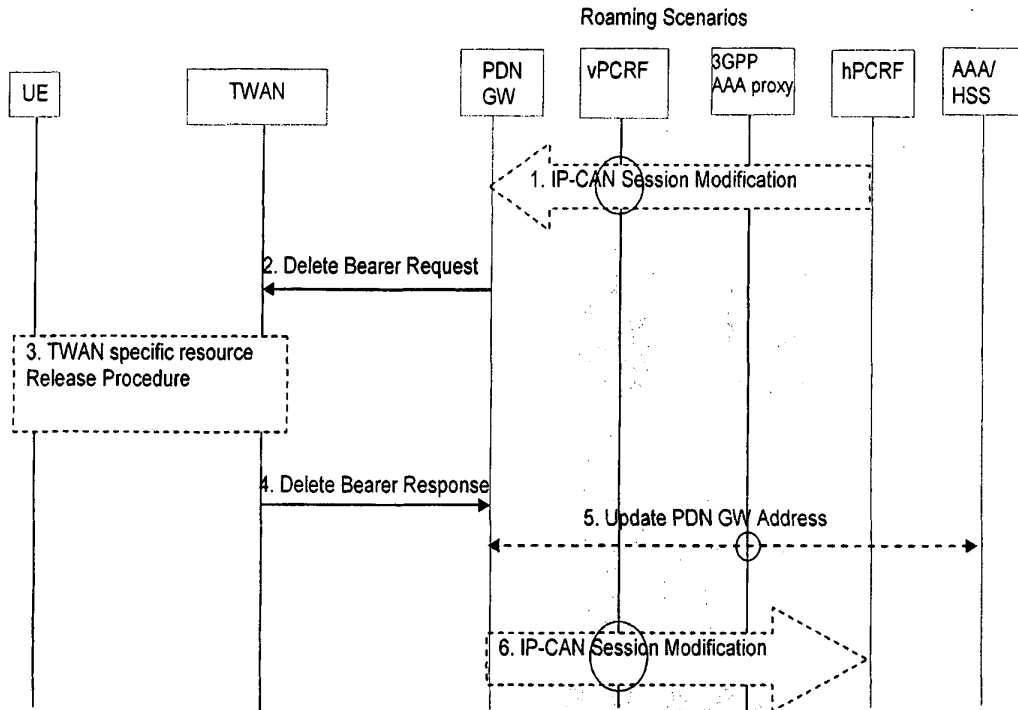


Fig. 11

**Fig. 12**

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/001660

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/12 H04W76/02
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 075 959 A1 (THOMSON LICENSING [FR]) 1 July 2009 (2009-07-01)	1,12-18, 31
Y	paragraph [0002]	2-11
A	paragraph [0021] - paragraph [0036]; figures 2-4	19-30
Y	----- CISCO ET AL: "Multiple APN Support - Approaches and Considerations", 3GPP DRAFT; S2-123004 FS-SAMOG MULTIPLE-APN-ARCHITECTU RAL-OPTIONS, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Barcelona, Spain, 3 July 2012 (2012-07-03), XP050633521, [retrieved on 2012-07-03]	2-11
A	page 3 - page 5 ----- -/-	1,12-31

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 November 2013

Date of mailing of the international search report

06/12/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Eraso Helguera, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/001660

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/174962 A1 (GUREVICH DAVID [US]) 11 August 2005 (2005-08-11) paragraph [0002] - paragraph [0071]; figures 1-13	1-31
A	----- "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on S2a Mobility based On GTP & WLAN access to EPC (SaMOG); Stage 2 (Release 12)", 3GPP STANDARD; 3GPP TR 23.852, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V1.2.0, 20 July 2012 (2012-07-20), pages 1-63, XP050648988, [retrieved on 2012-07-20] paragraph [0008] -----	1-31

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2013/001660

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2075959	A1	01-07-2009	EP 2075959 A1 01-07-2009
			EP 2232778 A1 29-09-2010
			JP 2011508551 A 10-03-2011
			KR 20100103639 A 27-09-2010
			US 2010290391 A1 18-11-2010
			WO 2009083430 A1 09-07-2009

US 2005174962	A1	11-08-2005	EP 1714399 A2 25-10-2006
			JP 2007527156 A 20-09-2007
			US 2005174962 A1 11-08-2005
			WO 2005076889 A2 25-08-2005

Form PCT/ISA/210 (patent family annex) (April 2005)

(19)



(11)

EP 3 220 697 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
06.06.2018 Bulletin 2018/23

(51) Int Cl.:
H04W 52/02 (2009.01) H04W 4/00 (2018.01)

(21) Application number: **17169607.3**

(22) Date of filing: **12.11.2013**

(54) **METHOD, APPARATUS, AND COMPUTER PROGRAM PRODUCT FOR POWER SAVE CONTROL FOR TETHERING CONNECTIONS**

VERFAHREN, VORRICHTUNG UND COMPUTERPROGRAMMPRODUKT ZUR
ENERGIESPARSTEUERUNG FÜR TETHERING-VERBINDUNGEN

PROCÉDÉ, APPAREIL ET PRODUIT-PROGRAMME D'ORDINATEUR POUR UNE COMMANDE
D'ÉCONOMIE D'ÉNERGIE DESTINÉE À DES CONNEXIONS D'ATTACHE

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

- **MARIN, Janne**
02210 Espoo (FI)
- **REUNAMÄKI, Jukka**
33820 Tampere (FI)

(30) Priority: **22.01.2013 US 201313746717**

(74) Representative: **Nokia EPO representatives**
Nokia Technologies Oy
Karaportti 3
02610 Espoo (FI)

(43) Date of publication of application:
20.09.2017 Bulletin 2017/38

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:
13192399.7 / 2 757 837

(56) References cited:
WO-A1-2011/019976 US-A1- 2008 076 411
US-A1- 2009 129 341 US-A1- 2011 263 242
US-A1- 2012 052 793 US-A1- 2012 115 471
US-A1- 2012 182 966

(73) Proprietor: **Nokia Technologies Oy**
02610 Espoo (FI)

(72) Inventors:
• **KIUKKONEN, Niko**
02880 Veikkola (FI)

EP 3 220 697 B1

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).

Description**FIELD:**

[0001] The field of the invention relates to wireless communication, and more particularly to configuring a mobile wireless hotspot in a wireless network.

BACKGROUND:

[0002] Modern society has adopted, and is becoming reliant upon, wireless communication devices for various purposes, such as connecting users of the wireless communication devices with other users. Wireless communication devices can vary from battery powered handheld devices to stationary household and/or commercial devices utilizing an electrical network as a power source. Due to rapid development of the wireless communication devices, a number of areas capable of enabling entirely new types of communication applications have emerged.

[0003] Cellular networks facilitate communication over large geographic areas. These network technologies have commonly been divided by generations, starting in the late 1970s to early 1980s with first generation (1G) analog cellular telephones that provided baseline voice communications, to modern digital cellular telephones. GSM is an example of a widely employed 2G digital cellular network communicating in the 900 MHz/1.8 GHz bands in Europe and at 850 MHz and 1.9 GHz in the United States. While long-range communication networks, like GSM, are a well-accepted means for transmitting and receiving data, due to cost, traffic and legislative concerns, these networks may not be appropriate for all data applications.

[0004] Short-range communication technologies provide communication solutions that avoid some of the problems seen in large cellular networks. Bluetooth™ is an example of a short-range wireless technology quickly gaining acceptance in the marketplace. In addition to Bluetooth™ other short-range communication technologies include Bluetooth™ Low Energy, IEEE 802.11 wireless local area network (WLAN), Wireless USB, ZigBee (IEEE 802.15.4, IEEE 802.15.4a), and ultra high frequency radio frequency identification (UHF RFID) technologies. All of these wireless communication technologies have features and advantages that make them appropriate for various applications.

[0005] Near field communication technologies, such as radio frequency identification (RFID) technologies, comprise a range of RF transmission systems, for example standardized and proprietary systems for a large number of different purposes, such as product tagging for inventory handling and logistics, theft prevention purposes at the point of sale, and product recycling at the end of the life-cycle of the tagged product. In addition to RFID technologies, Near Field Communication (NFC) technology has recently evolved from a combination of existing contactless identification and interconnection

technologies. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within close proximity of each other: A simple wave or touch can establish an NFC connection that may be used to exchange specific information for another communications protocol, which may then be used to create an actual connection in the other communications protocol, such as Bluetooth™ or wireless local area network (WLAN).

[0006] US2012/115471 discloses systems, methods, devices, and computer program products are described for discontinuous transmissions in a wireless communications system. In one example, a femtocell uses out-of-band (OOB) signals to detect the presence of user equipment (UEs) in a femtocell coverage area. In response to the detection, the femtocell may transmit in-band signals to facilitate communication with and registration of the detected UE. The femtocell may then perform discontinuous in-band transmissions to the registered UE.

SUMMARY:

[0007] Example method, apparatus, and computer program product embodiments are disclosed for configuring a mobile wireless hotspot in a wireless network.

[0008] Example embodiments of the invention include a method comprising:

establishing, by an apparatus operating as a mobile hotspot device, a control channel over a wireless out-of-band communications medium with a wireless device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

exchanging, by the apparatus operating as the mobile hotspot device, over the established control channel, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network and/or a wireless local area network provided by the apparatus operating as the mobile hotspot device.

[0009] Example embodiments of the invention include the method further comprising:

receiving, by the apparatus operating as the mobile hotspot device, over the control channel, a request from the wireless device for the in-band communi-

cations tethering connection for relaying, by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of the wide area communications network and/or the wireless local area network provided by the apparatus operating as the mobile hotspot device;

performing, by the apparatus operating as the mobile hotspot device, said exchanging over the control channel, with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and

transitioning, by the apparatus operating as the mobile hotspot device, from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection, in response to receiving the request.

[0010] Example embodiments of the invention include the method further comprising:

exchanging, by the apparatus operating as the mobile hotspot device, over the control channel, with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection with the wireless device.

[0011] Example embodiments of the invention include the method further comprising:

transitioning, by the apparatus operating as the mobile hotspot device, from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection, when no requests are received from any wireless device for the in-band communications tethering connection.

[0012] Example embodiments of the invention include the method further comprising:

wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol. Example embodiments of the invention include a method comprising:

establishing, by a wireless device, a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

exchanging, by the wireless device over the control channel, with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the apparatus operating as the mobile hotspot device in an in-band communications medium.

[0013] Example embodiments of the invention include the method further comprising:

transmitting, by the wireless device, over the control channel, a request to the apparatus operating as the mobile hotspot device for the in-band communications tethering connection;

performing, by the wireless device, said exchanging over the control channel, with the apparatus operating as the mobile hotspot device, of the in-band communications connectivity configuration information; and

establishing, by the wireless device, the in-band communications tethering connection with the apparatus operating as the mobile hotspot device, using the power saving features and optimized activity times for the in-band communications tethering connection.

[0014] Example embodiments of the invention include a computer program comprising computer readable program code configured to cause performing any of the preceding methods when said program is run on a computer.

[0015] Example embodiments of the invention include an apparatus operable as a mobile hotspot device, comprising:

means for establishing a control channel over a wireless out-of-band communications medium with a wireless device, wherein said means for establishing the control channel with the wireless device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

means for exchanging over the control channel, with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, for relaying by the apparatus, communications between the wireless device and one or more entities

in at least one of a wide area communications network and/or a wireless local area network provided by the apparatus.

[0016] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:

means for receiving over the control channel, a request from the wireless device for the in-band communications tethering connection for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of the wide area communications network and/or the wireless local area network provided by the apparatus;

means for performing said exchanging over the control channel, with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and

means for transitioning from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection, in response to receiving the request.

[0017] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:

means for exchanging over the control channel, with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection with the wireless device.

[0018] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, further comprising:

means for transitioning from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection, when no requests are received from any wireless device, for an in-band communications tethering connection

[0019] Example embodiments of the invention include the apparatus operable as a mobile hotspot device, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.

[0020] Example embodiments of the invention include an apparatus comprising:

means for establishing a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device,

wherein said means for establishing the control channel with the apparatus operating as the mobile hotspot device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and

means for exchanging over the control channel, with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the apparatus operating as the mobile hotspot device in an in-band communications medium.

[0021] The resulting embodiments configure a mobile wireless hotspot in a wireless network.

DESCRIPTION OF THE FIGURES:

[0022]

Figure 1 is an example network diagram of a mobile wireless hotspot device A and the other wireless device B, exchanging the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, in accordance with example embodiments of the invention.

Figure 1A is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1, establishing the Bluetooth control channel, in accordance with example embodiments of the invention.

Figure 1B is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1A, receiving, by the mobile hotspot device, over the control channel, a request from the wireless device for a WLAN tethering connection for relaying by the mobile hotspot device, communications between the wireless device and the cellular telephone network, in accordance with example embodiments of the invention.

Figure 1C is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1B, exchanging over the control channel, by at least one of transmitting or receiving WLAN connectivity configuration information to enable power saving features and optimize activity times in a WLAN tethering connection with the wireless device, for relaying by the mobile hotspot device, communications between the wireless device and a cellular telephone network, in accordance with

example embodiments of the invention.

Figure 1D is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1C, transitioning, by the mobile hotspot device, from a WLAN idle state to a WLAN active state using the power saving features and optimized activity times for the WLAN tethering connection, in response to receiving the request, in accordance with example embodiments of the invention.

Figure 1E is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging adjustments in the WLAN connectivity configuration information to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 1F is an example network diagram of the mobile wireless hotspot device A of Figure 1E, transitioning, by the mobile hotspot device, from the WLAN active state to the WLAN idle state of the WLAN tethering connection, when no requests are received from any wireless device, for a WLAN tethering connection for relaying by the mobile hotspot device, communications between the any wireless device and a cellular telephone network, in accordance with example embodiments of the invention.

Figure 1G is an example flow diagram of the operation of the mobile hot spot device, wherein tethering is active until there are no active clients and then it goes into the idle state and may check that its control radio is turned on and that all connected clients support the power save feature. After receiving a tethering request from a client, it turns on mobile tethering and may also inform the client that it is up and running, in accordance with example embodiments of the invention.

Figure 2A is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging adjustments in the WLAN connectivity configuration information over the Bluetooth control channel, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 2B is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 2A, exchanging adjustments in the WLAN connectivity configuration information over the Near Field Communications (NFC)

control channel or another local connectivity channel having low power, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection, in accordance with example embodiments of the invention.

Figure 3A is an example flow diagram of the process performed by mobile hotspot device, in accordance with example embodiments of the invention.

Figure 3B is an example flow diagram of the process performed by the other wireless device, in accordance with example embodiments of the invention.

Figure 4 illustrates an example embodiment of the invention, wherein examples of removable storage media are shown, based on magnetic, electronic and/or optical technologies, such as magnetic disks, optical disks, semiconductor memory circuit devices and micro-SD memory cards (SD refers to the Secure Digital standard) for storing data and/or computer program code as an example computer program product, in accordance with at least one embodiment of the present invention.

DISCUSSION OF EXAMPLE EMBODIMENTS OF THE INVENTION:

[0023] This section is organized into the following topics:

A. Wireless Short-Range Communication Networks

B. Connection Formation Between Bluetooth™ Devices

C. WLAN Communication Technology

1. IEEE 802.11 WLAN

2. Wi-Fi Protected Setup / Wi-Fi Simple Configuration (WSC)

3. Authentication in Wi-Fi Protected Setup / Wi-Fi Simple Configuration

4. Wi-Fi Direct - Software Access Points

D. Near-Field Communication (NFC) Technology

E. Power Save Control For Tethering Connections

A. Wireless Short-Range Communication Networks

[0024] Short-range communication technologies provide communication solutions appropriate for many data applications, without the cost, traffic and legislative concerns of longer-range communication technologies.

Short-range communication technologies include Bluetooth basic rate/enhanced data rate (BR/EDR), Bluetooth Low Energy (LE), IEEE 802.11 wireless local area network (WLAN), Wireless Universal Serial Bus (WUSB), ZigBee (IEEE 802.15.4, IEEE 802.15.4a), and near field communication technologies, such as radio frequency identification (RFID) and near field communication (NFC) technology that enable contactless identification and interconnection of wireless devices.

B. Connection Formation Between Bluetooth™ Devices

[0025] A procedure for forming connections between Bluetooth™ devices is described in the Bluetooth™ Specification, Version 4, June 30, 2010. The Bluetooth™ Baseband is the part of the Bluetooth™ system that implements the Media Access Control (MAC) and physical layer procedures to support the connection formation, exchange of data information streams, and ad hoc networking between Bluetooth™ devices. Connection formation may include inquiry, inquiry scanning, inquiry response, in addition to paging, page scanning, and page response procedures.

1. Inquiry

[0026] Inquiry is a procedure where a Bluetooth™ device transmits inquiry messages and listens for responses in order to discover the other Bluetooth™ devices that are within the coverage area and set discoverable. Bluetooth™ devices use the inquiry procedure to discover nearby devices, or to be discovered by devices in their locality. A Bluetooth™ device that tries to find other nearby devices is known as an inquiring device and actively sends inquiry requests. Bluetooth™ devices that are available to be found are known as discoverable devices, listen or scan for these inquiry requests, and send responses. The inquiry procedure uses dedicated physical channels for the inquiry requests and responses. The inquiry procedure does not make use of any of the architectural layers above the physical channel, although a transient physical link may be considered to be present during the exchange of inquiry and inquiry response information.

[0027] Bluetooth™ devices communicate with one another over a total bandwidth of 80 MHz divided into 79 physical channels of 1MHz each. An inquiring device wanting to discover other devices repetitively probes a first set of 16 frequencies, probing two frequencies every 625 microseconds. It repeats this at least 256 times. Then, it repetitively probes a second set of 16 frequencies. The inquiring device will repeat entire cycle at least two times. Of the 79 radio carriers, 32 are considered wake-up carriers and the inquiring device Broadcasts inquiry packets on these 32 carrier frequencies.

[0028] During the inquiry procedure, the master transmits inquiry messages with the general or dedicated in-

quiry access code. The timing for inquiry is the same as for paging. The identity or ID packet consists of the inquiry access code (IAC). It has a fixed length of 68 bits. The receiver uses a bit correlator to match the received packet to the known bit sequence of the ID packet. In order to discover other devices a device may enter inquiry substate. In this substate, it may repeatedly transmit the inquiry message (ID packet) at different hop frequencies. The inquiry hop sequence is derived from the Lower Address Part (LAP) of the General Inquiry Access Code (GIAC). Thus, even when dedicated inquiry access codes (DIACs) are used, the applied hopping sequence is generated from the GIAC LAP. A device that allows itself to be discovered, should regularly enter the inquiry scan substate to respond to inquiry messages. During the inquiry substate, the discovering device may collect the Bluetooth™ device Addresses of all devices that respond to the inquiry message. In addition, the discovering device also collects extended information (e.g. local name and supported services) from devices that respond with an extended inquiry response packet. It may then, if desired, make a connection to any one of the discovered devices by means of the page procedure described below. The inquiry message broadcast by the source does not contain any information about the source. However, it may indicate which class of devices should respond. There is one general inquiry access code (GIAC) to inquire for any device, and a number of dedicated inquiry access codes (DIAC) that only inquire for a certain type of device. The inquiry access codes are derived from reserved Bluetooth™ device addresses. There is only one DIAC defined in the Bluetooth™ Specification, and it is called the Limited Inquiry Access Code (LIAC). The LIAC is only intended to be used for limited time periods in scenarios where both devices have been explicitly caused to enter this state, usually by user action.

[0029] Inquiry scan is a procedure where a Bluetooth™ device listens for inquiry messages received on its inquiry scan physical channel. A device using one of its inquiry scan channels remains passive for duration of the inquiry scan window on that channel until it receives an inquiry message on this channel from another Bluetooth™ device. This is identified by the appropriate inquiry access code. If the inquiry scanning device receives an inquiry message during scan window it will then follow the inquiry response procedure to return a response to the inquiring device. The inquiry scan substate is very similar to the page scan substate. However, instead of scanning for the device's device Access code, the receiver should scan for the inquiry access code long enough to completely scan for 16 inquiry packets. The inquiry procedure uses 32 dedicated inquiry hop frequencies according to the inquiry hopping sequence. These frequencies are determined by the general inquiry address. The phase is determined by the native clock of the device carrying out the inquiry scan. Instead of, or in addition to, the general inquiry access code, the device may scan for one or more dedicated inquiry access codes. However, the scanning

may follow the inquiry scan hopping sequence determined by the general inquiry address. The inquiry scan interval may be less than or equal to 2.56 s.

2. Inquiry Response

[0030] An inquiry response packet (FHS) is transmitted from the slave to the master after the slave has received an inquiry message. This packet contains information necessary for the inquiring master to page the slave and follows 625 microseconds after the receipt of the inquiry message. The inquiry response packet is received by the master at the hop frequency when the inquiry message received by the slave was first in the master-to-slave slot. The slave response substate for inquiries differs completely from the slave response substate applied for pages. When the inquiry message is received in the inquiry scan substate, the recipient shall return an inquiry response (FHS) packet containing the recipient's device Address (BD_ADDR) and other parameters. If the recipient has non-zero extended inquiry response data to send, it may return an extended inquiry response packet after the FHS packet. On the first inquiry message received in the inquiry scan substate the slave may enter the inquiry response substate. If the slave has non-zero extended inquiry response data to send it may return an FHS packet, with the extended inquiry response bit set to one, to the master 625 microseconds after the inquiry message was received. It may then return an extended inquiry response packet 1250 microseconds after the start of the FHS packet. If the slave's extended inquiry response data is all zeroes the slave may only return an FHS packet with the extended inquiry response bit set to zero.

[0031] A contention problem could arise when several devices are in close proximity to the inquiring device or master and all respond to an inquiry message at the same time. However, because every device has a free running clock it is highly unlikely that they all use the same phase of the inquiry hopping sequence. In order to avoid repeated collisions between devices that wake up in the same inquiry hop channel simultaneously, a device will back-off for a random period of time. Thus, if the device receives an inquiry message and returns an FHS packet, it will generate a random number, RAND, between 0 and MAX_RAND. For scanning intervals greater than or equal to 1.28 seconds MAX_RAND will be 1023, however, for scanning intervals less than 1.28s MAX_RAND may be as small as 127. A profile that uses a DIAC may choose to use a smaller MAX_RAND than 1023 even when the scanning interval is greater than or equal to 1.28s. The slave will return to the CONNECTION or STANDBY state for the duration of at least RAND time slots. Before returning to the CONNECTION and STANDBY state, the device may go through the page scan substate. After at least RAND slots, the device will add an offset of 1 to the phase in the inquiry hop sequence (the phase has a 1.28 second resolution) and return to

the inquiry scan substate again. If the slave is triggered again, it will repeat the procedure using a new RAND. The offset to the clock accumulates each time an FHS packet is returned. During a period when the inquiry device is broadcasting inquiry packets, a slave may respond multiple times, but on different frequencies and at different times. Reserved synchronous slots should have priority over response packets; that is, if a response packet overlaps with a reserved synchronous slot, it will not be sent, but the next inquiry message is awaited. If a device has extended inquiry response data to send, but the extended inquiry response packet overlaps with a reserved synchronous slot, the FHS packet may be sent with the EIR bit set to zero.

[0032] The messaging during the inquiry routines is summarized as follows:

In step 1, the master transmits an inquiry message using the inquiry access code and its own clock.

In step 2, the slave responds with the FHS packet containing the slave's Bluetooth™ device Address, native clock and other slave information. This FHS packet is returned at times that tend to be random. The FHS packet is not acknowledged in the inquiry routine, but it is retransmitted at other times and frequencies as long as the master is probing with inquiry messages.

In step 3, if the slave has non-zero extended inquiry response data, it sends an extended inquiry response packet to the master.

3. Extended Inquiry Response

[0033] An Extended Inquiry Response may be used to provide miscellaneous information during the inquiry response procedure. Data types are defined for such things as local name and supported services, information that otherwise would have to be obtained by establishing a connection. A device that receives a local name and a list of supported services in an extended inquiry response does not have to connect to do a remote name request and a service discovery protocol (SDP) service search, thereby shortening the time to useful information. If the slave transmits an extended inquiry response packet, it is transmitted 1250 microseconds after the start of the inquiry response packet. The extended inquiry response packet is received by the master at the hop frequency when the inquiry message received by the slave was first in the master-to-slave slot. The extended inquiry response packet is an Asynchronous Connection-oriented Logical transport (ACL) data medium rate (DM) packet with type DM1, DM3, DM5, DH1, DH3 or DH5. To minimize interference it is recommended to use the shortest packet that is capable of containing the data. The packet is sent on the same frequency as the (frequency hop synchronization) FHS packet, 1250 microseconds after

the start of the FHS packet. In the packet header, the logical transport address (LT_ADDR) may be set to zero. TYPE may be one of DM1, DM3, DM5, DH1, DH3 or DH5. FLOW, ARQN and SEQN may all be set to zero and ignored during receipt. (ARQN is automatic repeat address acknowledgement indication and SEQN is sequential numbering scheme.) The header error check (HEC) linear feedback shift register (LFSR) may be initialized with the same default check initialization (DCI) as for the FHS packet. In the payload header, logical link identifier (LLID) may contain the value 10 (start of a logical link control and adaptation control (L2CAP) message or no fragmentation). FLOW may be set to zero and ignored upon receipt. The length of the payload body (LENGTH) may be smaller than or equal to 240 bytes. The cyclic redundancy check (CRC) linear feedback shift register (LFSR) may be initialized with the same DCI as for the FHS packet. The data whitening LFSR may be initialized with the same value as for the FHS packet. The length of the payload body (LENGTH) may be smaller than or equal to 240 bytes. The CRC LFSR may be initialized with the same DCI as for the FHS packet. The data whitening LFSR may be initialized with the same value as for the FHS packet. The payload data has two parts, a significant part followed by a non-significant part. The significant part contains a sequence of data structures. The non-significant part contains all zero octets. The baseband may not change any octets in the significant part. When transmitting data, the non-significant part octets may be omitted from the payload. A device may store a single extended inquiry response packet. This packet may be used with all inquiry access codes (IACs).

4. Page

[0034] Page is the initial phase of the connection procedure where a device transmits a train of page messages until a response is received from the target device, is stopped by host or a timeout occurs. Page scan is a procedure where a device listens for page messages received on its page scan physical channel. In forming a connection, the paging device will become the master and the page scan device will become the slave in a piconet. Initially, after the slave has received an inquiry message, an inquiry response packet is transmitted from the slave to the master. The inquiry response packet sent from the slave contains information necessary for the inquiring master to page the slave, such as Bluetooth™ device Address of the slave device. The necessary information may be received by other means, such as Out-Of-Band pairing. Also the page is not away always preceded with inquiry, because the address may be known beforehand (for example saved from previous connections). In the paging procedure, the Bluetooth™ device that will become the master carries out a page procedure by transmitting page messages in connection request packets to the specified Bluetooth™ slave device that carries out a page scanning procedure to listen for con-

nection request packets from the paging device. A connectable Bluetooth™ device listens for a page request on its page scan channel and, once received, enters into a sequence of exchanges with the paging device. In order for a device to connect to another device, it performs frequency hopping all page scan channel frequencies, sending a page request on each frequency and listening for a response. The page scan channel uses an access code derived from the scanning device's Bluetooth™ device Address BD_ADDR to identify communications on the channel. The page scan channel uses a slower hopping rate than the hop rate of the paging device, using the Bluetooth™ device clock of the scanning device as an input. A device listening on its page scan channel remains passive until it receives a page request from another Bluetooth™ device, identified by the page scan channel access code. The two devices will then follow the page procedure to form a connection where the paging device is the master and the page scan device is the slave in a piconet. In order for a paging device to connect to another Bluetooth™ device, it uses the page scan channel of the target device in order to send page requests. If the paging device does not know the phase of the target device's page scan channel, it does not know the current hop frequency of the target device. Therefore, the paging device transmits page requests on each of the page scan hop frequencies and listens for a page response. This is done at a faster hop rate, allowing the paging device to cover all page scan frequencies in a short period of time. The paging device may have some knowledge of the target device's Bluetooth™ clock, such as indicated during a previous inquiry transaction between the two devices, and may be able to predict the phase of the target device's page scan channel. It may use this information to optimize the synchronization of the paging and page scanning process and speed up the formation of the connection.

5. Service Discovery Protocol (SDP)

[0035] Bluetooth devices are designed to find other Bluetooth devices within their radio communications range and to discover what services they offer, using a service discovery protocol (SDP). The SDP searching function relies on links being established between the requesting Bluetooth device in a client role and the responding Bluetooth device in a server role. Once a link has been established, it can be used to find out about services in the responding Bluetooth device and how to connect to them.

[0036] Service Discovery Protocol (SDP) is used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (headset profile, hands free profile, advanced audio distribution profile, etc.) and the protocol multiplexor settings needed to con-

nect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

C. WLAN Communication Technology

1. IEEE 802.11 WLAN

[0037] The IEEE 802.11 standard specifies methods and techniques of an exemplary wireless local area network (WLAN) operation, examples include the IEEE 802.11b and 802.11g wireless local area network specifications, which have been a staple technology for traditional WLAN applications in the 2.4 GHz ISM band. The various amendments to the IEEE 802.11 standard were consolidated for IEEE 802.11a, b, d, e, g, h, i, j, k, n, r, s, u, v, and z protocols, into the base standard IEEE 802.11-2012, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, February 2012 (incorporated herein by reference). Since then, emerging broadband applications have stimulated interest in developing very high-speed wireless networks for short range communication, for example, the planned IEEE 802.11ac, and the planned IEEE 802.11ad WLAN specifications that are to provide a very high throughput in higher frequency bands. Applications of these IEEE 802.11 standards include products such as consumer electronics, telephones, personal computers, and access points for both for home and office.

[0038] An IEEE 802.11 WLAN may be organized as an independent basic service set (IBSS) or an infrastructure basic service set (BSS). The access point (AP) in an infrastructure basic service set (BSS) IEEE 802.11 WLAN network, is a central hub that must relay all communication between the mobile wireless devices (STAs) in an infrastructure BSS. If a STA in an infrastructure BSS wishes to communicate a frame of data to a second STA, the communication must take two hops. First, the originating STA transfers the frame to the AP. Second, the AP transfers the frame to the second STA. In an infrastructure BSS, the AP either transmits Beacons or responds to probes received from STAs for discover purposes. After a possible authentication of a STA that is conducted by the AP, an association occurs between the AP and a STA enabling data traffic to be exchanged with the AP. The Access Point (AP) in an Infrastructure BSS may bridge traffic out of the BSS onto a distribution network.

[0039] The IEEE 802.11 WLAN uses two types of transmission: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF employs Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Every packet sent is positively acknowledged by the receiver. A transmission begins with a Request to Send (RTS) and the receiver responds with a Clear to Send (CTS). The channel is cleared by these two messages, since all STAs that hear the CTS will sup-

press their own start of a transmission. Then when data packets are transmitted, each has a Network Allocation Vector (NAV) containing a duration value to reserve the channel for the sender and receiver for an interval after the current packet, equal to the NAV duration. The value of the NAV decrements with the passage of time. Once the sender and receiver have reserved the channel, they may hold it for the remaining duration of the NAV value. The last acknowledgement packet (ACK) contains a NAV value of zero, to immediately release the channel. The Point Coordination Function (PCF) is a polling method among the STAs of the BSS, which is coordinated by the access point.

[0040] IEEE 802.11 authentication operates at the link level between IEEE 802.11 STAs. IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is a station service that may be used by all STAs to establish their identity to STAs with which they communicate in both infrastructure and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, then an association is not established. IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the distribution system. Shared Key authentication relies on wired equivalent privacy to demonstrate knowledge of an encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods. A robust security network association (RSNA) supports authentication based on IEEE 802.1X-2004, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the Extensible Authentication Protocol (EAP) (IETF RFC 3748-2004) to authenticate STAs and an authentication server (AS) with one another. In IEEE 802.1X, a STA being authenticated and the authenticator device exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

[0041] The access point (AP) in an infrastructure BSS assists those mobile wireless devices (STAs) attempting to save power. The legacy IEEE 802.11e Wireless LAN standards provides for support of low power operation in handheld and battery operated STAs, called automatic power save delivery (APSD). A STA capable of APSD and currently in the power saving mode, will wake up at predetermined beacons received from the AP to listen to a Traffic Indication Map (TIM). If existence of buffered traffic waiting to be sent to the STA is signaled through the TIM, the STA will remain awake until AP sends out all the data. The STA does not need to send a polling signal to the AP to retrieve data, which is the reason for the term "automatic" in the acronym APSD.

[0042] A Traffic Indication Map (TIM) is a field transmitted in beacon frames, used to inform associated wireless client devices that the access point has buffered

data waiting to be transmitted to them. Access points buffer frames of data for wireless client devices while they are sleeping in a low-power state. The access point transmits beacons at a regular interval, the target beacon transmission time (TBTT). The Traffic Indication Map (TIM) information element in the periodically transmitted beacon frame, indicates which wireless client devices have buffered data waiting to be accessed in the access point. Each frame of buffered data is identified by an association identifier (AID) associated with a specific wireless client device. The AID is used to logically identify the wireless client device to which buffered frames of data are to be delivered. The traffic indication map (TIM) contains a bitmap, with each bit relating to a specific association identifier (AID). When data is buffered in the access point for a particular association identifier (AID), the bit is "1". If no data is buffered, the bit for the association identifier (AID) is "0". Wireless client devices must wake up and listen for the periodic beacon frames to receive the Traffic Indication Map (TIM). By examining the TIM, a wireless client device may determine if the access point has buffered data waiting for it. To retrieve the buffered data, the wireless client device may use a power-save poll (PS-Poll) frame. After transmitting the PS-Poll frame, the client mobile station may stay awake until it receives the buffered data or until the bit for its association identifier (AID) in the Traffic Indication Map (TIM) is no longer set to "1", indicating that the access point has discarded the buffered data.

[0043] Two variations of the APSD feature are unscheduled automatic power save delivery (U-APSD) and scheduled automatic power save delivery (S-APSD). In U-APSD, the access point (AP) is always awake and hence a mobile wireless device (STA) in the power save mode may send a trigger frame to the AP when the STA wakes up, to retrieve any queued data at the AP.. In S-APSD, the AP assigns a schedule to a STA and the STA wakes up, sends a power save poll packet to the AP in order to retrieve from the AP any data queued. An AP may maintain multiple schedules either with the same STA or with different STAs in the infrastructure BSS network. Since the AP is never in sleep mode, an AP will maintain different scheduled periods of transmission with different STAs in the infrastructure BSS network to ensure that the STAs get the maximum power savings.

2. Wi-Fi Protected Setup / Wi-Fi Simple Configuration (WSC)

[0044] Network setup for IEEE 801.11 WLANs has been simplified by the Wi-Fi Protected Setup™ system that is included in most access points. The Wi-Fi Alliance published the Wi-Fi Protected Setup (WPS) specification 1.0, Wi-Fi Protected Setup Specification, Version 1.0h, December 2006 (incorporated herein by reference). The Wi-Fi Simple Configuration (WSC) Specification, Version 2.0, December 20, 2010, (incorporated herein by reference), updates the Wi-Fi Protected Setup Specification,

Version 1.0h. The acronym WSC, for Wi-Fi Simple Configuration Specification, may be used interchangeably with the acronym WPS, for Wi-Fi Protected Setup. Wi-Fi Protected Setup facilitates the initial setting up of IEEE 802.11 devices in a Wi-Fi infrastructure network so that they may be more easily configured with security features and so that that new Wi-Fi devices may be added to the network. Wi-Fi Protected Setup allows access points to be set up by entering a PIN. The Protected Setup system uses this information to send data to a computer connected to the access point, to complete the network setup. Wi-Fi Protected Setup defines new IEEE 802.11 information elements (IE) that are included in beacons, probe requests and probe responses. The purpose of these IEs is to advertise the presence of devices that are capable of performing Wi-Fi Protected Setup operations. **[0045]** Initial discovery of Wi-Fi Simple Configuration devices is accomplished using IEEE 802.11 Information Elements in management frames (Beacon, Probe Request, and Probe Response). If the Enrollee decides to pursue a connection to the network, it initiates an IEEE 802.1X/EAP connection for the Extensible Authentication Protocol (EAP)-based Registration Protocol. The Wi-Fi Simple Configuration Information Element complies with the IEEE 802.11 Information Element format and indicates specific data necessary for network information, capabilities and modes, to configure an Enrollee for the wireless network and to report problems with the Enrollee associating with a specified wireless network with the supplied settings.

[0046] The Wi-Fi Protected Setup 1.0 standard defines three types of components in a network: a Registrar, an Enrollee, and an Access Point (AP). A Registrar is a component with the authority to issue and revoke credentials to a network. A Registrar may be integrated into an AP or it may be separate from the AP. An Enrollee is a component seeking to join a wireless LAN network. An Authenticator is an AP functioning as a proxy between a Registrar and an Enrollee. A Registrar wireless device configures the Enrollee wireless device, and the AP acts as an Authenticator to proxy the relevant messages between the Registrar and the Enrollee. The messages exchanged in the session are a series of Extensible Authentication Protocol (EAP) request/response messages, ending with the Enrollee reconnecting to the network with its new configuration. EAP is an authentication framework defined in RFC 5247, for providing the transport and usage of keying material and parameters needed to establish a secure Wi-Fi network. The Wi-Fi Simple Configuration Specification, Version 2.0, December 20, 2010, (incorporated herein by reference), updates the Wi-Fi Protected Setup Specification, Version 1.0h.

[0047] A standalone AP that supports Wi-Fi Protected Setup, includes a built-in Registrar and does not use an external Registrar. In initial WLAN setup with Wi-Fi Protected Setup, when initializing in a standalone mode, a Wi-Fi Protected Setup AP automatically chooses a random SSID and channel. A standalone AP that includes

a Wi-Fi Protected Setup Registrar, issues keys to Enrollees via the Registration Protocol.

[0048] When an Enrollee is initialized, it looks for Beacons from APs and sends probe requests with the WSC information element (IE), into either selected networks or into each network sequentially. It may also send probe requests to each IEEE 802.11 channel with the WSC IE included. It looks for the WSC IE in probe-responses that it receives and can engage with one or more Registrars to further discover Registrar capabilities and to see if the user has selected a Registrar. The Enrollee may continue looking for selected Registrar flags in Beacons, probe-responses and any M2 messages and may cease scanning when it finds a Registrar indicating that it is prepared to configure the Enrollee.

[0049] The following example describes an example in-band setup procedure using Wi-Fi Protected Setup for adding Member devices using a Standalone AP/Registrar. The user may convey the Enrollee's device password to the AP/Registrar using keyboard entry or an out-of-band channel with Near-Field Communication (NFC) Connection Handover. This example does not show the exchange of preliminary M1 and M2D messages that may take place after the probe message exchange, because the Enrollee may be waiting for the user to configure the AP/Registrar with the Enrollee's device password.

1. The Enrollee sends its Discovery data in a probe request to a Wi-Fi Protected Setup AP or ad hoc wireless Registrar. The AP or wireless Registrar responds with its own Discovery data in the probe response.

2. The user may be prompted to enter the Enrollee's device password into the AP/Registrar using a keypad interface or an out-of-band channel.

3. The Enrollee connects and initiates the IEEE 802.1X port-based Network Access Control procedure for port-based authentication.

4. The Enrollee and Registrar exchange messages M1 -M8 to provision the Enrollee.

5. The Enrollee disassociates and reconnects, using its new WLAN authentication Credential. The Enrollee is now connected to the network with its new configuration.

3. Authentication in Wi-Fi Protected Setup/Wi-Fi Simple

Configuration

[0050] The Wi-Fi Simple Configuration Specification, Version 2.0 (renamed from the original name "Wi-Fi Protected Setup"), uses the IEEE 802.1X Port-Based Au-

thentication and Extensible Authentication Protocol (EAP) to transport in-band Registration Protocol messages. This protocol is mapped onto a custom EAP method described below. Wi-Fi Simple Configuration does not require the AP to support remote authentication dial-in user service (RADIUS) (IETF RFC 2865-2000), and the network need not include an authentication server. In fact, many Wi-Fi Simple Configuration APs may support IEEE 802.1X only to configure Wi-Fi Protected Access 2 (WPA2)-Personal Credentials using Wi-Fi Simple Configuration. Enrollees using Wi-Fi Simple Configuration are not granted direct access to the WLAN through the Wi-Fi Simple Configuration custom EAP method. The EAP method is used to configure the Enrollee with a Credential that can be used subsequently with whatever access method is supported by that WLAN. For example, if the AP only supports WPA2-Personal with a network-wide shared Pre-Shared Key (PSK), then the Enrollee would run the 802.1X exchange to obtain the PSK, disassociate, and then reconnect and use WPA2-Personal to access the WLAN. Alternatively, if the AP supports 802.1X authentication, the Enrollee may first run the Wi-Fi Simple Configuration EAP method to obtain a shared secret Credential and then reconnect using that secret in conjunction with another EAP method to access the WLAN.

[0051] The Wi-Fi Simple Configuration EAP method (EAP-WSC) can be used for Registrar and Enrollee discovery and for Credential establishment. The first time the Enrollee encounters a new WLAN, it sends out its Discovery information and executes the EAP-WSC method. In both the Discovery message and in Registration Protocol Message M1, the Enrollee provides information about itself to the WLAN. The M2 and M2D messages sent to the Enrollee likewise provide information about the available Registrars. When the Enrollee first discovers and attempts to connect to the WLAN, the WLAN's Registrar(s) may not yet know the Enrollee's device password. Therefore, Registrars without the device password respond with M2D messages. Although these M2D messages are unauthenticated, they can help Enrollees with rich user interfaces, to guide the user through the enrollment process.

[0052] As the Enrollee scans over the M2D messages sent by the network, it may discover that none of them possesses its device password. At this point, the Enrollee has an opportunity to prompt the user to perform a trust bootstrapping operation such as connecting an available out-of-band channel or entering a device password into one of the available Registrars. If the user decides to enter the Enrollee's device password into the Registrar, the Enrollee can reconnect and run the EAP method once more to perform the complete Registration Protocol. If the Enrollee has no user interface to lead the user through the enrollment, it is likely that one or more of the WLAN's Registrars can do this. Both the Registrar and the Enrollee are given sufficient information about each others' capabilities through the EAP method to successfully lead

the user through the enrollment. If the user decides to use an out-of-band channel for registration, then message M2 is implicitly authenticated by the channel and can carry the network configuration data.

[0053] The AP functions as the EAP authenticator on the WLAN. Thus, the AP generates EAP Request messages and Enrollees and Registrars generate EAP Responses. If the Registrar is external to the AP, then it uses universal plug and play (UPnP) to exchange Registration Protocol messages with the AP. A Registrar may also function in the role of an 802.1X authenticator, which is useful for networks with legacy APs.

[0054] The Wi-Fi Simple Configuration EAP method uses EAP, as specified in RFC 3748, and Extensible Authentication Protocol (EAP) over LAN (EAPoL), as specified in IEEE 802.1X-2001, but does not represent a network authentication protocol. Rather Wi-Fi Simple Configuration utilizes the 802.1X data connection for acquiring settings necessary for connecting to the network and the resulting EAP exchange must always terminate with EAP-Failure.

[0055] When the Enrollee decides to connect to the network and run the Wi-Fi Simple Configuration EAP method, it associates with the AP and sends an EAPoL-Start message. The AP responds with an EAP-Request/Identity. The Enrollee sends an EAP-Response/Identity containing the defined Wi-Fi Alliance name for a Simple Configuration Enrollee ("WFA-SimpleConfig-Enrollee-1-0"). This causes the AP to start running the Simple Configuration EAP method. The Registration Protocol messages are exchanged until M8 is received and validated by the Enrollee. If it successfully processes M8, the Enrollee sends an EAP-Response/Done message to the authenticator, which sends the WSC_Done message to any External Registrar and the authenticator returns an EAP-Failure message to the Enrollee. An Enrollee should assume that the received credentials are valid after successfully processing message M8 and sending the WSC_Done message. The Enrollee then disassociates and reconnects with the Credential obtained from M8's ConfigData. If M2D is received by the Enrollee, it should respond with an ACK message so that the AP can continue to send it discovery messages from other Registrars. After the AP sends an EAP-failure to the Enrollee, the Enrollee can do one of two things (given that the AP did not de-authenticate the Enrollee after sending the EAP-Failure): it can disconnect from the AP and reconnect some time later to rerun the Wi-Fi Simple Configuration EAP method by sending an EAPoL-Start message or it can stay connected to the AP and rerun the Wi-Fi Simple Configuration EAP method by sending another EAPoL-Start message.

[0056] Once the Enrollee sends an M3 message, both the Registrar and the Enrollee must proceed in lock-step fashion until either a failure or until success occurs (indicated by the Done response message). If the Enrollee (IEEE 802.1X supplicant) detects any errors in these later phases, it responds by sending a NACK message and

transitioning to the termination state to terminate the connection. At this point, the Enrollee computes a fresh device password for use in the next instance of the Registration Protocol. If the same password is reused with multiple instances of the protocol, it will be susceptible to active attack.

[0057] The Registration Protocol Messages M1 to M8 are described in the Wi-Fi Simple Configuration Specification, Version 2.0. They include an exchange of public keys, description of the sending device, including its MAC address and device capabilities, and various message authentication values, culminating in the Registrar sending to the Enrollee credentials for accessing the network.

[0058] A credential is a data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network. With out-of-band configuration, WLAN credentials are sent across the out-of-band channel to the Enrollee. The NFC interfaces operating in peer-to-peer mode between an AP or Group Owner (GO) having an integrated Registrar and an Enrollee device, have the strongest security properties supported by the Wi-Fi Simple Configuration Specification, because practical man-in-the-middle attacks against NFC are not feasible. In this mode, a 1536-bit Diffie-Hellman exchange is performed over the NFC interface, and WLAN settings are encrypted using 128-bit Advanced Encryption Standard (AES) and delivered over the same interface between an AP or Group Owner (GO) and an Enrollee device. The Diffie-Hellman public keys and WLAN settings are implicitly authenticated by both the Registrar and the Enrollee, because they are received over the NFC channel.

4. Wi-Fi Direct - Software Access Points

[0059] The Wi-Fi Alliance has developed a Wi-Fi Peer-to-Peer technology named Wi-Fi Direct™ that is specified in the Wi-Fi Alliance Peer-to-Peer Specification, October 2010 (incorporated herein by reference). Wi-Fi Direct, is also referred to herein as Peer-to-Peer or P2P. Wi-Fi Direct enables IEEE 802.11a, g, or n devices to connect to one another, peer-to-peer, without prior setup or the need for wireless access points. Wi-Fi Direct embeds a software access point into any device, which provides a version of Wi-Fi Protected Setup. When a device enters the range of a STA supporting Wi-Fi Direct (a Wi-Fi Direct device), it can connect to it and then gather setup information using a Wi-Fi Protected Setup transfer. Devices that support Wi-Fi Direct may discover one another and advertise available services. Wi-Fi Direct devices support typical Wi-Fi ranges and the same data rates as can be achieved with an 802.11a, g, or n infrastructure connection. When a device enters the range of the Wi-Fi Direct device, it may connect to it using the existing protocol, and then gather setup information using a Wi-Fi Protected Setup 2.0 transfer.

[0060] Wi-Fi Direct enables IEEE 802.11 devices that support Wi-Fi Direct, to connect to one another, point-to-point. The specification may be implemented in any Wi-

Fi device. Devices that support the specification will be able to discover one another and advertise available services. Wi-Fi Direct devices will support typical Wi-Fi ranges and the same data rates as can be achieved with an infrastructure connection. Wi-Fi Direct provides point-to-point connections for networks by embedding a software access point into any device that wishes to support Wi-Fi Direct. The soft AP provides a version of Wi-Fi Protected Setup 2.0. When a device enters the range of the Wi-Fi Direct device, it may connect to it using the existing protocol, and then gather setup information using a Wi-Fi Protected Setup 2.0 transfer.

[0061] Wi-Fi Direct-certified devices may create direct connections between Wi-Fi client devices without requiring the presence of a traditional Wi-Fi infrastructure network of an access point or router. Wi-Fi Direct-certified devices support connection with existing legacy Wi-Fi devices using the IEEE 802.11 a/g/n protocols. Wi-Fi Direct Device Discovery and Service Discovery features allow users to identify available devices and services before establishing a connection, for example, discovering which Wi-Fi device is a printer.

[0062] A Wi-Fi Direct device may support an infrastructure network of an access point or router in addition to a peer-to-peer (P2P) connection. Wi-Fi Direct devices may join infrastructure networks as stations (STAs) and may support Wi-Fi Protected Setup enrollee functionality. Wi-Fi Direct devices may connect by forming Groups in a one-to-one or one-to-many topology. The Groups function in a manner similar to an infrastructure basic service set (BSS). A single Wi-Fi Direct device will be the Group Owner (GO) that manages the Group, including controlling which devices are allowed to join and when the Group is started or terminated. The Group Owner (GO) will appear as an access point to legacy client's devices.

[0063] Wi-Fi Direct devices include a Wi-Fi Protected Setup Internal Registrar functionality and communication between Clients in the Group. Wi-Fi Direct devices may be a Group Owner (GO) of a Group and may be able to negotiate which device adopts this role when forming a Group with another Wi-Fi Direct device. A Group may include both Wi-Fi Direct devices and legacy devices (i.e., that are not compliant with the Wi-Fi Alliance Peer-to-Peer Specification). Legacy Devices can only function as Clients within a Group.

[0064] Wi-Fi Direct devices support Discovery mechanisms. Device Discovery is used to identify other Wi-Fi Direct devices and establish a connection by using a scan similar to that used to discover infrastructure access points. If the target is not already part of a Group, a new Group may be formed. If the target is already part of a Group, the searching Wi-Fi Direct device may attempt to join the existing Group. Wi-Fi Protected Setup may be used to obtain credentials from the Group Owner (GO) and authenticate the searching Wi-Fi Direct device. Wi-Fi Direct devices may include Service Discovery that enables the advertisement of services supported by higher layer applications to other Wi-Fi Direct devices. Service

Discovery may be performed at any time (e.g. even before a connection is formed) with any other discovered Wi-Fi Direct device.

[0065] A Group may be created by a single Wi-Fi Direct device, such as when connecting a legacy device. When forming a connection between two Wi-Fi Direct devices, a Group may be formed automatically and the devices may negotiate to determine which device is the Group Owner. The Group Owner may decide if this is a temporary (single instance) or persistent (multiple, recurring use) Group. After a Group is formed, a Wi-Fi Direct device may invite another Wi-Fi Direct device to join the Group. The decision of whether or not to accept an invitation may be left to the invited Wi-Fi Direct device.

[0066] Wi-Fi Direct Devices may participate in multiple Groups. A Wi-Fi Direct Device that may be in a Group while maintaining a WLAN infrastructure connection at the same time is considered a Concurrent Device or a dual stack device. For example, a laptop connected directly to a printer while simultaneously using a WLAN connection is operating as a Concurrent Device. Concurrent connections may be supported by a single radio and may support connections on different channels. Concurrent operation may be supported by multiple protocol stacks, for example, one for operation as a WLAN-STA and one for operating as a Wi-Fi Direct device. For example, two separate physical MAC entities may be maintained, each associated with its own PHY entity, or they may use a single PHY entity supporting two virtual MAC entities.

[0067] The Wi-Fi Peer-to-Peer Technical Specification v1.1, 2010 published by the Wi-Fi Alliance, provides for provisioning in Wi-Fi Direct networks. Provisioning is a phase of peer-to-peer group formation in which credentials for the peer-to-peer group are exchanged based on the use of Wi-Fi Simple Configuration. Credentials are information that is required to join a peer-to-peer group as defined in the Wi-Fi Simple Configuration Specification.

[0068] To allow for peer-to-peer device configuration, peer-to-peer devices may delay starting the provisioning phase until the expiration of the larger of the peer-to-peer group owner's (GO) configuration time and the peer-to-peer client's client configuration time, based on respective configuration timeout attributes exchanged during a preceding group owner negotiation.

[0069] The peer-to-peer device selected as peer-to-peer group owner (GO) during group owner negotiation may start a peer-to-peer group session using the credentials it intends to use for that group. The peer-to-peer group owner (GO) may use the operating channel indicated during group owner negotiation, if available. The peer-to-peer client may connect to the peer-to-peer group owner to obtain credentials. If the operating channel is not available the peer-to-peer group owner may use another channel from a channel list attribute sent in the group owner negotiation confirmation frame. The peer-to-peer client may have to scan to find the peer-to-

peer group owner if the intended operating channel is not available. A group formation bit in a peer-to-peer group capability bitmap of the peer-to-peer capability attribute may be set to one until provisioning succeeds.

[0070] Provisioning may be executed in Wi-Fi Direct networks, as described, for example, in the Wi-Fi Simple Configuration (WSC) Specification, Version 2.0, December 20, 2010. The peer-to-peer group owner (GO) may serve the role as the access point with an internal registrar. It will only allow association by the peer-to-peer device that it is currently with in a group formation. Since the user has entered the WSC PIN or triggered the WSC pushbutton functionality on both devices, the registrar may send an M2 message in response to an M1 message. The peer-to-peer client may serve the role as the STA enrollee. It may associate to the peer-to-peer device that it is currently with in the group formation.

[0071] If provisioning fails, then group formation ends and the peer-to-peer group owner (GO) may end the peer-to-peer group session. If provisioning fails, the peer-to-peer device may retry group formation or return to device discovery. On successful completion of provisioning in Wi-Fi Direct networks, the peer-to-peer group owner (GO) may set the group formation bit in the peer-to-peer group capability bitmap of the peer-to-peer capability attribute to zero. At this point the peer-to-peer client may join the peer-to-peer group in the Wi-Fi Direct network, using the credentials supplied during provisioning.

D. Near-Field Communication (NFC) Technology

[0072] One of the methods provided by the Wi-Fi Simple Configuration Specification, Version 2.0, is the Near-Field Communication (NFC) method, in which the user brings a new wireless client device (STA) close to an access point (AP) or Registrar of the Network to allow near field communication between the devices.

[0073] Near field communication technologies, such as radio frequency identification (RFID) technologies, comprise a range of RF transmission systems, for example standardized and proprietary systems for a large number of different purposes, such as product tagging for inventory handling and logistics, theft prevention purposes at the point of sale, and product recycling at the end of the life-cycle of the tagged product. In addition to RFID technologies, Near Field Communication (NFC) technology has recently evolved from a combination of existing contactless identification and interconnection technologies. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within close proximity of each other: A simple wave or touch can establish an NFC connection, which is then compatible with other known wireless technologies, such as Bluetooth™ or wireless local area network (WLAN).

[0074] Near-field communication (NFC) technology used in the Wi-Fi Protected Setup (WPS) standard, communicates between two NFC Devices or between an

NFC device And an NFC Tag via magnetic field induction, where two loop antennas are located within each other's near field, effectively energizing a wireless contact by forming an air-core transformer. An example NFC radio operates within the unlicensed radio frequency ISM band of 13.56 MHz, with a bandwidth of approximately 2 MHz over a typical distance of a few centimeters. The NFC radio may be affixed to a new wireless client device (STA) and the user brings the NFC radio on the device close to an access point (AP) or Registrar of the Network to allow near field communication between the devices.

[0075] NFC technology is an extension of the ISO/IEC 14443 proximity-card standard (incorporated herein by reference) for contactless smartcards and radio frequency ID (RFID) devices, which combines the interface of a contactless smartcard and a reader into a single device, and uses the ISO/IEC 18092 NFC communication standard (incorporated herein by reference) to enable two-way communication. An NFC radio may communicate with both existing ISO/IEC 14443 contactless smartcards and readers, as well as with other NFC devices by using ISO/IEC 18092. The NFC Forum™, a non-profit industry association, has released specifications that enable different operation modes called: tag emulation, read/write mode, and peer to peer communication. Furthermore, NFC Forum has defined specifications for NFC Data Exchange Format (NDEF), NFC Tag Types, NFC Record Type Definition, and Connection Handover Specification. See, for example, Connection Handover Technical Specification, NFC Forum™, Connection Handover 1.2, NFCForum_1.2, 2010-07-07 (incorporated herein by reference). The ISO/IEC 18092 standard defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductively coupled devices operating at the center frequency of 13.56 MHz for interconnection of computer peripherals. The ISO/IEC 18092 standard specifies modulation schemes, codings, transfer speeds and frame format of the RF interface, initialization schemes, conditions required for data collision control during initialization, and a transport protocol including protocol activation and data exchange methods.

[0076] The basic handover to a WLAN carrier stores WLAN parameters and credentials on NFC Forum Tags as part of Wi-Fi Protected Setup (WPS). The information is stored in the payload of an NFC Data Exchange Format (NDEF) record identified by the mime-type "application/vnd.wfa.wsc", known as the "WPS Record". The wireless LAN parameters and credentials information provided inside a WPS Record includes the IEEE 802.11 Service Set Identifier (SSID), authentication and encryption type deployed by the wireless network, the secret network key that a wireless station needs to authenticate with the network, and the MAC address of the device receiving the configuration (if unknown, this address is set to all-zeros). The Wi-Fi Protected Setup specification 1.0 uses the term "Registrar" for a device that is able to provide WLAN credentials and "Enrollee" for a device

that wants to join a wireless network.

[0077] In the Wi-Fi Simple Configuration Specification, Version 2.0, December 20, 2010, a Handover Requester with Wi-Fi capability may format an NFC Handover Request Message in the NFC Data Exchange Format (NDEF), which indicates that the requester is an IEEE 802.11 device, but which does not include any configuration information. A Handover Request may be sent via the NFC link in at least two scenarios: [1] the requester may not have yet joined a wireless domain or [2] even if the requester is already member of a WLAN network, a peer device may be in a different network and thus a Connection Handover is required to obtain the peer device's credentials. In the Wi-Fi Protected Setup specification 2.0, the Handover Selector would deduce from this message that the Handover Requester supports a Wi-Fi certified IEEE 802.11 radio. In the Wi-Fi Protected Setup specification 2.0, if the Handover Selector is a Wi-Fi device with wireless connectivity, it should respond with an NFC Handover Select Message in the NFC Data Exchange Format (NDEF), with a configuration record that includes credentials, such as network index, SSID, authentication type, encryption type, network key, and MAC address.

[0078] The NFC Data Exchange Format (NDEF) specification, NFC Forum Data Exchange Format (NDEF) Specification, NFC Forum™, 2006 (incorporated herein by reference), defines a common data format for NFC devices to exchange application or service specific data. An NDEF message is constructed of a number of NDEF records, with the first and the last record providing message begin and end markers. Between two NFC Devices, NDEF messages may be exchanged over the NFC Logical Link Control Protocol (LLCP) protocol, specified in NFC Forum Logical Link Control Protocol Specification, NFC Forum™, 2009 (incorporated herein by reference). The NFC Connection Handover specification, NFC Forum Connection Handover Specification, NFC Forum™, 2010-07-07 (incorporated herein by reference), defines the exchange of NDEF messages between two NFC Devices in a negotiated handover to discover and negotiate alternative wireless communication technologies.

[0079] The Handover Requester in the Wi-Fi Protected Setup specification 2.0, would then typically use the SSID and Network Key to enroll on the same Wi-Fi network to which the Handover Selector is connected. Further actions depend on the provision of an IP address identifying the Handover Selector, the available services, and the Handover Requester's intended activity.

E. Power Save Control For Tethering Connections

[0080] A hotspot may be a location that offers Internet access via one or more WLAN access points installed at the location. For example, stationary hotspots in coffee shops and other public places may offer free access to the Internet, up to a maximum number of users. A mobile hotspot may be a mobile telephone or smartphone that

has WLAN communication capability and serves as a WLAN gateway to the cellular telephone network. The mobile hotspot enables other WLAN-capable devices that are tethered to the mobile hotspot, to relay their traffic via the WLAN connection and the cellular telephone network, to the Internet. The mobile hotspot may also relay traffic between tethered devices.

[0081] Setting up the WLAN tethering option in a smartphone may require assigning an SSID network name and passkey for the smartphone and the smartphone may automatically issue an IP address. Then, to connect another WLAN-capable device as a tethered device via a WLAN connection to the smartphone, the SSID, passkey, and IP address may need to be entered into the tethered device.

[0082] In accordance with an example embodiment of the invention, the configuration of the WLAN tethering connections with the SSID and passkeys may be automatically set up in a user friendly manner, so that that the user does not need to enter set up data into any other of the WLAN-capable devices.

[0083] WLAN tethering may consume significant power in a mobile hotspot device, since the device may need to stay active as a gateway device for other client devices, even if there is no ongoing data traffic or other client devices. Further, the mobile hotspot device may need to transmit beacons regularly to maintain connections, wasting the device's battery power.

[0084] In accordance with an example embodiment of the invention, to minimize power consumption in the mobile hotspot device, a control connection is initially established between the mobile hotspot device and the client wireless device using an out-of-band communications connection in an out-of-band communications medium, such as Bluetooth, Bluetooth Low Energy, or Near Field Communications. The mobile hotspot device and the client wireless device may then exchange over the control channel, in-band communications connectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and passkeys. The mobile hotspot device and the client wireless device may further exchange over the control channel, in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN. In this manner the mobile hotspot device A may relay communications between the wireless device B and a wide area communications network, such as a cellular telephone network, and enable WLAN power save features of the WLAN tethering connection. The mobile hotspot device A may also relay communications between devices connected to the mobile hotspot device.

[0085] Figure 1 is an example network diagram of a mobile wireless hotspot device A with its Bluetooth circuit 14A and the other wireless device B with its Bluetooth circuit 14B, exchanging information 50 that may be re-

quired to create a Bluetooth control channel connection between the mobile hotspot device A and the wireless device B. The devices may exchange the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, in accordance with example embodiments of the invention. If the Bluetooth control channel connection setup requires authentication, link keys may be initially exchanged using a Near Field Communications link, for example, with an NFC Data Exchange Format (NDEF) configuration record that includes the link keys. As a result, setting up the WLAN tethering option in a smartphone and in tethered wireless devices may be performed as a part of the initial device set-up, requiring minimal user involvement.

[0086] The figure shows two stationary hotspot access points AP1 and AP2 at fixed locations, connected to the Internet 46. When the other wireless device B is within communication range of at least one of the stationary hotspot access points AP1 or AP2, it may use that stationary access point within range to access the Internet 46. If the other wireless device B moves beyond the communication range of any of the stationary hotspot access points AP1 and AP2, the other wireless device B may still be able to access the internet 46 by becoming tethered over a WLAN connection to the mobile hotspot device A. The mobile hotspot device A may serve as a WLAN gateway to the cellular base station 18, cellular telephone network 39, internet gateway 44, and Internet 46. The mobile hotspot device A may then relay the communications traffic of the other wireless device B, via the WLAN tethering connection between the devices A and B, and via the cellular telephone network 39 and internet gateway 44, to the Internet 39.

[0087] In another example embodiment of the invention, the devices may exchange the Bluetooth MAC address of the hotspot device, the Bluetooth MAC address of the wireless device, Bluetooth pairing information, and shared secret for establishing the control channel, via the cellular telephone network connected to a server that provides this information.

[0088] Figure 1A is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1, establishing the Bluetooth control channel 52 between the Bluetooth circuit 14A and the Bluetooth circuit 14B, in accordance with example embodiments of the invention.

[0089] Figure 1B is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1A,

[0090] In accordance with an example embodiment of the invention, request message 54 may request a tethering connection requesting the mobile hotspot device A to relay communications between wireless device B, via cellular base station 18 and Internet 46, to either the social network server 36 or the other network server 37. Request message 54 may request a tethering connection

requesting the mobile hotspot device A to relay communications between wireless device B, via cellular base station 18 and over one or more cellular wireless connections 19 to one or more wireless devices C. Request message 54 may request a tethering connection requesting the mobile hotspot device A to relay communications between wireless device B and over one or more WLAN connections 13 to one or more wireless devices D connected to the hotspot device A. The figure shows a second WLAN circuit 12' on the mobile hotspot device A, shown to clarify the description of the WLAN connection 13 to the wireless device D, however, the mobile hotspot device A may accomplish its WLAN communications with the single WLAN circuit 12.

[0091] In another example embodiment of the invention, the mobile hotspot device A may receive a request from the client wireless device D over a Bluetooth control channel between Bluetooth circuits 14D and 14A, for a WLAN tethering connection for relaying by the mobile hotspot device A, communications between the wireless device D and one or more entities in at least one of the cellular telephone network 18 and a wireless local area network provided by the mobile hotspot device A, in accordance with example embodiments of the invention.

[0092] Figure 1C is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1B, exchanging over the Bluetooth control channel 52, WLAN connectivity configuration information 56. The mobile hotspot device A and the client wireless device B may exchange over the control channel 52, by at least one of transmitting or receiving in-band communications connectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and passkeys, a required authentication procedure, the public key of the mobile hotspot device A, available data rates, available data throughput, a required site blacklist for virus protection, and the like.

[0093] In accordance with an example embodiment of the invention, the mobile hotspot device A and the wireless device B may further exchange over the Bluetooth control channel 52, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in the in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN. Example power saving features may include scheduled sleep and awake periods wherein both the mobile hotspot device A and the wireless device B observe substantially the same sleep and awake periods. Control information may also be exchanged to optimize the timing of the sleep and awake periods in the WLAN tethering connection, in accordance with example embodiments of the invention.

[0094] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may exchange over a Bluetooth control channel between Bluetooth circuits 14D and 14A, by at least one of transmitting or receiving in-band communications con-

nectivity configuration information, such as IEEE 802.11 WLAN tethering connections with the SSID and pass-keys, a required authentication procedure, the public key of the mobile hotspot device A, available data rates, available data throughput, a required site blacklist for virus protection, and the like. The mobile hotspot device A and the wireless device D may further exchange over the Bluetooth control channel between Bluetooth circuits 14D and 14A, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in the in-band communications tethering connection with the wireless device in an in-band communications medium, such as IEEE 802.11 WLAN, in accordance with example embodiments of the invention.

[0095] Figure 1D is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1C, establishing the WLAN tethering connection 58 between the WLAN circuit 12A of the mobile wireless hotspot A and the WLAN circuit 12B of the wireless device B. The figure shows the transitioning, by the mobile hotspot device A, from a WLAN idle state to a WLAN active state, using the power saving features and optimized activity times for the WLAN tethering connection 58, in response to receiving the request 54 over the Bluetooth control channel 52, in accordance with example embodiments of the invention.

[0096] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may establish a WLAN tethering connection between the WLAN circuit 12A' of the mobile wireless hotspot A and the WLAN circuit 12D of the wireless device B, in response to receiving the request over the Bluetooth control channel between Bluetooth circuits 14D and 14A, in accordance with example embodiments of the invention.

[0097] Figure 1E is an example network diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging messages for adjustments 59 in the WLAN connectivity configuration information to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention. WLAN traffic 75 from the wireless device B is shown being relayed by the mobile hotspot device A from its cell phone circuit 18A as the relayed traffic 75' to the antenna 17 of the cellular base station 18. The cellular base station 18 passes the traffic on to the telephone network 39, and internet gateway 44 to the Internet 46, towards a destination server 36, in accordance with example embodiments of the invention. The destination server 36 may be a social network server connected to the Internet 46.

[0098] In another example embodiment of the invention, the mobile hotspot device A and the client wireless device D may exchange over a Bluetooth control channel between Bluetooth circuits 14D and 14A, messages for adjustments in the WLAN connectivity configuration in-

formation to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection between the WLAN circuit 12A' of the mobile wireless hotspot A and the WLAN circuit 12D of the wireless device B, in accordance with example embodiments of the invention.

[0099] Figure 1F is an example network diagram of the mobile wireless hotspot device A of Figure 1E, transitioning from the WLAN active state to the WLAN idle state of the WLAN tethering connection, when no requests are received from any wireless device, for a WLAN tethering connection for relaying by the mobile hotspot device A, communications between the any wireless device and the cellular telephone network 18, in accordance with example embodiments of the invention.

[0100] Figure 1G is an example flow diagram 100 of the operation of the mobile hot spot device A, wherein tethering is active in step 102 until here are no active clients as determined in step 104. If there are no active clients, then the mobile hot spot A goes into the idle state in step 106 and may check that its Bluetooth control radio 14A is turned on and that all connected clients support the power save feature. After receiving a tethering request from a client in step 108, the mobile hot spot A turns on mobile tethering in s102 and may also inform the client that it is up and running, in accordance with example embodiments of the invention.

[0101] Figure 2A is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 1D, exchanging adjustments 59 in the WLAN connectivity configuration information over the Bluetooth control channel 52, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention.

[0102] In accordance with an embodiment of the invention, mobile hotspot device A further includes an NFC reader/writer 16A, a Bluetooth transceiver 14A, a IEEE 802.11 WLAN transceiver 12A, and a cellular telephone transceiver 18A. The cellular telephone transceiver 18A may be based on Wide Area (WAN) communications protocols that include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0103] In an example embodiment of the invention, the mobile hotspot device A may be a device having an overall function as a PDA, cell phone, laptop or palmtop computer, or the like. The mobile hotspot device A includes a processor 20 that includes a single core, dual core or multi-core central processing unit (CPU_1 and CPU_2), a random access memory (RAM), a read only memory (ROM), and interface circuits to interface with circuits, such as a cell phone radio, a battery and other power sources, key pad, touch screen, display, microphone, speakers, ear pieces, camera or other imaging devices, etc. in the device A. The RAM and ROM may be remov-

able memory devices 126 such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMs, flash memory devices, etc., as shown in Figure 4. The IEEE 802.11 MAC and PHY 12A, provide the medium access control and radio for IEEE 802.11 WLAN communications. The mobile hotspot device A may include a user interface such as a key pad and a location detection device such as the global positioning system (GPS). Device A may measure its location by the GPS, by cellular telephone Cell-ID sensed by the wide area wireless transceiver 18A, or by WLAN signals sensed by the IEEE 801.11 transceiver 12A, for example. With reference to Figure 2B, the other wireless device B has similar components to mobile hotspot device A in Figure 2A.

[0104] In an example embodiment of the invention, the mobile hotspot device A may include the connectivity management system 28A, to read device capabilities of the mobile hotspot device A. The connectivity management system 28A may generate the user specific device connectivity configurations to enable the other wireless device B, to automatically connect to the mobile hotspot device A as a tethered wireless device, the connectivity configurations including a specification of a WLAN tethering connection having a network name (SSID) and passkey.

[0105] Figure 2B is an example functional block diagram of the mobile wireless hotspot device A and the other wireless device B of Figure 2A, exchanging adjustments 59' in the WLAN connectivity configuration information over the Near Field Communications (NFC) control channel via the NFC reader/writer 16A and NFC reader/writer 16B, to modify at least one of the power saving features and optimized activity times in the WLAN tethering connection 58, in accordance with example embodiments of the invention. In an example embodiment of the invention, the mobile wireless hotspot device A and the other wireless device B of Figure 2A, may exchange adjustments 59' in the WLAN connectivity configuration information over another local connectivity channel having low power.

[0106] In an example embodiment of the invention, the connectivity management system 28A in the mobile hotspot device A, may read device capabilities mobile hotspot device A. The connectivity management system 28A may generate user specific device connectivity configurations to enable a other wireless device B, to automatically connect to the mobile hotspot device A as a tethered wireless device, the connectivity configurations including specification of a WLAN tethering connection having a network name and passkey. The connectivity management system 28A may receive from the other wireless device B, a WLAN tethering connection request based on the user specific device connectivity configurations.

[0107] In an example embodiment of the invention, the other wireless device B may exchange information directly with the mobile hotspot device A via a short range communications link, such as the Bluetooth (or Bluetooth

Low Energy) circuits 14A and 14B or the Near Field Communications (NFC) reader/writer circuits 16A and 16B.

[0108] Figure 3A is an example flow diagram 300 of the process performed by mobile hotspot device A, in accordance with example embodiments of the invention. The steps of the flow diagram represent computer code instructions stored in the RAM and/or ROM memory of the mobile hotspot device A, which when executed by the central processing units (CPU), carry out the functions of the example embodiments of the invention. The steps may be carried out in another order than shown and individual steps may be combined or separated into component steps. Additional steps may be included in this sequence. The steps of the example method are as follows.

[0109] Step 302: establishing, by a mobile hotspot device, a control channel with a wireless device, using an out-of-band communications connection in an out-of-band communications medium; and

[0110] Step 304: exchanging, by the mobile hotspot device over the control channel, with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the wireless device in an in-band communications medium, for relaying by the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network and a wireless local area network provided by the mobile hotspot device.

[0111] Figure 3B is an example flow diagram 350 of the process performed by the other wireless device B, in accordance with example embodiments of the invention. The steps of the flow diagram represent computer code instructions stored in the RAM and/or ROM memory of the other wireless device B, which when executed by the central processing units (CPU), carry out the functions of the example embodiments of the invention. The steps may be carried out in another order than shown and individual steps may be combined or separated into component steps. Additional steps may be included in this sequence. The steps of the example method are as follows.

[0112] Step 352: establishing, by a wireless device, a control channel with a mobile hotspot device, using an out-of-band communications connection in an out-of-band communications medium; and

[0113] Step 354: exchanging, by the wireless device over the control channel, with the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection with the mobile hotspot device in an in-band communications medium, for relaying by the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications

network and a wireless local area network provided by the mobile hotspot device.

[0114] Figure 4 illustrates an example embodiment of the invention, wherein examples of removable storage media 126 are shown, based on magnetic, electronic and/or optical technologies, such as magnetic disks, optical disks, semiconductor memory circuit devices and micro-SD memory cards (SD refers to the Secure Digital standard) for storing data and/or computer program code as an example computer program product, in accordance with at least one embodiment of the present invention.

[0115] In an alternate example embodiment of the invention, RFID transponders may be used in devices A and B, which may be the passive type or the active type, instead of the NFC transponders. A passive RFID transponder requires no internal power source to communicate with an RFID reader, and is only active when it is near an RFID reader that energizes the transponder with a continuous radio frequency signal at a resonant frequency of the antenna. The small electrical current induced in the antenna by the continuous radio frequency signal provides enough power for an integrated circuit in the transponder to power up and transmit a modulated response, typically by backscattering the continuous carrier wave from the RFID reader. A passive RFID transponder may include writable electrically erasable, programmable, read-only memory (EEPROM) for storing data received from the RFID reader, which modulates the continuous carrier wave sent by the RFID reader. Reading distances for passive RFID transponders typically range from a few centimeters to a few meters, depending on the radio frequency and antenna design. By contrast, active RFID transponders require a power source to receive and transmit information with an RFID reader. The RFID transponder may be affixed to or integrated with the wireless device A and device B and the user brings the RFID transponder on the device A close to an RFID reader circuit in device B to allow near field communication between the devices. In example embodiments, both devices A and B may have RFID reader circuits to read RFID signals from the other device.

[0116] In an example embodiment, the wireless transceiver carrier in device A and device B may be a suitable short-range communications protocol, such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Infrared Data Association (IrDA), or Ultra Wide Band (UWB), for example.

[0117] An example of the Radio Frequency Identification (RFID) out-of-band short-range carrier is described, for example, ISO 11785 (air interface protocol), ISO 14443 (air interface protocol), and ISO 15693, incorporated herein by reference.

[0118] An example of the Near Field Communication (NFC) out-of-band short-range carrier is described, for example, in ISO/IEC 14443 and ISO/IEC 18092, incorporated herein by reference.

[0119] An example of the Infrared Data Association (IrDA) out-of-band short-range carrier is described, for ex-

ample, in IrDA Link Access Protocol, v1.1 (1996), incorporated herein by reference.

[0120] An example of the Ultra Wide Band (UWB) out-of-band short-range carrier is described, for example, in WiMedia Common Radio Platform Specification, Version 1.5 (2010), incorporated herein by reference.

[0121] In example embodiments, the wireless transceiver carrier in device A and device B may be a suitable communications protocol, such as a Vehicle Area (WVAN) communications protocol, Wireless Video Networks (WVAN-TV) communications protocol, Personal Area (WPAN) communications protocol, Local Area (WLAN) communications protocol, or Wide Area (WAN) communications protocol, using the standard procedures and primitives defined by the respective standards. Personal Area (WPAN) communications protocols include Bluetooth BR/EDR, Bluetooth Low Energy, Wireless USB (WUSB), Ultra Wide-band (UWB), ZigBee (IEEE 802.15.4, or IEEE 802.15.4a) for short range communication between devices. Local Area (WLAN) communications protocols include IEEE 802.11, digital enhanced cordless telecommunications (DECT) and HIPERLAN. Wide Area (WAN) communications protocols include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0122] Using the description provided herein, the embodiments may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0123] Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media such as resident memory devices, smart cards or other removable memory devices, or transmitting devices, thereby making a computer program product or article of manufacture according to the embodiments. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program.

[0124] As indicated above, memory/storage devices include, but are not limited to, disks, optical disks, removable memory devices such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, etc. Transmitting mediums include, but are not limited to, transmissions via wireless communication networks, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links.

[0125] Although specific example embodiments have been disclosed, a person skilled in the art will understand

that changes can be made to the specific example embodiments without departing from the scope of the invention.

[0126] An example of the Infrared Data Association (IrDA) out-of-band short-range carrier is described, for example, in IrDA Link Access Protocol, v1.1 (1996), incorporated herein by reference.

[0127] An example of the Ultra Wide Band (UWB) out-of-band short-range carrier is described, for example, in WiMedia Common Radio Platform Specification, Version 1.5 (2010), incorporated herein by reference.

[0128] In example embodiments, the wireless transceiver carrier in device A and device B may be a suitable communications protocol, such as a Vehicle Area (WVAN) communications protocol, Wireless Video Networks (WVAN-TV) communications protocol, Personal Area (WPAN) communications protocol, Local Area (WLAN) communications protocol, or Wide Area (WAN) communications protocol, using the standard procedures and primitives defined by the respective standards. Personal Area (WPAN) communications protocols include Bluetooth BR/EDR, Bluetooth Low Energy, Wireless USB (WUSB), Ultra Wide-band (UWB), ZigBee (IEEE 802.15.4, or IEEE 802.15.4a) for short range communication between devices. Local Area (WLAN) communications protocols include IEEE 802.11, digital enhanced cordless telecommunications (DECT) and HIPERLAN. Wide Area (WAN) communications protocols include Global System for Mobile Communications (GSM), General Packet Radio service (GPRS), Enhanced data rates for GSM evolution (EDGE), Evolution-Data Optimized (EV-DO), and Wideband Code Division Multiple Access (W-CDMA).

[0129] Using the description provided herein, the embodiments may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0130] Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media such as resident memory devices, smart cards or other removable memory devices, or transmitting devices, thereby making a computer program product or article of manufacture according to the embodiments. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program.

[0131] As indicated above, memory/storage devices include, but are not limited to, disks, optical disks, removable memory devices such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, etc. Transmitting mediums include, but are not limited to, transmissions via wireless communication networks, the Internet, intranets, telephone/modem-based network

communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links.

[0132] Although specific example embodiments have been disclosed, a person skilled in the art will understand that changes can be made to the specific example embodiments without departing from the scope of the invention.

Claims

1. A method, comprising:

establishing (302), by an apparatus operating as a mobile hotspot device, a control channel (52) over a wireless out-of-band communications medium with a wireless device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and exchanging (304), by the apparatus operating as the mobile hotspot device, over the established control channel (52), by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of a wide area communications network (39,46) and/or a wireless local area network provided by the apparatus operating as the mobile hotspot device.

2. The method of claim 1, further comprising:

receiving, by the apparatus operating as the mobile hotspot device, over the control channel (52), a request from the wireless device for the in-band communications tethering connection (58) for relaying, by the apparatus operating as the mobile hotspot device, communications between the wireless device and one or more entities in at least one of the wide area communications network (39,46) and/or the wireless local area network provided by the apparatus operating as the mobile hotspot device; performing, by the apparatus operating as the mobile hotspot device, said exchanging over the control channel (52), with the wireless device, of the in-band communications connectivity configuration information, in response to receiving

- the request; and
 transitioning, by the apparatus operating as the mobile hotspot device, from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection (58), in response to receiving the request.
3. The method of claim 1 or claim 2, further comprising:
 exchanging, by the apparatus operating as the mobile hotspot device, over the control channel, with the wireless device, adjustments (59,59') in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection (58) with the wireless device.
4. The method of any of the preceding claims, further comprising:
 transitioning, by the apparatus operating as the mobile hotspot device, from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection (58), when no requests are received from any wireless device for the in-band communications tethering connection.
5. The method of any of the preceding claims, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.
6. A method, comprising:
 establishing (352), by a wireless device, a control channel (52) over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said establishing of the control channel with the wireless device comprises exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and
 exchanging (354), by the wireless device over the control channel (52), with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device in an in-band communications medium.
7. The method of claim 6, further comprising:
 transmitting, by the wireless device, over the control channel (52), a request to the apparatus operating as the mobile hotspot device for the in-band communications tethering connection (58);
 performing, by the wireless device, said exchanging over the control channel (52), with the apparatus operating as the mobile hotspot device, of the in-band communications connectivity configuration information; and
 establishing, by the wireless device, the in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device, using the power saving features and optimized activity times for the in-band communications tethering connection.
8. A computer program comprising computer readable program code configured to cause performing of the method of any of the preceding claims when said program is run on a computer.
9. The computer program product of claim 8, wherein the computer program is a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.
10. An apparatus operable as a mobile hotspot device, comprising:
 means (14A) for establishing a control channel (52) over a wireless out-of-band communications medium with a wireless device, wherein said means for establishing the control channel with the wireless device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret information; and
 means (14A) for exchanging over the control channel (52), with the wireless device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the wireless device in an in-band communications medium, for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of a wide area communications network (39,46) and/or a wireless local area network provided by the apparatus.
11. The apparatus of claim 10, further comprising:

- means (14A) for receiving over the control channel (52), a request from the wireless device for the in-band communications tethering connection (58) for relaying by the apparatus, communications between the wireless device and one or more entities in at least one of the wide area communications network (39,46) and/or the wireless local area network provided by the apparatus;
- means (14A) for performing said exchanging over the control channel (52), with the wireless device, of the in-band communications connectivity configuration information, in response to receiving the request; and
- means (12A,20) for transitioning from an in-band communications idle state to an in-band communications active state using the power saving features and optimized activity times for the in-band communications tethering connection (58), in response to receiving the request.
12. The apparatus of claim 10 or claim 11, further comprising:
means (14A) for exchanging over the control channel (52), with the wireless device, adjustments in the in-band communications connectivity configuration information to modify at least one of the power saving features and optimized activity times in the in-band communications tethering connection (58) with the wireless device.
13. The apparatus of any of the claims 10-12, further comprising:
means (12A,20) for transitioning from the in-band communications active state to the in-band communications idle state of the in-band communications tethering connection (58), when no requests are received from any wireless device, for an in-band communications tethering connection.
14. The apparatus of any of the claims 10-13, wherein the out-of-band communications medium comprises one of a Bluetooth communications protocol, or a Bluetooth Low Energy communications protocol, and the in-band communications medium comprises a IEEE 802.11 communications protocol.
15. An apparatus, comprising:

means (14B) for establishing a control channel over a wireless out-of-band communications medium with an apparatus operating as a mobile hotspot device, wherein said means for establishing the control channel with the apparatus operating as the mobile hotspot device comprises means for exchanging, via the wireless out-of-band communications medium, at least out-of-band pairing information, or shared secret in-

formation; and
means (14B) for exchanging over the control channel (52), with the apparatus operating as the mobile hotspot device, by at least one of transmitting or receiving in-band communications connectivity configuration information to enable power saving features and optimize activity times in an in-band communications tethering connection (58) with the apparatus operating as the mobile hotspot device in an in-band communications medium.

Patentansprüche

1. Verfahren, umfassend:

Einrichten (302), durch ein Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einer drahtlosen Vorrichtung, wobei das Einrichten des Steuerkanals mit dem drahtlosen Medium umfasst, über das drahtlose Außerbandkommunikationsmedium, zumindest Außerband-Paarungsinformationen oder geteilte geheime Informationen auszutauschen; und
Austauschen (304), durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den eingerichteten Steuerkanal (52) durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungsparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung in einem Inbandkommunikationsmedium zu optimieren, um Kommunikationen durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem eines Weitbereichskommunikationsnetzwerks (39, 46) und/oder eines drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, weiterzuleiten.

2. Verfahren nach Anspruch 1, ferner umfassend:

Empfangen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den Steuerkanal (52), einer Anforderung, von der drahtlosen Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) zum Weiterleiten, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von Kommunikationen zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens ei-

- nem des Weitbereichskommunikationsnetzwerks (39, 46) und/oder des drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird;
- Durchführen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, des Austauschens, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen als Reaktion auf Empfangen der Anforderung; und
- Übergehen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von einem Inbandkommunikation-Ruhezustand zu einem Inbandkommunikation-Aktivzustand unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung (58) als Reaktion auf Empfangen der Anforderung.
3. Verfahren nach Anspruch 1 oder Anspruch 2, ferner umfassend:
- Austauschen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, über den Steuerkanal mit der drahtlosen Vorrichtung, von Anpassungen (59, 59') in den Inbandkommunikation-Konnektivitätskonfiguration-Informationen zum Modifizieren mindestens eines der Leistungssparmerkmale und der optimierten Aktivitätszeiten in der Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung.
4. Verfahren nach einem der vorhergehenden Ansprüche, ferner umfassend:
- Übergehen, durch das Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, von dem Inbandkommunikation-Aktivzustand zu dem Inbandkommunikation-Ruhezustand der Inbandkommunikation-Anbindungsverbindung (58), wenn keine Anforderungen, von einer drahtlosen Vorrichtung, für die Inbandkommunikation-Anbindungsverbindung empfangen werden.
5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Außerbandkommunikationsmedium ein Bluetooth-Kommunikationsprotokoll oder ein Bluetooth-Low-Energy-Kommunikationsprotokoll umfasst und das Inbandkommunikationsmedium ein IEEE 802.11-Kommunikationsprotokoll umfasst.
6. Verfahren, umfassend:
- Einrichten (352), durch eine drahtlose Vorrichtung, eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einem Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, wobei das Einrichten des
- Steuerkanals mit der drahtlosen Vorrichtung umfasst, über das drahtlose Außerbandkommunikationsmedium, zumindest Außerband-Paarungsinformationen oder geteilte geheime Informationen auszutauschen; und
- Austauschen (354), durch die drahtlose Vorrichtung, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, in einem Inbandkommunikationsmedium zu optimieren.
7. Verfahren nach Anspruch 6, ferner umfassend:
- Übertragen, durch die drahtlose Vorrichtung, über den Steuerkanal (52), einer Anforderung, an das Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, für die Inbandkommunikation-Anbindungsverbindung (58);
- Durchführen, durch die drahtlose Vorrichtung, des Austauschens, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen; und
- Einrichten, durch die drahtlose Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung.
8. Computerprogramm, umfassend computerlesbaren Programmcode, konfiguriert zum Bewirken, dass das Verfahren nach einem der vorstehenden Ansprüche durchgeführt wird, wenn das Programm auf einem Computer ausgeführt wird.
9. Computerprogrammprodukt nach Anspruch 8, wobei das Computerprogramm ein Computerprogrammprodukt ist, umfassend ein computerlesbares Medium, das Computerprogrammcode trägt, der darin für Verwendung mit einem Computer verkörpert ist.
10. Gerät, betreibbar als eine mobile Hotspot-Vorrichtung, umfassend:
- Mittel (14A) zum Einrichten eines Steuerkanals (52) über ein drahtloses Außerbandkommunikationsmedium mit einer drahtlosen Vorrich-

tung, wobei das Mittel zum Einrichten des Steuerkanals mit dem drahtlosen Medium Mittel zum Austauschen, über das drahtlose Außerbandkommunikationsmedium, von zumindest Außerband-Paarungsinformationen oder geteilten geheimen Informationen umfasst; und Mittel (14A) zum Austauschen, über den Steuerkanal (52) mit der drahtlosen Vorrichtung durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung in einem Inbandkommunikationsmedium zu optimieren, um Kommunikationen durch das Gerät zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem eines Weitbereichskommunikationsnetzwerks (39, 46) und/oder eines drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät, weiterzuleiten.

11. Gerät nach Anspruch 10, ferner umfassend:

Mittel (14A) zum Empfangen, über den Steuerkanal (52), einer Anforderung, von der drahtlosen Vorrichtung, der Inbandkommunikation-Anbindungsverbindung (58) zum Weiterleiten, durch das Gerät, von Kommunikationen zwischen der drahtlosen Vorrichtung und einer oder mehreren Entitäten in mindestens einem des Weitbereichskommunikationsnetzwerks (39, 46) und/oder des drahtlosen Nahbereichsnetzwerks, bereitgestellt durch das Gerät; Mittel (14A) zum Durchführen des Austauschs, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, der Inbandkommunikation-Konnektivitätskonfiguration-Informationen als Reaktion auf Empfangen der Anforderung; und Mittel (12A, 20) zum Übergehen von einem Inbandkommunikation-Ruhezustand zu einem Inbandkommunikation-Aktivzustand unter Verwendung der Leistungssparmerkmale und optimierten Aktivitätszeiten für die Inbandkommunikation-Anbindungsverbindung (58) als Reaktion auf Empfangen der Anforderung.

12. Gerät nach Anspruch 10 oder Anspruch 11, ferner umfassend:

Mittel (14A) zum Austauschen, über den Steuerkanal (52) mit der drahtlosen Vorrichtung, von Anpassungen in den Inbandkommunikation-Konnektivitätskonfiguration-Informationen zum Modifizieren mindestens eines der Leistungssparmerkmale und der optimierten Aktivitätszeiten in der Inbandkommunikation-Anbindungsverbindung (58) mit der drahtlosen Vorrichtung.

13. Gerät nach einem der Ansprüche 10-12, ferner umfassend:

Mittel (12A, 20) zum Übergehen von dem Inbandkommunikation-Aktivzustand zu dem Inbandkommunikation-Ruhezustand der Inbandkommunikation-Anbindungsverbindung (58), wenn keine Anforderungen, von einer drahtlosen Vorrichtung, einer Inbandkommunikation-Anbindungsverbindung empfangen werden.

14. Gerät nach einem der Ansprüche 10-13, wobei das Außerbandkommunikationsmedium ein Bluetooth-Kommunikationsprotokoll oder ein Bluetooth-Low-Energy-Kommunikationsprotokoll umfasst und das Inbandkommunikationsmedium ein IEEE 802.11-Kommunikationsprotokoll umfasst.

15. Gerät, umfassend:

Mittel (14B) zum Einrichten eines Steuerkanals über ein drahtloses Außerbandkommunikationsmedium mit einem Gerät, das als eine mobile Hotspot-Vorrichtung betrieben wird, wobei das Mittel zum Einrichten des Steuerkanals mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, Mittel zum Austauschen, über das drahtlose Außerbandkommunikationsmedium, von zumindest Außerband-Paarungsinformationen oder geteilten geheimen Informationen umfasst; und Mittel (14B) zum Austauschen, über den Steuerkanal (52) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, durch mindestens eines von Übertragen oder Empfangen, von Inbandkommunikation-Konnektivitätskonfiguration-Informationen, um Leistungssparmerkmale zu aktivieren und Aktivitätszeiten in einer Inbandkommunikation-Anbindungsverbindung (58) mit dem Gerät, das als die mobile Hotspot-Vorrichtung betrieben wird, in einem Inbandkommunikationsmedium zu optimieren.

Revendications

1. Procédé, comprenant les étapes suivantes :

établir (302), par un appareil fonctionnant comme dispositif de point d'accès mobile, un canal de commande (52) sur un support de communication hors bande sans fil avec un dispositif sans fil, où ledit établissement du canal de commande avec le dispositif sans fil comprend le fait d'échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et échanger (304), par l'appareil fonctionnant com-

- me dispositif de point d'accès mobile sur le canal de commande établi (52), par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec le dispositif sans fil dans un support de communication dans la bande, pour relayer par l'appareil fonctionnant comme dispositif de point d'accès mobile, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi un réseau de communication étendu (39, 46) et un réseau local sans fil fourni par l'appareil fonctionnant comme dispositif de point d'accès mobile.
2. Procédé selon la revendication 1, comprenant en outre les étapes suivantes :
- recevoir, par l'appareil fonctionnant comme dispositif de point d'accès mobile, sur le canal de commande (52), une demande provenant du dispositif sans fil pour la connexion de type modem de communication dans la bande (58) pour relayer, par l'appareil fonctionnant comme dispositif de point d'accès mobile, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi le réseau de communication étendu (39, 46) et le réseau local sans fil fourni par l'appareil fonctionnant comme dispositif de point d'accès mobile ;
- procéder, par l'appareil fonctionnant comme dispositif de point d'accès mobile, audit échange sur le canal de commande (52), avec le dispositif sans fil, des informations de configuration de connectivité de communication dans la bande, en réponse à la réception de la demande ; et effectuer une transition, par l'appareil fonctionnant comme dispositif de point d'accès mobile, d'un état de repos de communication dans la bande à un état actif de communication dans la bande utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande (58), en réponse à la réception de la demande.
3. Procédé selon la revendication 1 ou la revendication 2, comprenant en outre l'étape suivante : échanger, par l'appareil fonctionnant comme dispositif de point d'accès mobile, sur le canal de commande, avec le dispositif sans fil, des ajustements (59, 59') dans les informations de configuration de connectivité de communication dans la bande pour modifier au moins un des éléments parmi les fonctionnalités d'économie d'énergie et les temps d'activité optimisés dans la connexion de type modem de communication dans la bande (58) avec le dispositif sans fil.
4. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre les étapes suivantes : effectuer une transition, par l'appareil fonctionnant comme dispositif de point d'accès mobile, de l'état actif de communication dans la bande à l'état de repos de communication dans la bande de la connexion de type modem de communication dans la bande (58), lorsqu'aucune demande n'est reçue d'un quelconque dispositif sans fil, pour la connexion de type modem de communication dans la bande.
5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le support de communication hors bande comprend un protocole de communication Bluetooth ou un protocole de communication Bluetooth à faible énergie, et le support de communication dans la bande comprend un protocole de communication IEEE 802.11.
6. Procédé, comprenant les étapes suivantes :
- établir (352), par un dispositif sans fil, un canal de commande (52) sur un support de communication hors bande sans fil avec un appareil fonctionnant comme dispositif de point d'accès mobile, où ledit établissement du canal de commande avec le dispositif sans fil comprend le fait d'échanger, par l'intermédiaire du support de communication hors bande sans fil au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et échanger (354), par le dispositif sans fil sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile dans un support de communication dans la bande.
7. Procédé selon la revendication 6, comprenant en outre les étapes suivantes :
- transmettre, par le dispositif sans fil, sur le canal de commande (52), une demande à l'appareil fonctionnant comme dispositif de point d'accès mobile pour la connexion de type modem de

- communication dans la bande (58) ;
procéder, par le dispositif sans fil, audit échange sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, des informations de configuration de connectivité de communication dans la bande ; et
établir, par le dispositif sans fil, la connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile, en utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande.
8. Programme informatique comprenant un code de programme lisible par ordinateur configuré pour amener l'exécution du procédé selon l'une quelconque des revendications précédentes lorsque ledit programme est exécuté sur un ordinateur.
9. Produit programme informatique selon la revendication 8, dans lequel le programme informatique est un produit programme informatique comprenant un support lisible par ordinateur intégrant un code de programme informatique destiné à être utilisé avec un ordinateur.
10. Appareil pouvant fonctionner comme dispositif de point d'accès mobile, comprenant :
- des moyens (14A) pour établir un canal de commande (52) sur un support de communication hors bande sans fil avec un dispositif sans fil, où lesdits moyens pour établir le canal de commande avec le dispositif sans fil comprennent des moyens pour échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et
des moyens (14A) pour échanger sur le canal de commande (52), avec le dispositif sans fil, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec le dispositif sans fil dans un support de communication dans la bande, pour relayer par l'appareil des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau de communication étendu (39, 46) et un réseau local sans fil fourni par l'appareil.

11. Appareil selon la revendication 10, comprenant en outre :

des moyens (14A) pour recevoir sur le canal de commande (52) une demande provenant du dispositif sans fil pour la connexion de type modem de communication dans la bande (58) pour relayer, par l'appareil, des communications entre le dispositif sans fil et une ou plusieurs entités dans au moins un réseau parmi le réseau de communication étendu (39, 46) et le réseau local sans fil fourni par l'appareil ;
des moyens (14A) pour procéder audit échange sur le canal de commande (52), avec le dispositif sans fil, des informations de configuration de connectivité de communication dans la bande, en réponse à la réception de la demande ; et
des moyens (12A, 20) pour effectuer une transition d'un état de repos de communication dans la bande à un état actif de communication dans la bande en utilisant les fonctionnalités d'économie d'énergie et les temps d'activité optimisés pour la connexion de type modem de communication dans la bande (58), en réponse à la réception de la demande.

12. Appareil selon la revendication 10 ou la revendication 11, comprenant en outre :

des moyens (14A) pour échanger sur le canal de commande (52), avec le dispositif sans fil, des ajustements dans les informations de configuration de connectivité de communication dans la bande pour modifier au moins un des éléments parmi les fonctionnalités d'économie d'énergie et les temps d'activité optimisés dans la connexion de type modem de communication dans la bande (58) avec le dispositif sans fil.

13. Appareil selon l'une quelconque des revendications 10 à 12, comprenant en outre :

des moyens (12A, 20) pour effectuer une transition de l'état actif de communication dans la bande à l'état de repos de communication dans la bande de la connexion de type modem de communication dans la bande (58), lorsqu'aucune demande n'est reçue d'un quelconque dispositif sans fil, pour une connexion de type modem de communication dans la bande.

14. Appareil selon l'une quelconque des revendications 10 à 13, dans lequel le support de communication hors bande comprend un protocole de communication Bluetooth ou un protocole de communication Bluetooth à faible énergie, et le support de communication dans la bande comprend un protocole de communication IEEE 802.11.

15. Appareil comprenant :

des moyens (14B) pour établir un canal de commande sur un support de communication hors bande sans fil avec un appareil fonctionnant comme dispositif de point d'accès mobile, où lesdits moyens pour établir le canal de commande avec l'appareil fonctionnant comme dispositif de point d'accès mobile comprennent des moyens pour échanger, par l'intermédiaire du support de communication hors bande sans fil, au moins des informations d'appariement hors bande ou des informations confidentielles partagées ; et
des moyens (14B) pour échanger sur le canal de commande (52), avec l'appareil fonctionnant comme dispositif de point d'accès mobile, par au moins une opération parmi la transmission ou la réception des informations de configuration de connectivité de communication dans la bande pour activer des fonctionnalités d'économie d'énergie et optimiser les temps d'activité dans une connexion de type modem de communication dans la bande (58) avec l'appareil fonctionnant comme dispositif de point d'accès mobile dans un support de communication dans la bande.

5

10

15

20

25

30

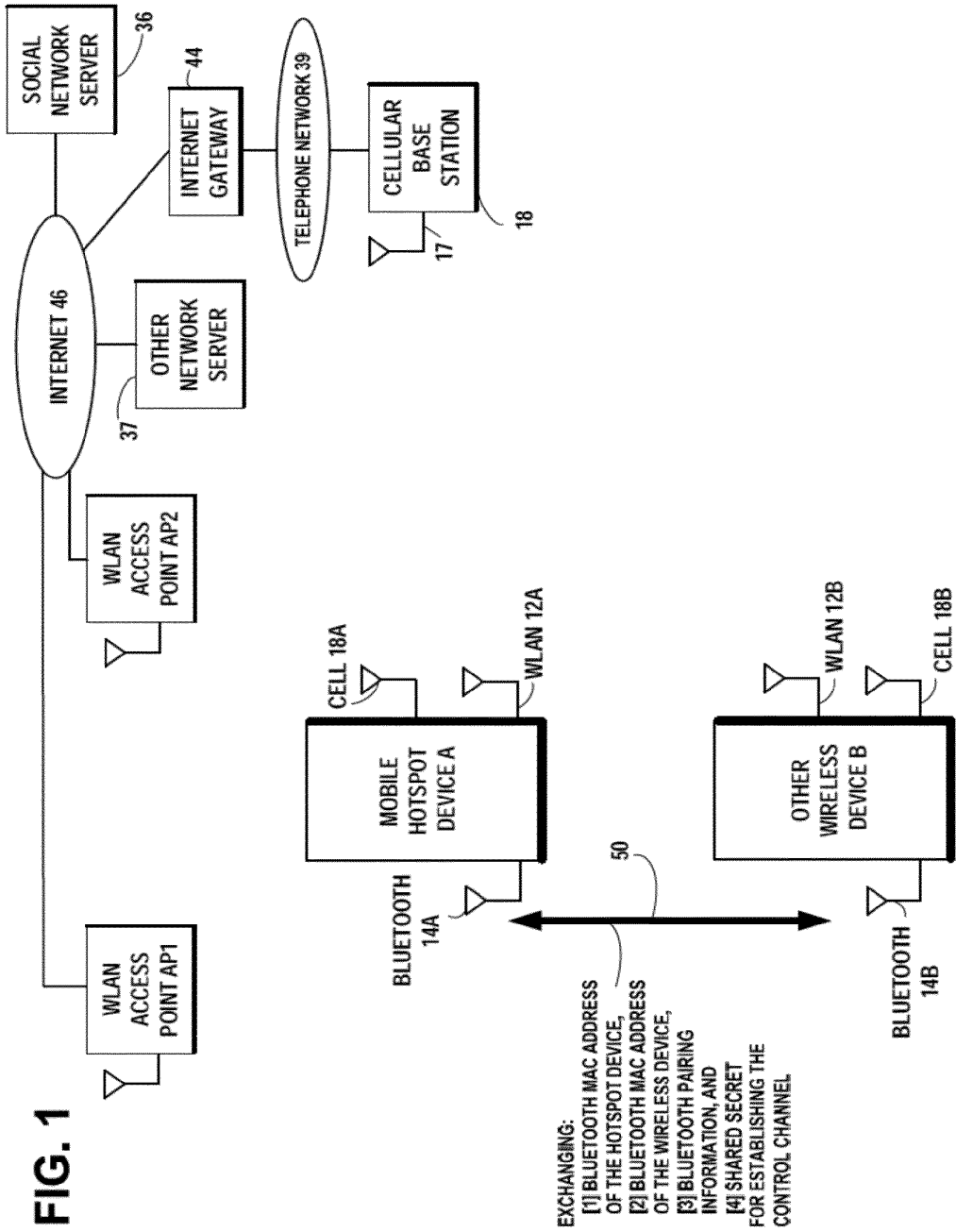
35

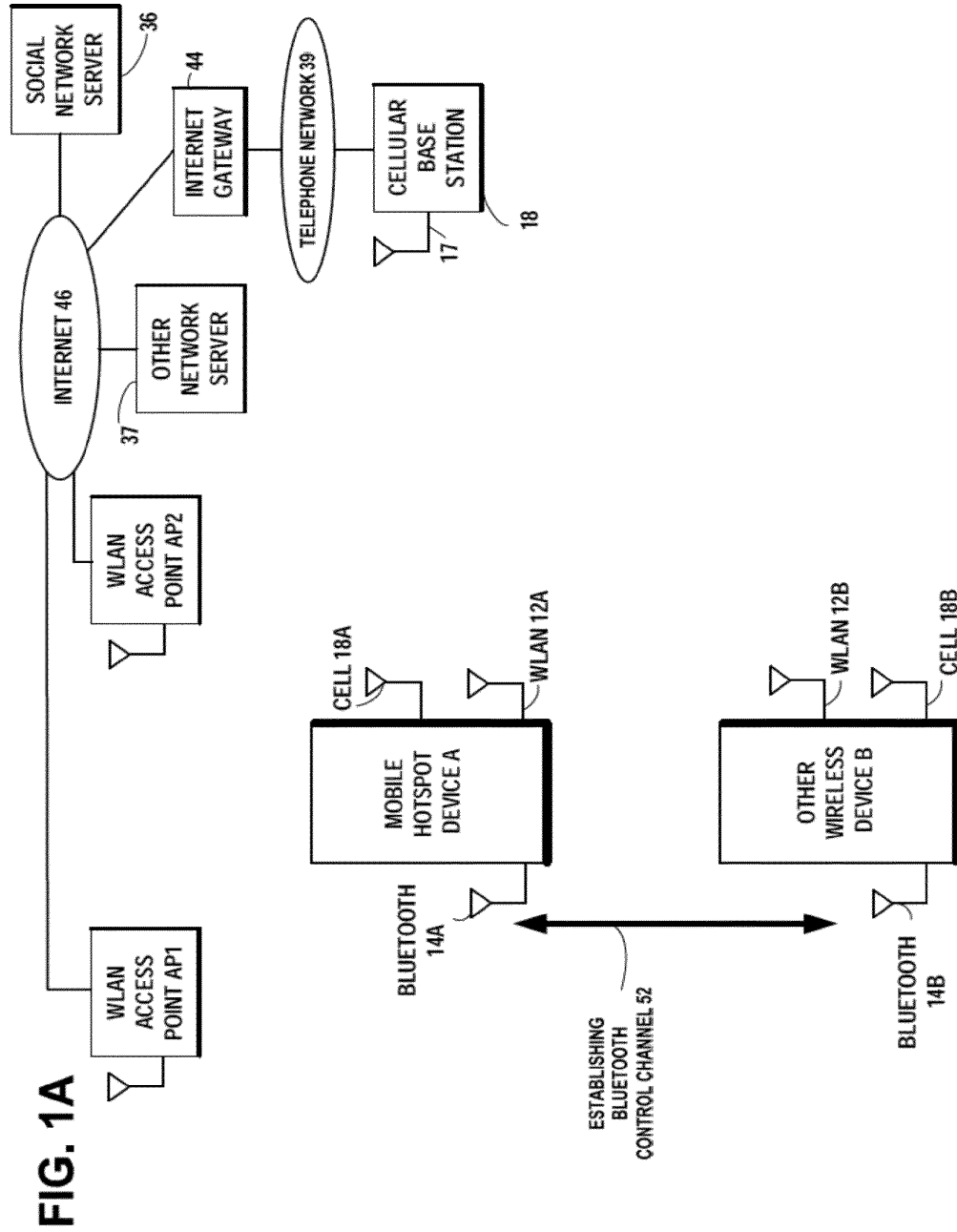
40

45

50

55





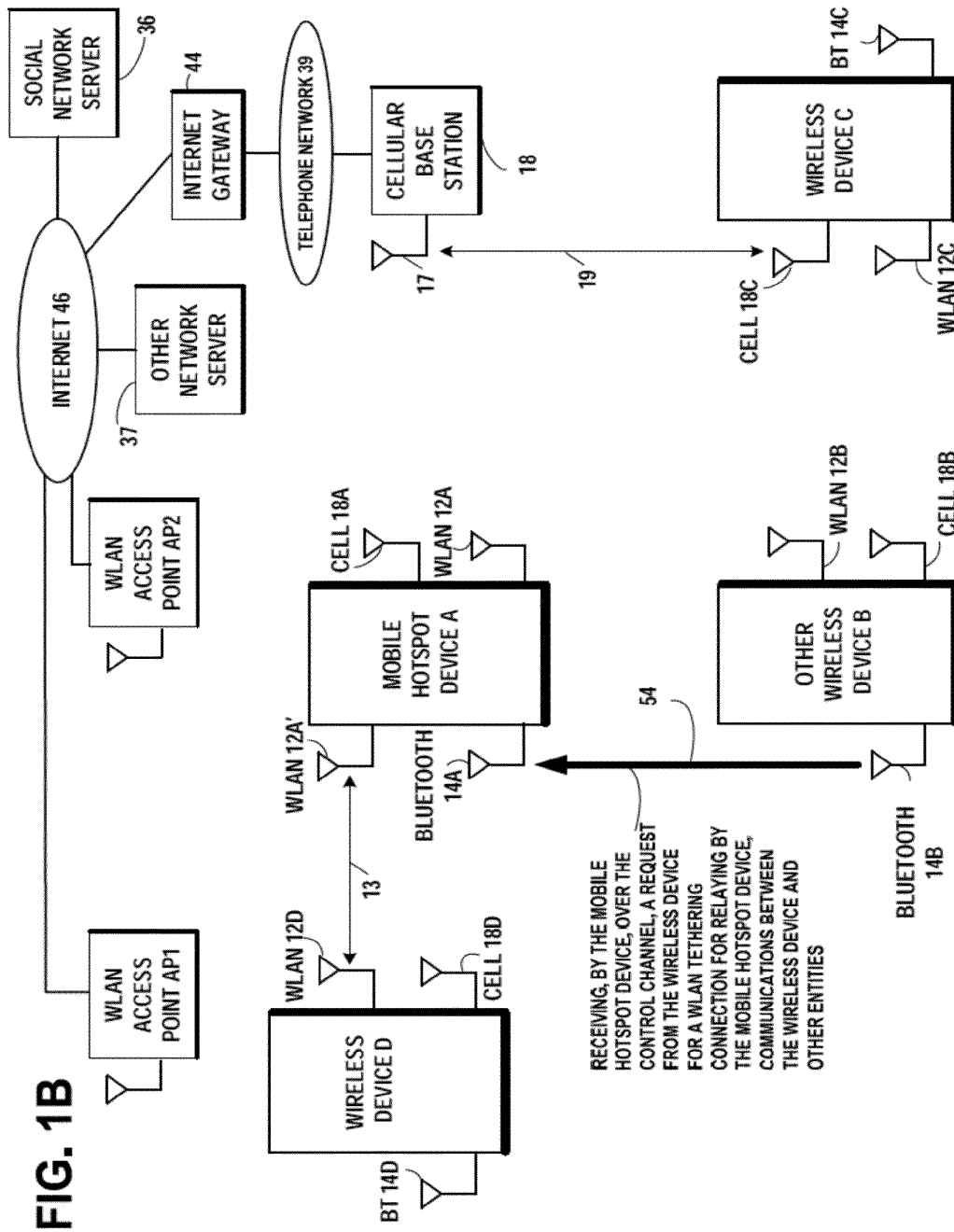
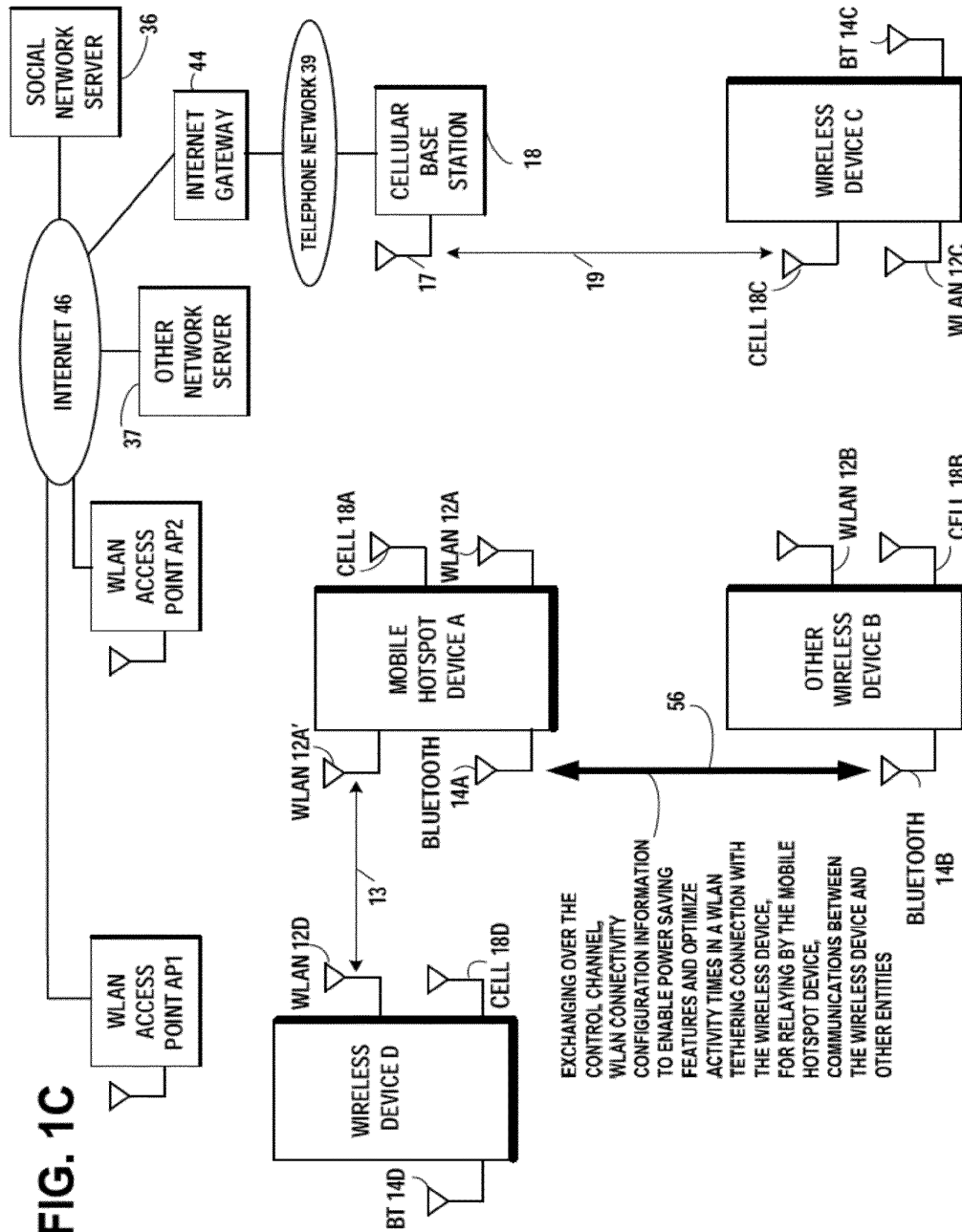


FIG. 1C

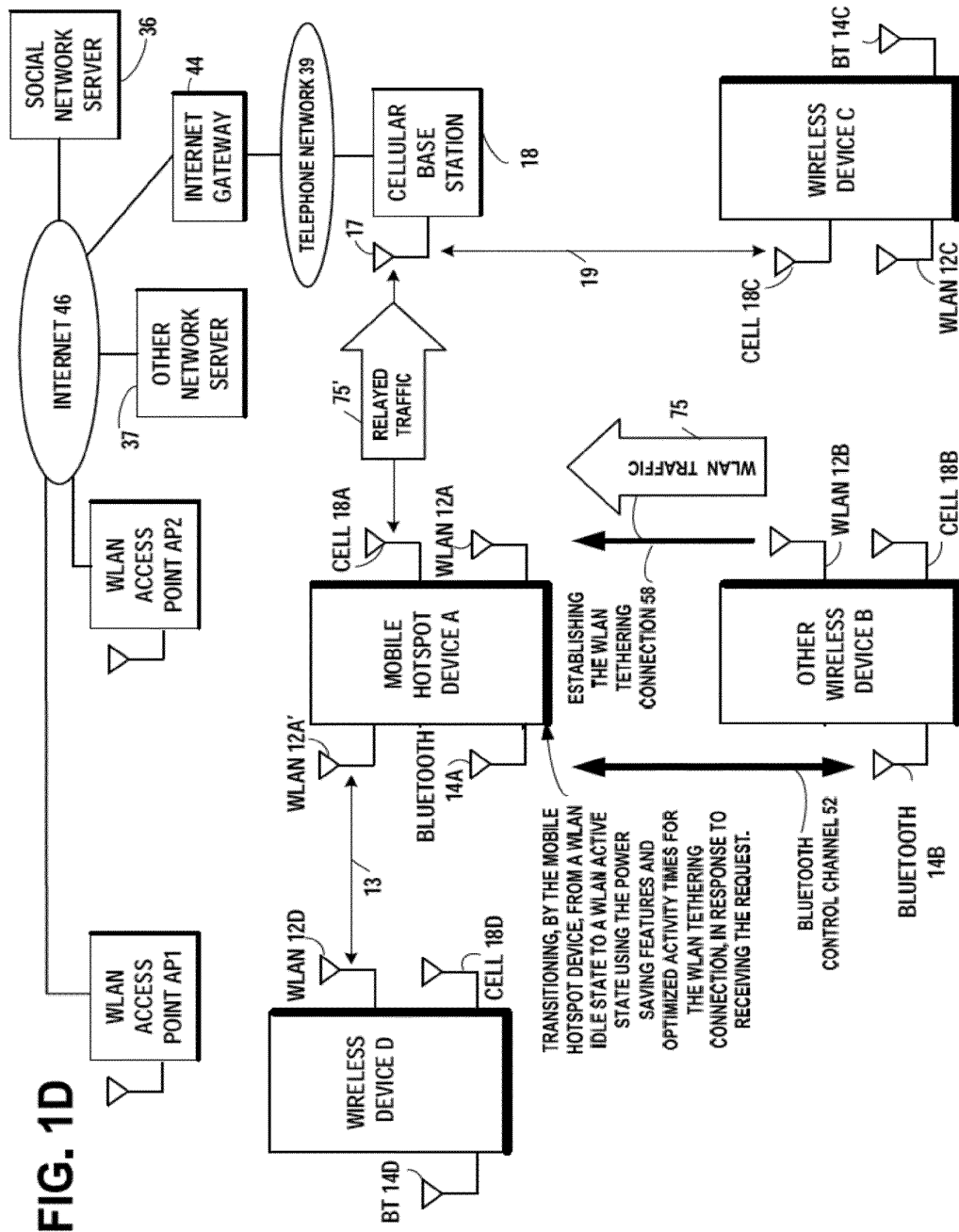
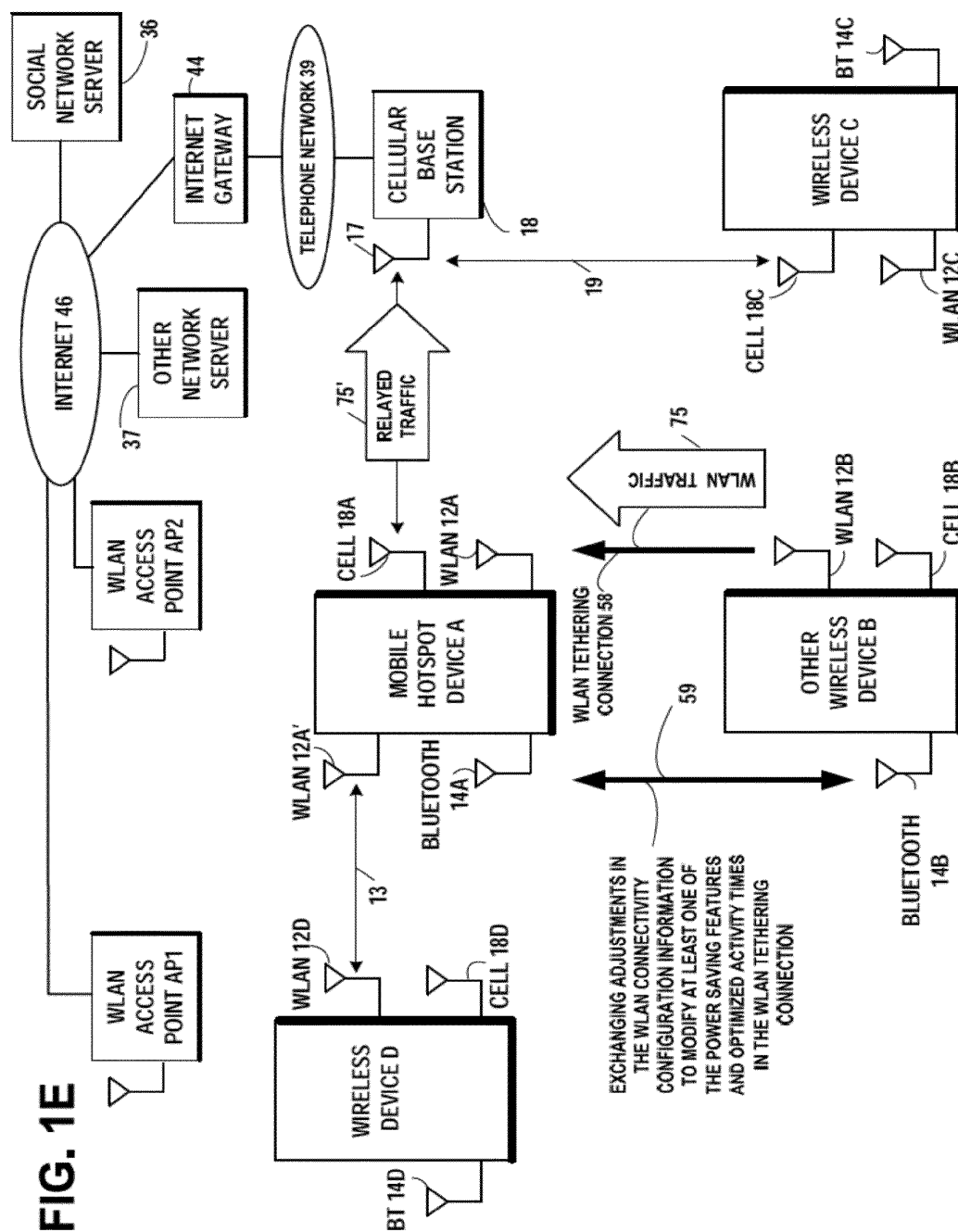


FIG. 1E



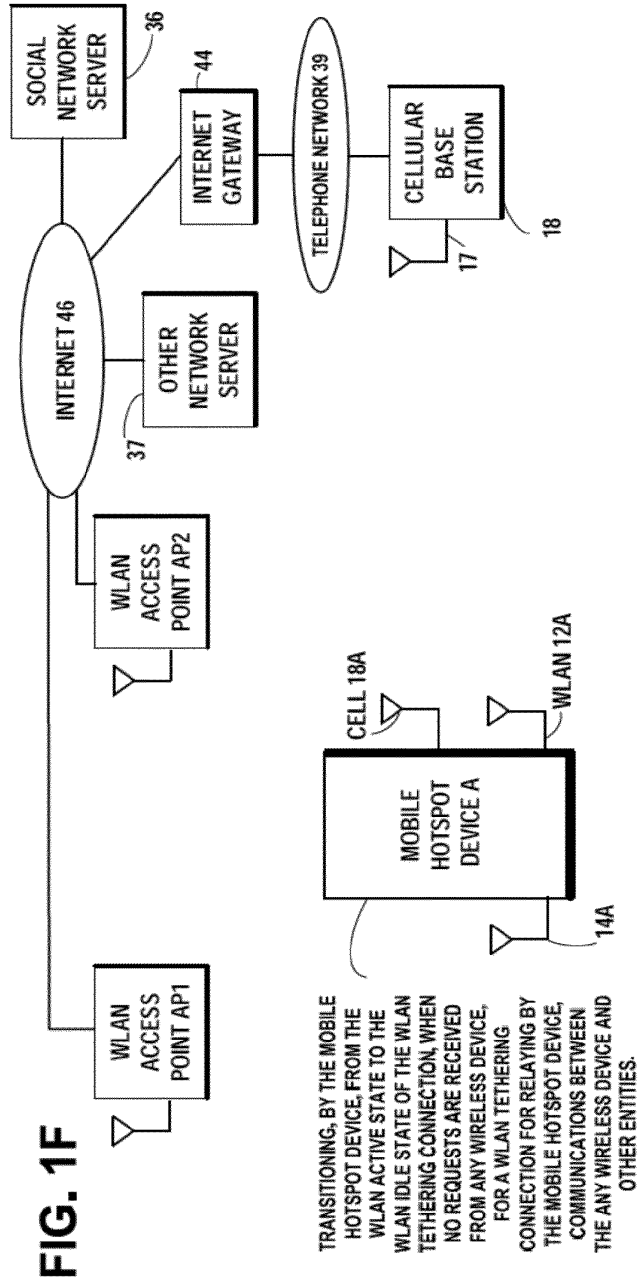


FIG. 1G

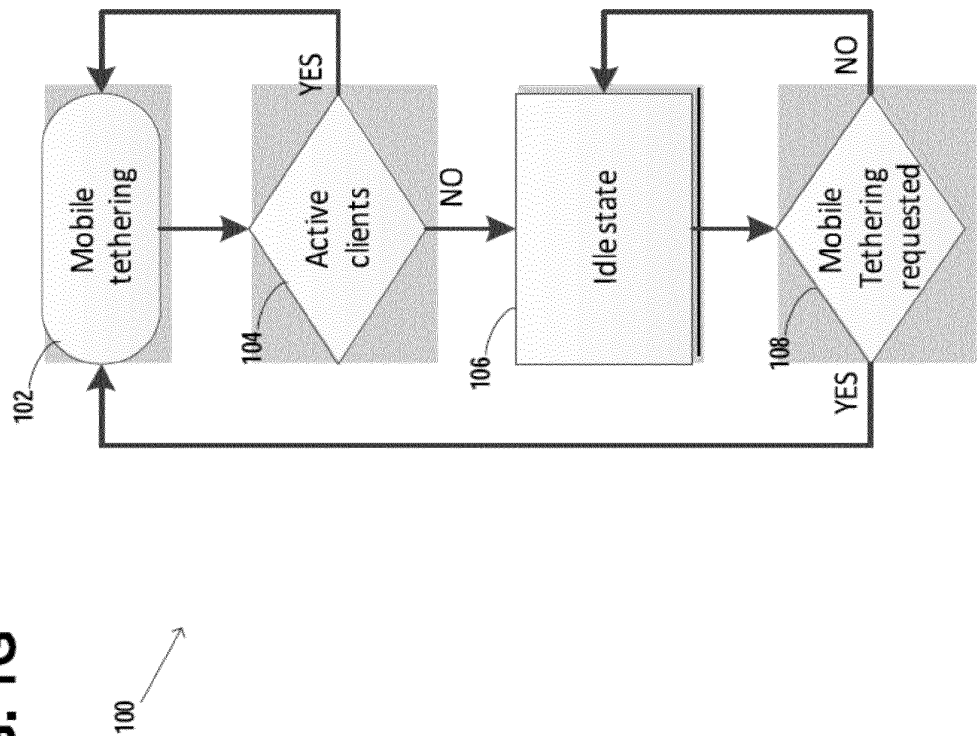


FIG. 2A

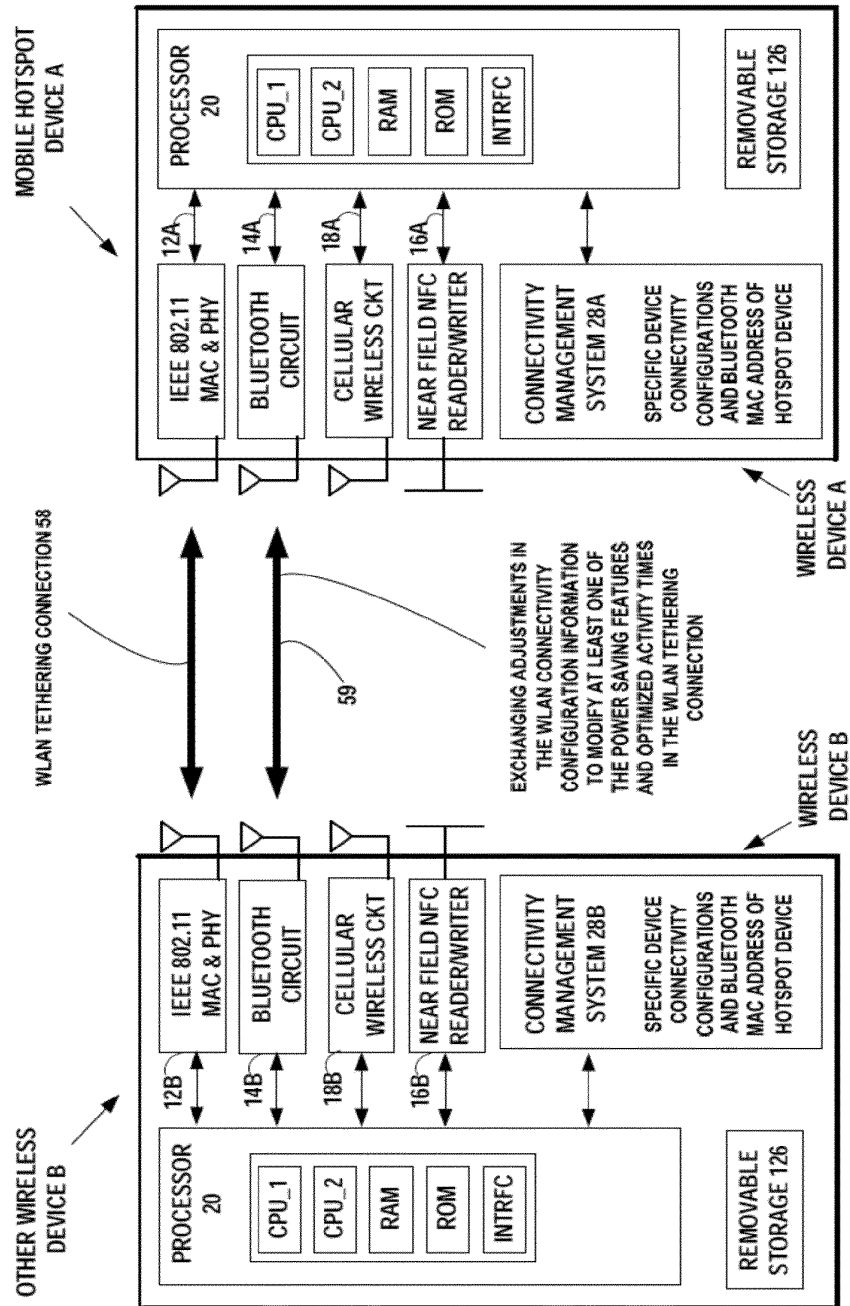


FIG. 2B

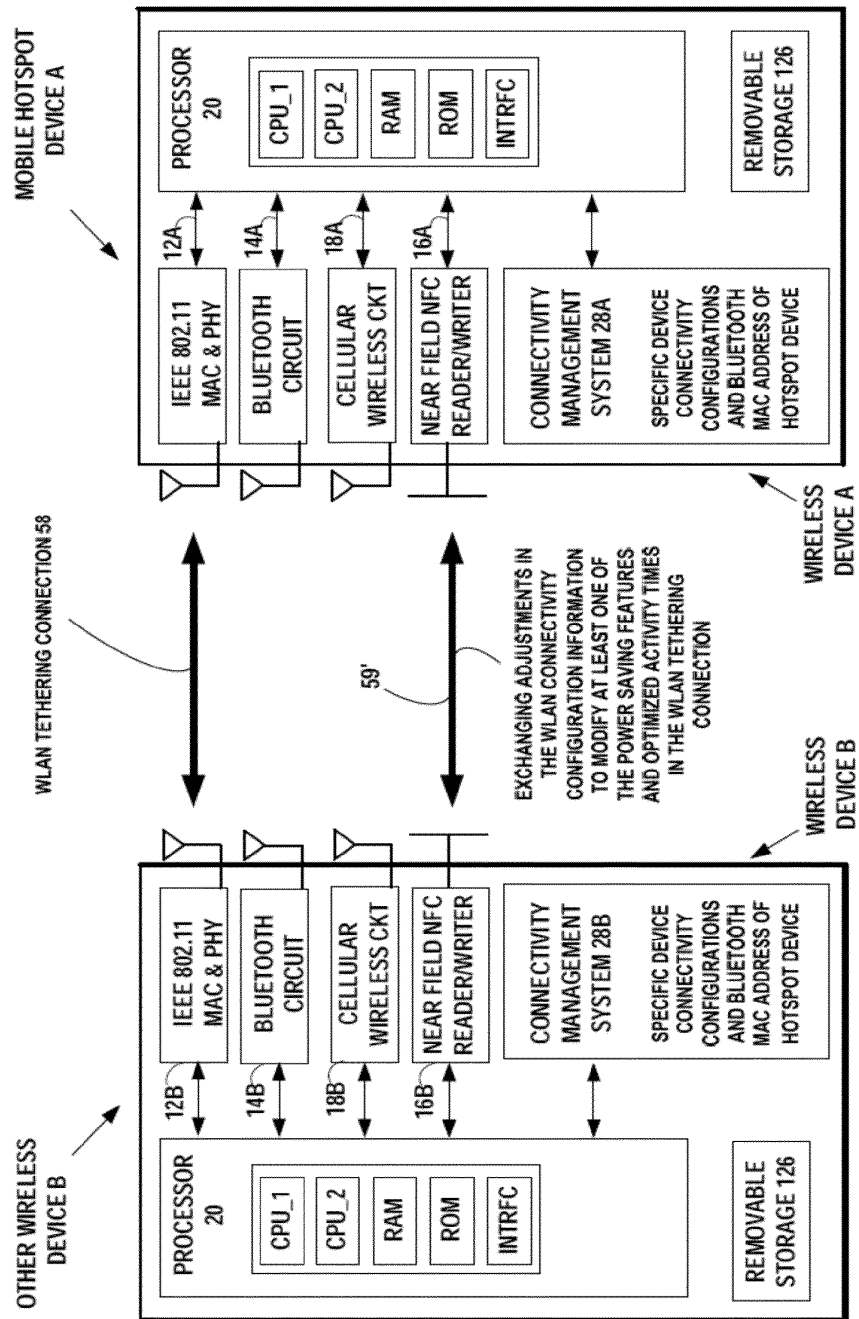


FIG. 3A

300

STEP 302: ESTABLISHING, BY A MOBILE HOTSPOT DEVICE, A CONTROL CHANNEL WITH A WIRELESS DEVICE, USING AN OUT-OF-BAND COMMUNICATIONS CONNECTION IN AN OUT-OF-BAND COMMUNICATIONS MEDIUM; AND

STEP 304: EXCHANGING, BY THE MOBILE HOTSPOT DEVICE OVER THE CONTROL CHANNEL, WITH THE WIRELESS DEVICE, BY AT LEAST ONE OF TRANSMITTING OR RECEIVING IN-BAND COMMUNICATIONS CONNECTIVITY CONFIGURATION INFORMATION TO ENABLE POWER SAVING FEATURES AND OPTIMIZE ACTIVITY TIMES IN AN IN-BAND COMMUNICATIONS TETHERING CONNECTION WITH THE WIRELESS DEVICE IN AN IN-BAND COMMUNICATIONS MEDIUM, FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND ONE OR MORE ENTITIES IN AT LEAST ONE OF A WIDE AREA COMMUNICATIONS NETWORK AND A WIRELESS LOCAL AREA NETWORK PROVIDED BY THE MOBILE HOTSPOT DEVICE.

FIG. 3B

350

STEP 352: ESTABLISHING, BY A WIRELESS DEVICE, A CONTROL CHANNEL WITH A MOBILE HOTSPOT DEVICE, USING AN OUT-OF-BAND COMMUNICATIONS CONNECTION IN AN OUT-OF-BAND COMMUNICATIONS MEDIUM; AND

STEP 354: EXCHANGING, BY THE WIRELESS DEVICE OVER THE CONTROL CHANNEL, WITH THE MOBILE HOTSPOT DEVICE, BY AT LEAST ONE OF TRANSMITTING OR RECEIVING IN-BAND COMMUNICATIONS CONNECTIVITY CONFIGURATION INFORMATION TO ENABLE POWER SAVING FEATURES AND OPTIMIZE ACTIVITY TIMES IN AN IN-BAND COMMUNICATIONS TETHERING CONNECTION WITH THE MOBILE HOTSPOT DEVICE IN AN IN-BAND COMMUNICATIONS MEDIUM, FOR RELAYING BY THE MOBILE HOTSPOT DEVICE, COMMUNICATIONS BETWEEN THE WIRELESS DEVICE AND ONE OR MORE ENTITIES IN AT LEAST ONE OF A WIDE AREA COMMUNICATIONS NETWORK AND A WIRELESS LOCAL AREA NETWORK PROVIDED BY THE MOBILE HOTSPOT DEVICE.

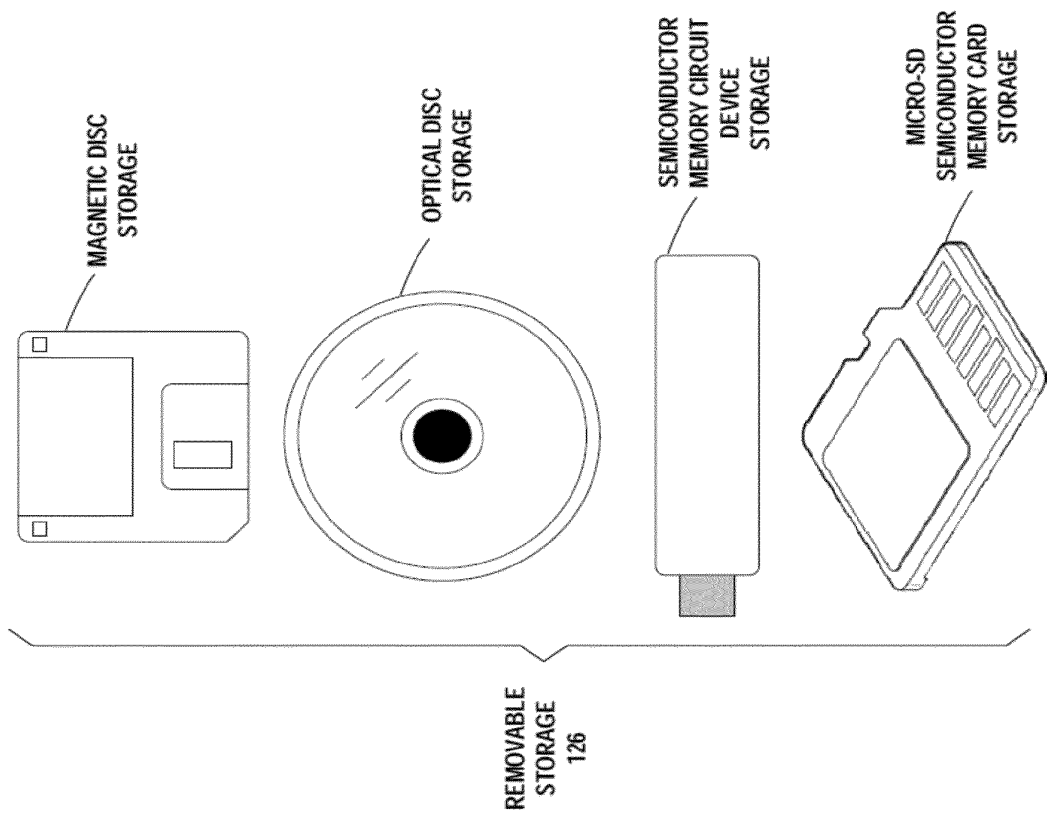


FIG. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2012115471 A [0006]

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				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				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
Sheet	1	of	3	Attorney Docket Number	020505-000006

U.S. PATENT DOCUMENTS					
Examiner Initial *	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code ² (if known)			
	1	US-20020152305 A1	10-17-2002	Jackson et al.	
	2	US-20040053602 A1	03-18-2004	Wurzberg	
	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	GHAJ 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		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Country ³ Code	Number ⁴ Kind Code (if known) ⁵			
	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	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.

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 <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				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
Sheet	2	of	3		

[illegible][illegible]

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

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

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

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

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

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 <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				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
Sheet	3	of	3	Attorney Docket Number	020505-000006

[illegible]

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

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

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

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the 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 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	09/18/2023	EXAMINER	
WOODARD, EMHARDT, HENRY, REEVES & WAGNER, LLP 111 MONUMENT CIRCLE, SUITE 3700 INDIANAPOLIS, IN 46204-5137			CENTRAL, DOCKET	
			ART UNIT	PAPER NUMBER
			OPAP	
			NOTIFICATION DATE	DELIVERY MODE
			09/18/2023	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

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 18/448,281	Applicant(s) Manapragada, Sai C.	
	Examiner CHERYL P GIBSON BAYLOR	Art Unit OPET	AIA (FITF) Status Yes
1. THE REQUEST FILED <u>11 August 2023</u> IS GRANTED . The above-identified application has met the requirements for prioritized examination A. ☒ for an original nonprovisional application (Track I). B. ☐ for an application undergoing continued examination (RCE). 2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs: A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply; B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim; C. filing a <u>request for continued examination</u> ; D. filing a notice of appeal; E. filing a request for suspension of action; F. mailing of a notice of allowance; G. mailing of a final Office action; H. completion of examination as defined in 37 CFR 41.102; or I. abandonment of the application. Telephone inquiries with regard to this decision should be directed to CHERYL GIBSON BAYLOR at (571)272-3213. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.			
/CHERYL GIBSON BAYLOR/ Paralegal Specialist, OPET			



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
18/448,281	08/11/2023		1064	020505-000006	30	1

CONFIRMATION NO. 1540

30565

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

FILING RECEIPT



0000000061249640

Date Mailed: 08/31/2023

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

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

Inventor(s)

Sai C. Manapragada, Cypress, TX;

Applicant(s)

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

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

Domestic Priority data as claimed by applicant

This application is a CON of 17/468,509 09/07/2021
which is a CON of 16/039,660 07/19/2018 PAT 11,115,834
which is a CON of 14/526,799 10/29/2014 PAT 10,034,179
which claims benefit of 61/897,219 10/30/2013
and claims benefit of 61/897,216 10/30/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

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

If Required, Foreign Filing License Granted: 08/29/2023

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/448,281**

Projected Publication Date: 12/07/2023

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

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

Preliminary Class

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 18/448,281			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	64		N/A			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	280		N/A			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	320		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	*	x 40 =	400	OR				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x =	0					
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0					
			TOTAL	1064		TOTAL			
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	* Minus **	=	x =		OR	x =		
	Independent (37 CFR 1.16(h))	* Minus ***	=	x =		OR	x =		
	Application Size Fee (37 CFR 1.16(s))					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR			
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	* Minus **	=	x =		OR	x =		
	Independent (37 CFR 1.16(h))	* Minus ***	=	x =		OR	x =		
	Application Size Fee (37 CFR 1.16(s))					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR			
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									

TERMINAL DISCLAIMER TO OBTAIN A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) 020505-000006
In re Application of: Sai C. Manapragada Application No.: New Application Filed: August 11, 2023 For: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERS The applicant, <u>XiFi Networks R&D Inc.</u>, owner of <u>100</u> 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 <u>18/447,597</u>, filed, <u>September 7, 2021</u>, 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. <u>73453</u> _____ /Blake R. Hartz, Reg. No. 73453/ Signature _____ Blake R. Hartz, Reg. No. 73453 Typed or printed name _____ Attorney of Record Title _____ August 11, 2023 Date _____ 317-634-3456 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.



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
18/448,281

RECEIPT DATE / TIME
08/11/2023 11:49:56 AM ET

ATTORNEY DOCKET #
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 # 62601642

FILING DATE -

CUSTOMER # 30565

FIRST NAMED INVENTOR Sai C. Manapragada

CORRESPONDENCE ADDRESS -

AUTHORIZED BY Blake Hartz

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Terminal Disclaimer.pdf	1	Terminal Disclaimer Filed	288 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Terminal Disclaimer.pdf	E9E741EC268BCB45BDDCC9FE0DE67847C3A3D5AB828C4A D0A564CB13FA28FFFCDC337EF9CF78AE8C5D2B1BEBED755 F04353E1AFFC1A89A69541B5DEDC502BF0

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 #
18/448,281

RECEIPT DATE / TIME
08/11/2023 11:49:56 AM ET

ATTORNEY DOCKET #
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 # 62601642

AUTHORIZED BY Blake Hartz

CUSTOMER # 30565

FILING DATE -

CORRESPONDENCE
ADDRESS -

FIRST NAMED
INVENTOR Sai C. Manapragada

Payment Information

PAYMENT METHOD
CARD / 1649

PAYMENT TRANSACTION ID
E20238AB51075503

PAYMENT AUTHORIZED BY
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.

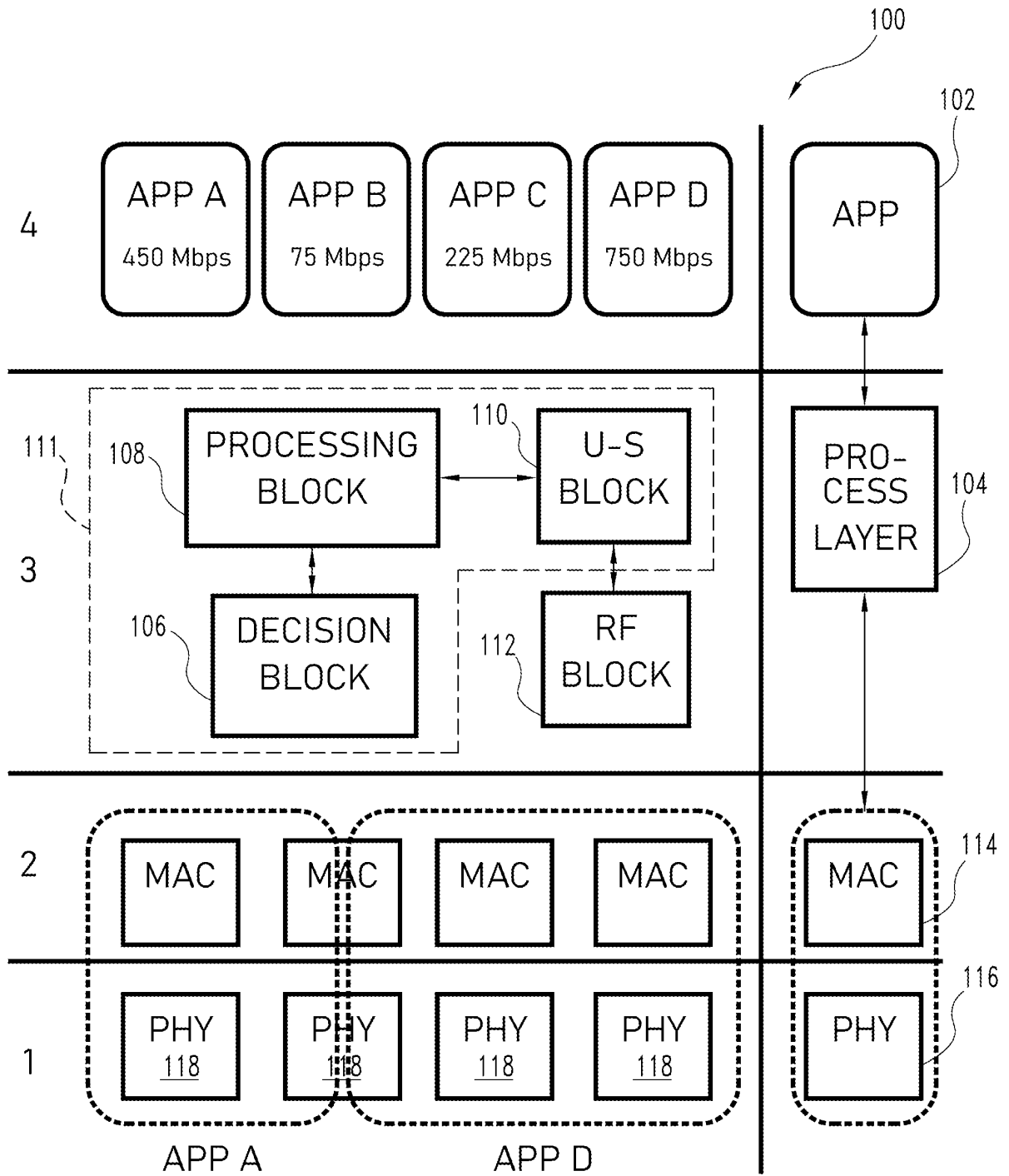


Fig. 1

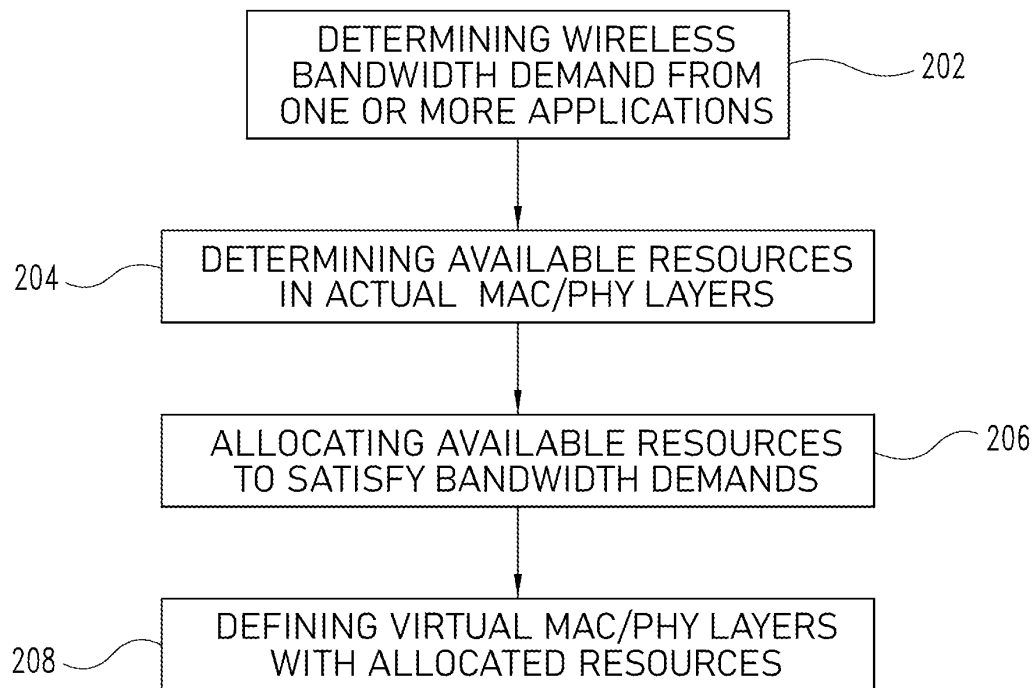
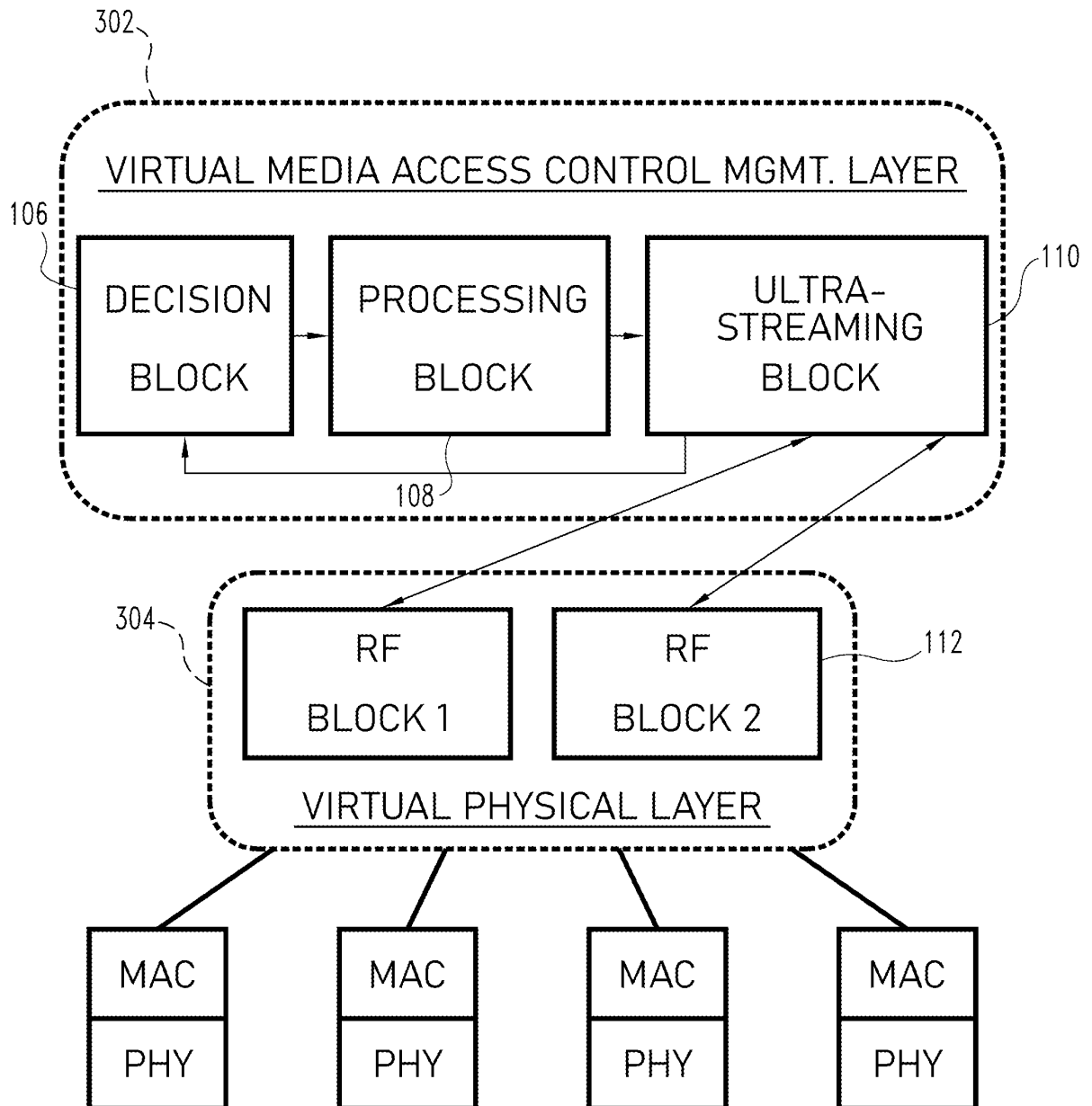


Fig. 2

*Fig. 3*

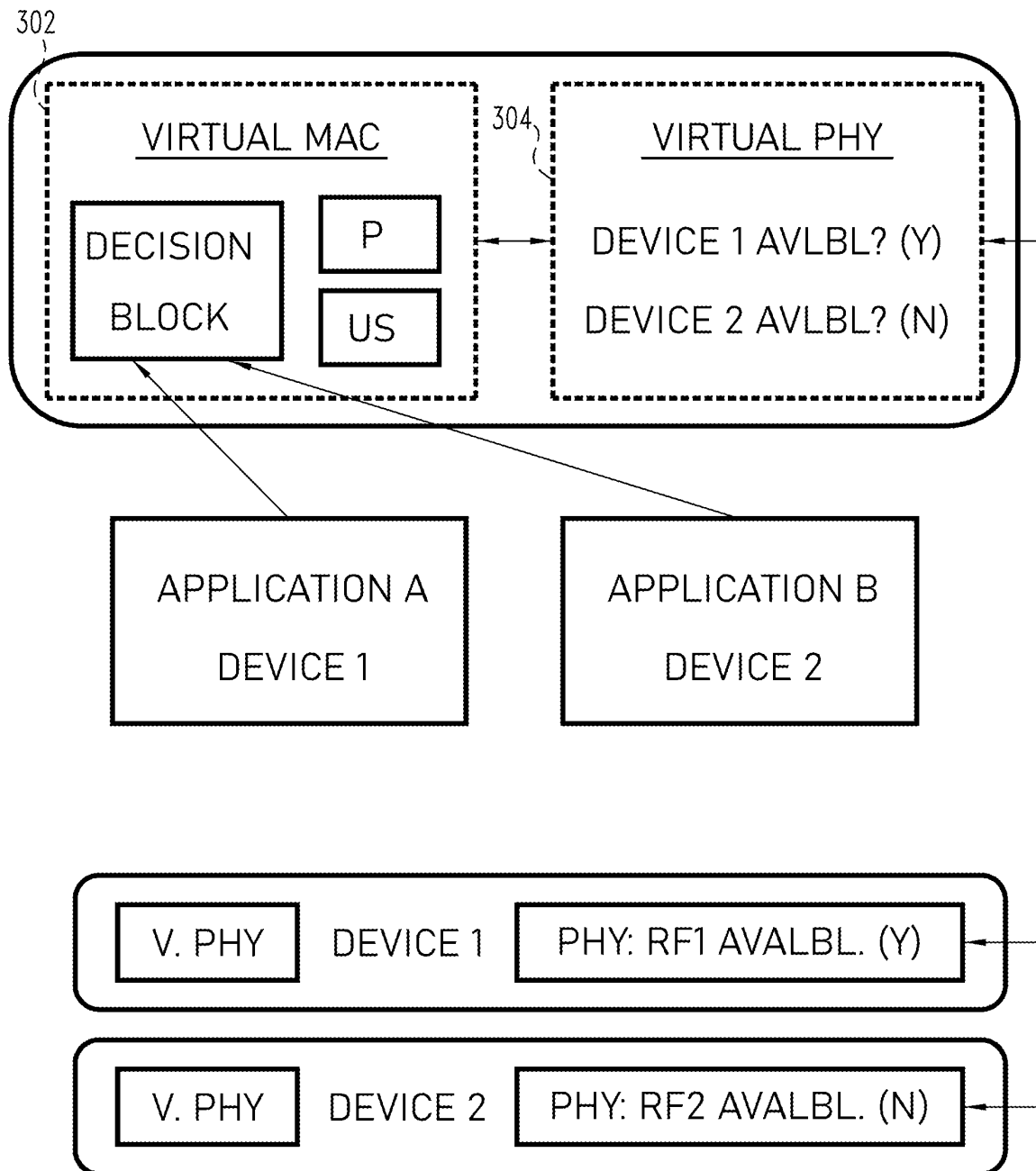
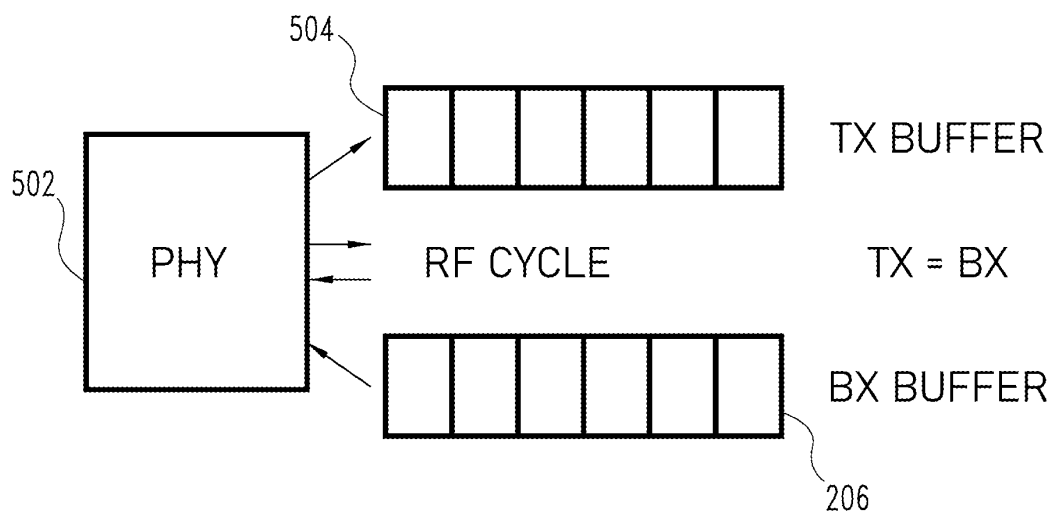
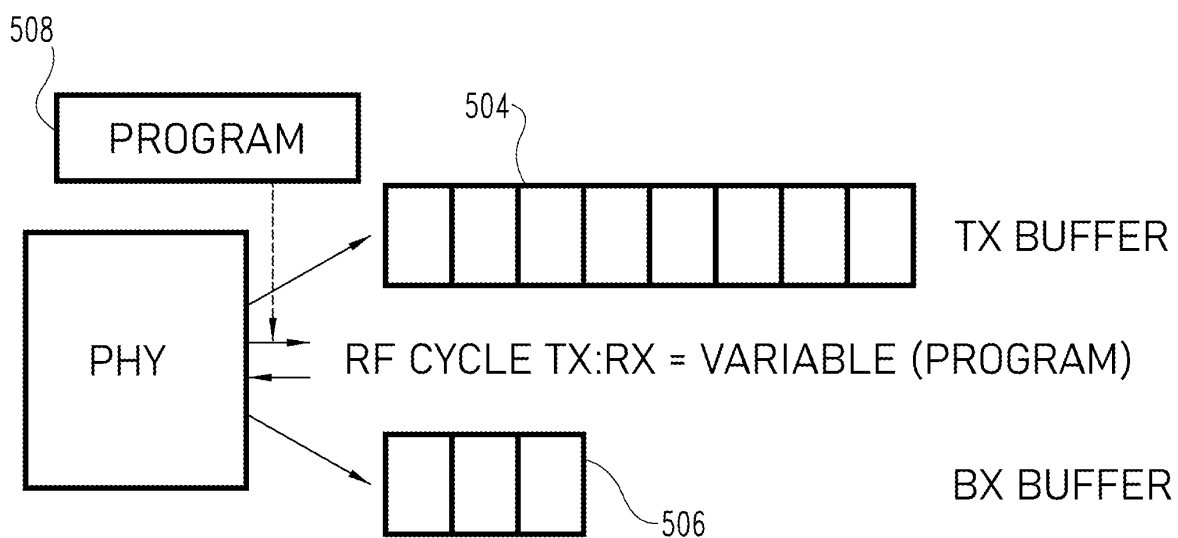


Fig. 4

*Fig. 5A**Fig. 5B*

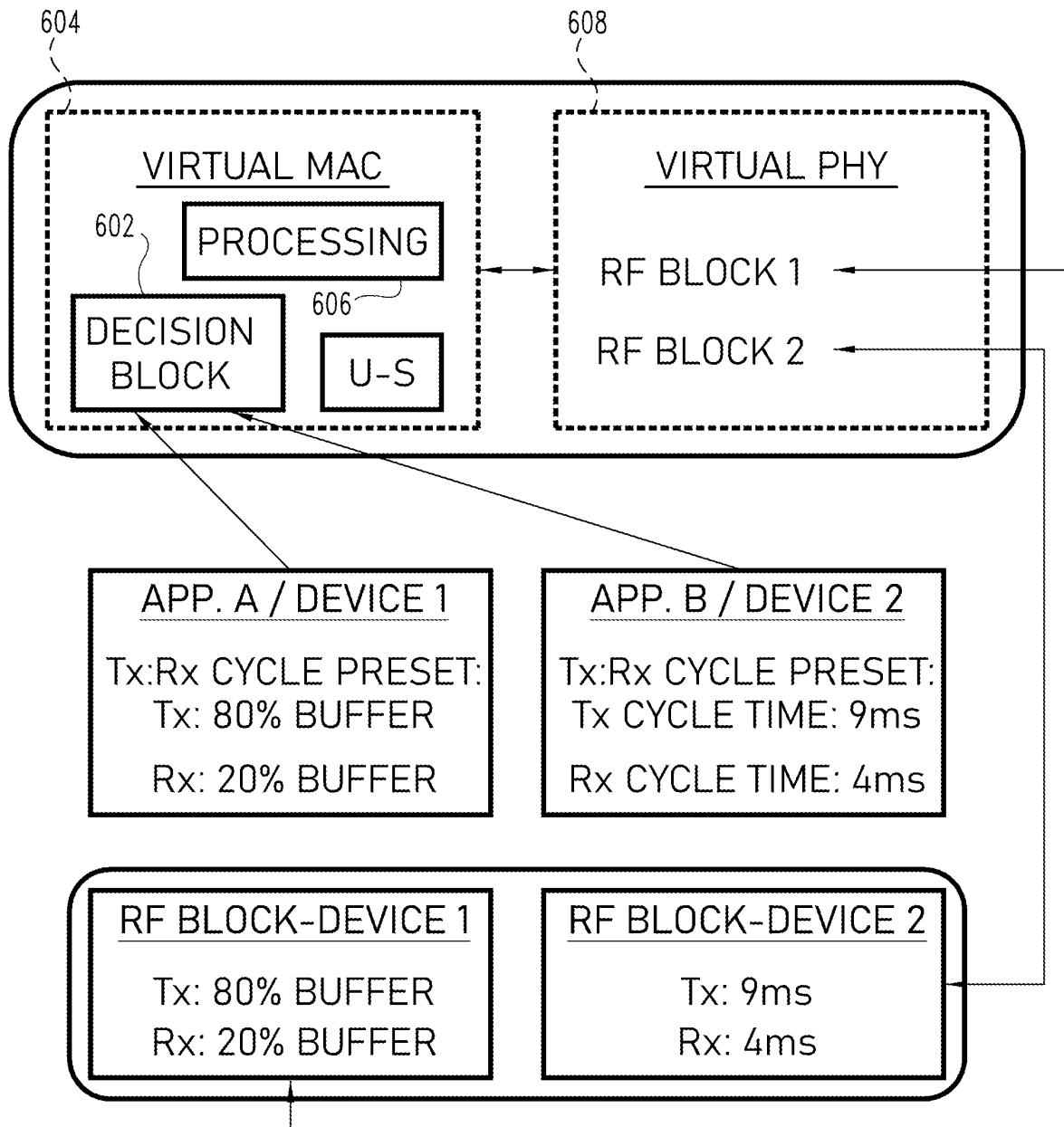


Fig. 6

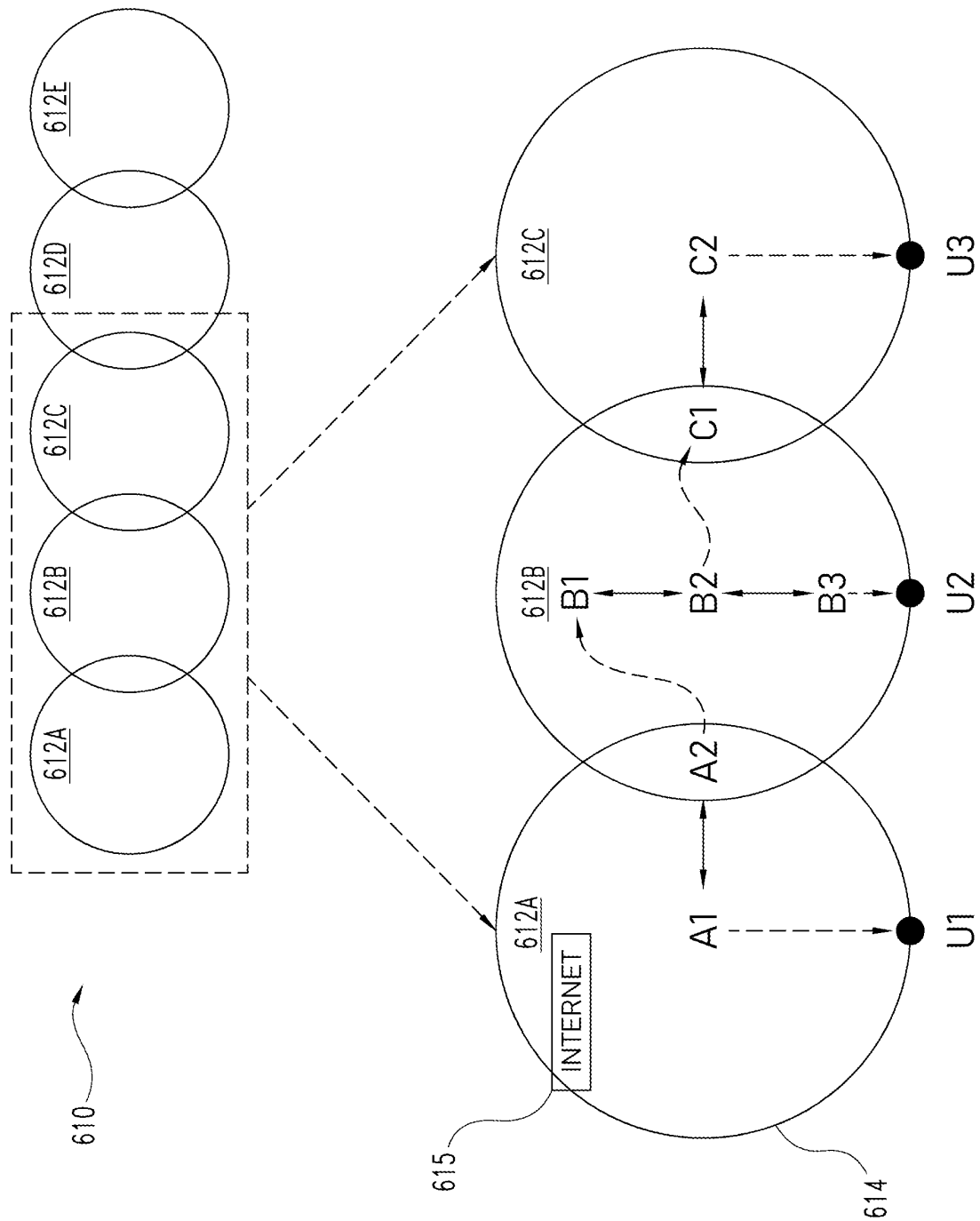


Fig. 7

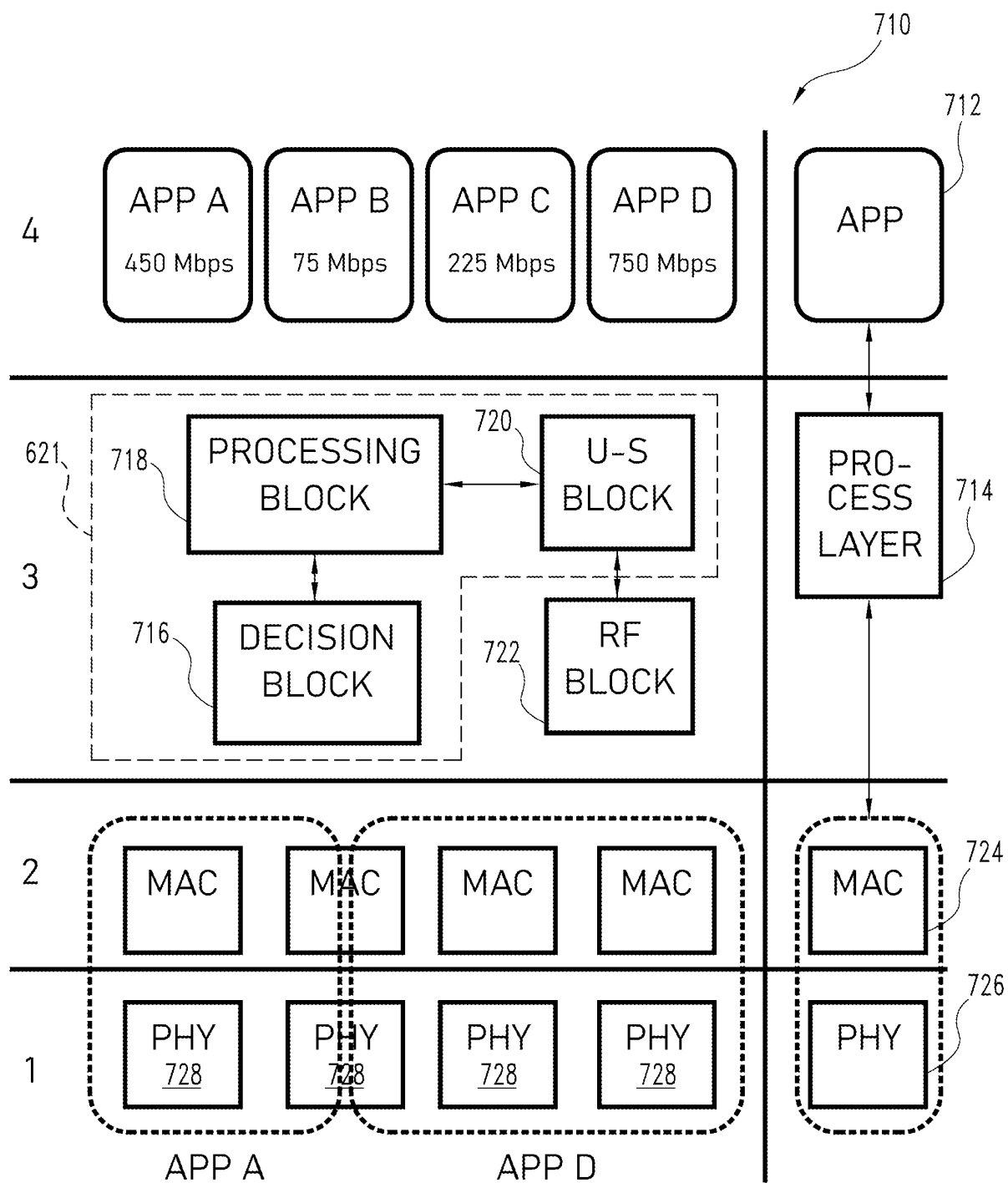


Fig. 8

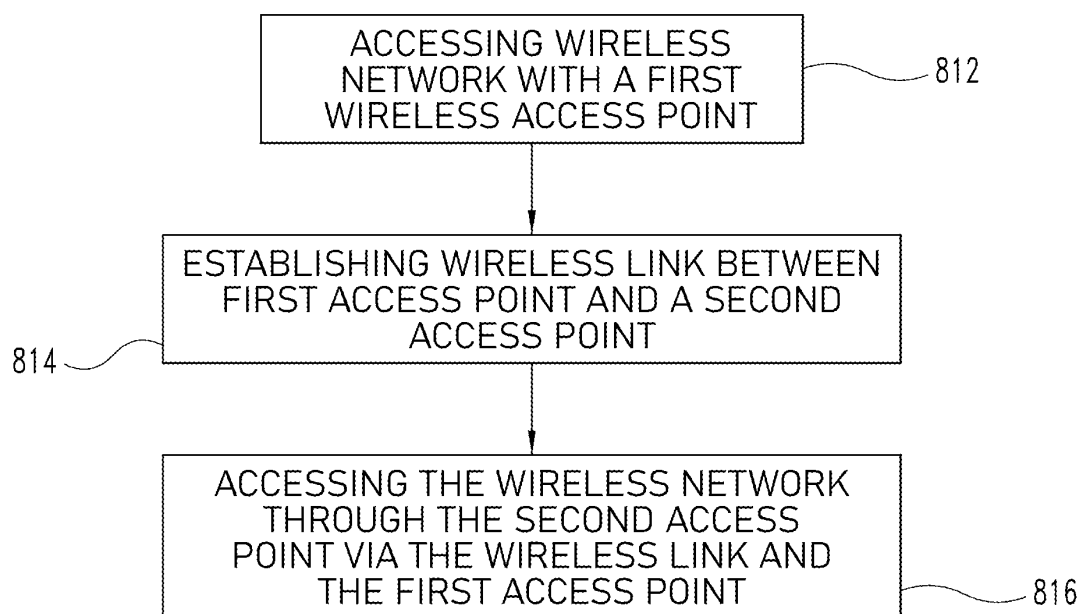


Fig. 9

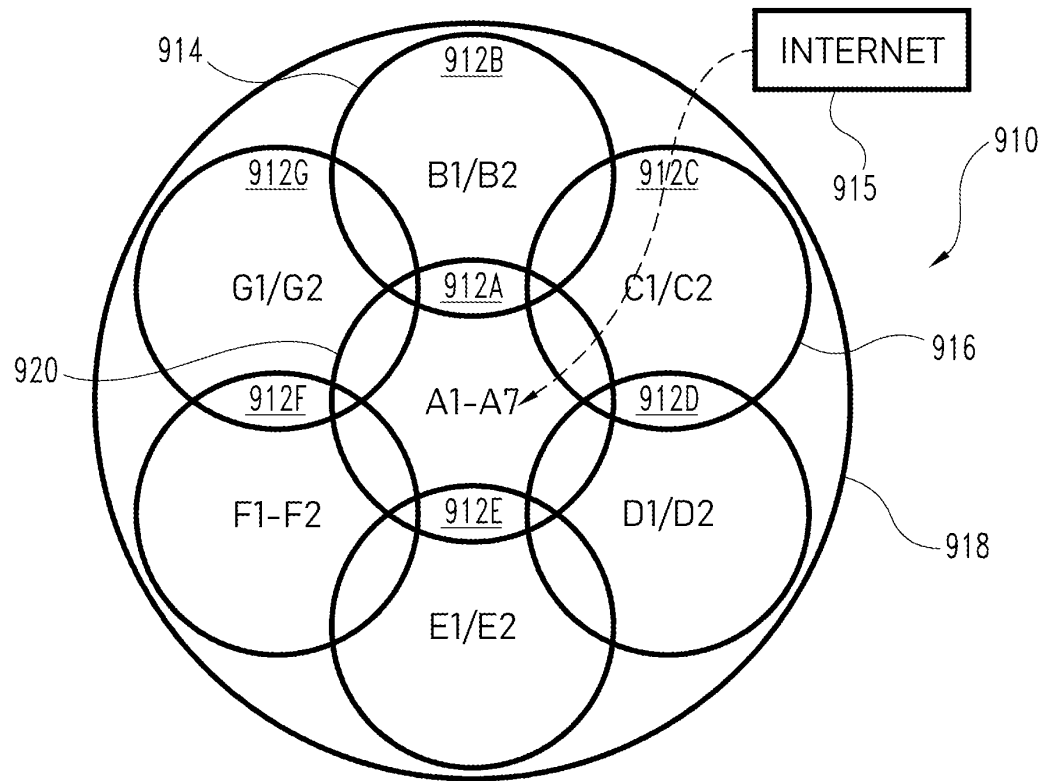


Fig. 10A

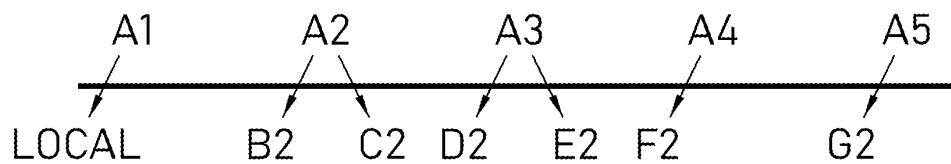


Fig. 10B

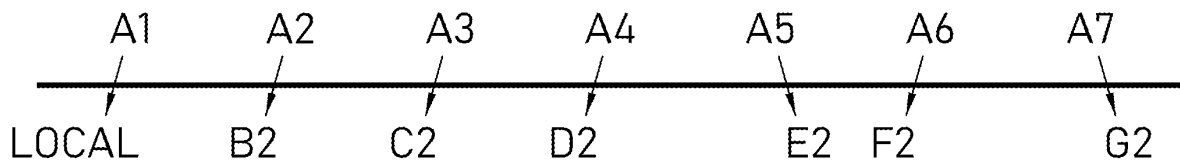


Fig. 10C

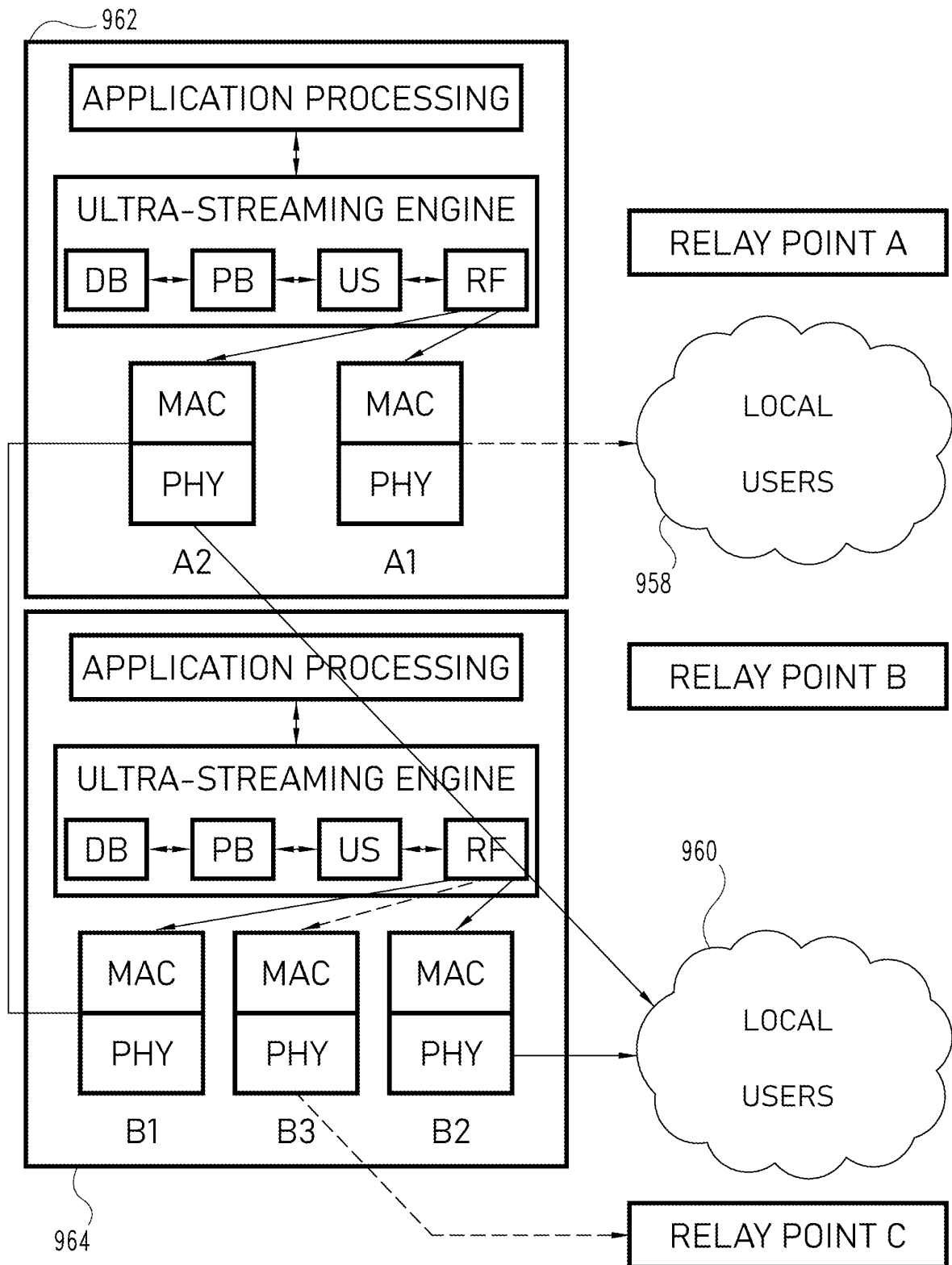


Fig. 11

Attorney Docket No.: <PSYC.P101>

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

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

As a below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

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

_____ United States Application Number _____, filed on _____.

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

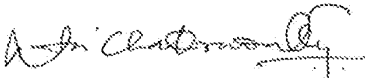
I have authorized and/or hereby do authorize my assignee to file patent applications claiming priority from the application referenced above, including provisional, non-provisional, design, divisional, continuation, continued prosecution, continuation-in-part, substitute, supplemental examination application,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

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

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

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

Legal Name of Inventor:

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

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

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., ‘< signal name >’) is also used to indicate an active low signal. The term “coupled” is used herein to express a direct connection as well as a connection through one or more intervening circuits or structures. Integrated circuit device “programming” may include, for example and without limitation, loading a control value into a register or other storage circuit within the device in response to a host instruction and thus controlling an operational aspect of the device,

establishing a device configuration or controlling an operational aspect of the device through a one-time programming operation (e.g., blowing fuses within a configuration circuit during device production), and/or connecting one or more selected pins or other contact structures of the device to reference voltage lines (also referred to as strapping) to establish a particular device configuration or operation aspect of the device. The term “exemplary” is used to express an example, not a preference or requirement.

[0059] While the invention has been described with reference to specific embodiments thereof, it will be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. For example, features or aspects of any of the embodiments may be applied, at least where practicable, in combination with any other of the embodiments or in place of counterpart features or aspects thereof. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method of improving the performance of 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 that, when the wireless networking device is being used, provides a first data stream and 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 to the first and second actual MAC interfaces;
 - associating first and second wireless transceivers with the first and second actual PHY interfaces, wherein the first and second wireless transceivers (i) are suitable for use in a wireless local area network, (ii) have a first and second bandwidth availability up to first and second actual bandwidths, and (iii) 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, 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. The method of claim 1,

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

wherein the processing interface is configured, 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 first and second wireless transceivers using a

specific subset of frequencies corresponding to the identified at least one portion of their available bandwidth, and (ii) cause the prepared first and second data streams to be simultaneously 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.

3. 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 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 unidentified 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. 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 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 unidentified 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. The method of claim 4,

wherein the processing interface is configured, 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, compare the magnitude of the first bandwidth requirement of the first application to the identified bandwidth availabilities of the first and second wireless transceivers; and

wherein, if, during operation of the wireless networking device, the first bandwidth requirement of the first application is not at least partially satisfied by the bandwidth availability of the selected transceiver, then 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 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 wireless bandwidth requirement of the first application.

6. The method of claim 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, during operation of the wireless networking device, feeds 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, 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 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 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 data stream 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 device 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 first, second and third wireless transceivers.

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

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

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

10. The method of claim 6, wherein at least one of the first, second and third wireless transceivers are adapted to communicate with a recipient via a variable and programmable duplex link.

11. The method of claim 10, wherein the variable duplex link exhibits an asymmetric transmit and receive profile.

12. The method of claim 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, during their operation, to communicate with each other regarding at least one aspect of operation of the first wireless access point.

13. 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. 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. The method of claim 1, wherein the wireless networking device comprises a wireless access point.
16. The method of claim 1, wherein the wireless networking device comprises a handheld computing device.
17. The method of claim 16, wherein the handheld computing device comprises a tablet.
18. 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. 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. The method of claim 1, wherein the virtual MAC interface includes a decision block.
21. The method of claim 1, wherein the virtual MAC interface includes a processing block.
22. The method of claim 1, wherein the virtual MAC interface includes an ultra-streaming block.
23. The method of claim 1, wherein each one of the virtual PHY interface includes an RF block.
24. The method of claim 1, wherein the wireless networking device comprises a telephone.
25. The method of claim 1, wherein the at least one portion the first bandwidth of the first transceiver comprises a single portion.
26. The method of claim 1, wherein the at least one portion the first bandwidth of the first transceiver is contiguous.
27. The method of claim 1, wherein the at least one portion the second bandwidth of the second transceiver comprises a single portion.
28. The method of claim 1, wherein the at least one portion the second bandwidth of the second transceiver is contiguous.
29. The method of claim 1, wherein the first virtual PHY layer is not contiguous with the virtual MAC interface.

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

ABSTRACT OF THE DISCLOSURE

A wireless networking system is disclosed. The wireless networking system includes an application layer associated with one or more applications having a wireless bandwidth requirement. A first wireless transceiver resource associated with an actual MAC layer and PHY layer is employed. The first wireless transceiver resource has a first bandwidth availability up to a first actual bandwidth. A second wireless transceiver resource associated with the actual MAC layer and the PHY layer is employed. The second wireless transceiver resource has a second bandwidth availability up to a second actual bandwidth. A processing layer evaluates the wireless bandwidth requirement and the first and second bandwidth availabilities of the wireless transceiver resources. The processing layer includes a bandwidth allocator to allocate at least a portion of each of the first and second actual bandwidths to virtual MAC and virtual PHY layers, and to satisfy the application layer wireless bandwidth requirement.

#2120235

APPLICATION DATA SHEET

APPLICATION INFORMATION

Application number::

Filing Date::

Application Type:: Non-Provisional

Subject Matter:: Utility

Suggested classification::

Suggested Group Art Unit::

CD-ROM or CD-R?::

Number of CD disks::

Number of copies of CDs::

Sequence submission?::

Computer Readable Form (CRF)?::

Number of copies of CRF::

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

Attorney Docket Number:: 020505-000006

Request For Early Publication?::

Request for Non-Publication?::

Suggested Drawing Figure:: 1

Total Drawing Sheets:: 11

Small Entity?:: Yes

Licensed US Govt. Agency:: No

Contract or Grant Numbers::

Secrecy Order in Parent Appl.?::

INVENTOR INFORMATION

Given Name:: Sai

Middle Name:: C.

Family Name:: Manapragada

APPLICATION DATA SHEET

Name Suffix::
City of Residence:: Cypress
State or Province of Residence:: TX
Country of Residence:: United States
Street of mailing address:: 21214 Chelton Beach Drive

City of mailing address:: Cypress
State or Province of mailing address:: TX
Country of mailing address:: United States
Postal or Zip Code of mailing address:: 77433

CORRESPONDENCE INFORMATION

Correspondence Customer Number:: 30565
Phone number:: 317-634-3456
Fax Number:: 317-637-7561

REPRESENTATIVE INFORMATION

Representative Customer Number:: 30565

DOMESTIC PRIORITY INFORMATION

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	17/468,509	2021-09-07
17/468,509	Continuation of	16/039,660	2018-07-19
16/039,660	Continuation of	14/526,799	2014-10-29
14/526,799	Claims the benefit of	61/897,219	2013-10-30
14/526,799	Claims the benefit of	61/897,216	2013-10-30

FOREIGN PRIORITY INFORMATION

Country::	Application Number::	Filing Date::	Priority	Access Code::
			Claimed::	

APPLICATION DATA SHEET

STATEMENT UNDER 37 CFR 1.55 OR 1.78 FOR AIA (FIRST INVENTOR TO FILE) TRANSITION APPLICATIONS

- ☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

AUTHORIZATION OR OPT-OUT OF AUTHORIZATION TO PERMIT ACCESS

When this Application Data Sheet is properly signed and filed with the application, Applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, application **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) – Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO – Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of the search results from the instant application without delay in a European patent application that claims priority to the instant application.

APPLICATION DATA SHEET

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

- ☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information and identified in subsection 1A above.
- ☐ B. Applicant **does not** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

APPLICANT INFORMATION

Applicant name:: XiFi Networks R&D Inc.
Street of mailing address:: 21214 Chelton Beach Drive

City of mailing address:: Cypress
State or Province of mailing address:: TX
Country of mailing address:: United States
Postal or Zip Code of mailing address:: 77433

SIGNATURE

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Respectfully submitted,

By /Blake R. Hartz, Reg. No. 73453/
Blake R. Hartz, Reg. No. 73453
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700, Indianapolis, Indiana 46204-5137
Telephone (317) 634-3456 Fax (317) 637-7561 Email: bhartz@uspatent.com



(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I500350 B

(45)公告日：中華民國 104 (2015) 年 09 月 11 日

(21)申請案號：102135927

(22)申請日：中華民國 102 (2013) 年 10 月 04 日

(51)Int. Cl. : H04W76/04 (2009.01) H04L29/06 (2006.01)

(71)申請人：瑞昱半導體股份有限公司 (中華民國) REALTEK SEMICONDUCTOR CORPORATION (TW)

新竹市新竹科學園區創新二路 2 號

(72)發明人：顏光裕 YEN, KUANG YU (TW) ; 劉又誠 LIU, YU CHEN (TW) ; 程崇嘉 CHEN, CHUNG CHIA (TW)

(74)代理人：林昱初；鄭慶鴻

(56)參考文獻：

US 2013/0016708A1

WO 03/028313A2

審查人員：陳奕昌

申請專利範圍項數：15 項 圖式數：3 共 22 頁

(54)名稱

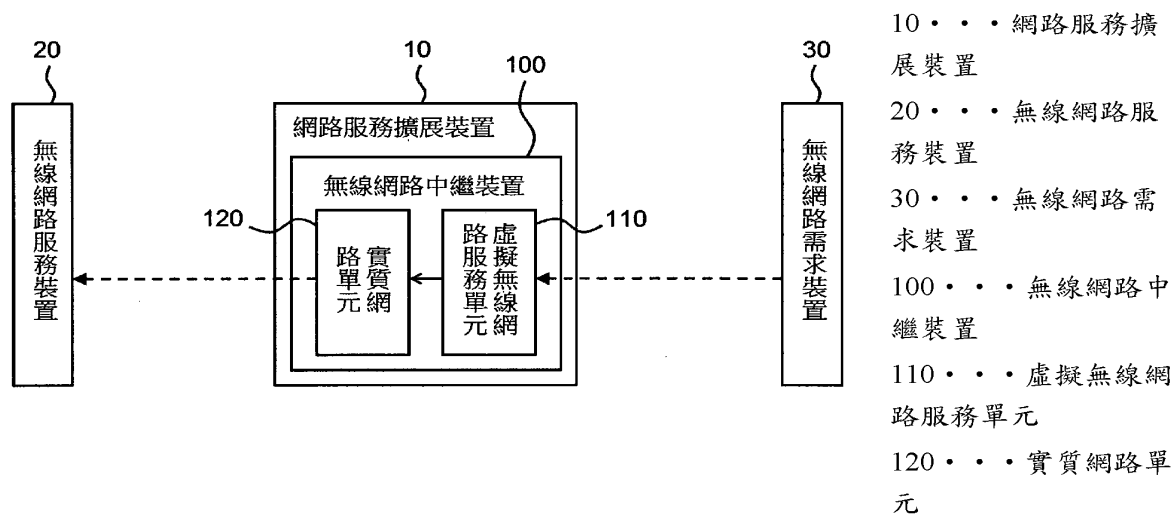
網路服務擴展方法與裝置

NETWORK SERVICE EXTENSION METHOD AND DEVICE

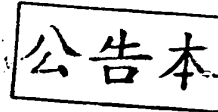
(57)摘要

本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

The present invention discloses a network service extension method which is capable of increasing the range of a network service and carried out by a network service extension device. The method comprises: establishing the link between a real network unit of a wireless network relay device and a wireless network serving device; configuring a virtual wireless network serving unit according to the link setting of the wireless network serving device in which the link settings of the serving device and the serving unit are the same; establishing the link between the virtual wireless network serving unit and a wireless network demand device; and establishing the connection between the wireless network serving device and the wireless network demand device via the virtual wireless network serving unit and the real network unit.



【圖1】

**【發明摘要】****【中文發明名稱】** 網路服務擴展方法與裝置**【英文發明名稱】** Network service extension method and device**【中文】**

本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【英文】

The present invention discloses a network service extension method which is capable of increasing the range of a network service and carried out by a network service extension device. The method comprises: establishing the link between a real network unit of a wireless network relay device and a wireless network serving device; configuring a virtual wireless network serving unit according to the link setting of the wireless network serving device in which the link settings of the serving device and the serving unit are the same; establishing the link between the virtual wireless network serving unit and a wireless network demand device; and establishing the connection between the wireless network

serving device and the wireless network demand device via the virtual wireless network serving unit and the real network unit.

【指定代表圖】 圖1

【代表圖之符號簡單說明】

- 10 網路服務擴展裝置
- 20 無線網路服務裝置
- 30 無線網路需求裝置
- 100 無線網路中繼裝置
- 110 虛擬無線網路服務單元
- 120 實質網路單元

【發明說明書】

【中文發明名稱】 網路服務擴展方法與裝置

【英文發明名稱】 Network service extension method and device

【技術領域】

【0001】 本發明是關於網路方法與裝置，尤其是關於網路服務擴展方法與裝置。

【先前技術】

【0002】 無線網路基於其便利性已廣泛地應用於日常生活中。一般無線網路之架構包含一基礎服務裝置（Basic Service Set, BSS。例如一無線網路接取點（Access Point, AP）），該基礎服務裝置連線至一可靠網路（例如一有線網路），於一服務範圍內提供一基礎無線網路服務，並允許該服務範圍內的其它無線網路裝置經由它連線至該可靠網路。然而根據目前技術，若一第一無線網路裝置擁有該基礎無線網路服務之連線設定且位於前述服務範圍內，而一第二無線網路裝置擁有該基礎無線網路服務之連線設定但位於該服務範圍外或無法穩定地連線至該基礎服務裝置，此第二無線網路需透過該第一無線網路裝置所提供之一有別於前述基礎無線網路服務之連線服務方能穩定地連線至該基礎服務裝置，舉例來說，該基礎無線網路服務係一第一無線區域網路（Wireless Local Area Network, WLAN）服務，該連線服務係一第二無線區域網路服務，該第一與第二無線區域網路服務之連線設定（例如一服務設定識別碼（Service Set Identifier, SSID）、一保密類型（Security Type）、一金鑰）不同，因此該第二無

線網路裝置需同時具備該第一與第二無線區域網路服務之連線設定才能借道該第一無線網路裝置連線至該基礎服務裝置，換言之，倘若該第二無線網路裝置不具有該第一無線網路裝置之連線設定，即無法經由該第一無線網路裝置連線至該基礎服務裝置，此一限制減少了該第二無線網路裝置之連線機會。

【發明內容】

【0003】鑑於先前技術之不足，本發明之一目的在於提供一種網路服務擴展方法與一種網路服務擴展裝置，以擴展一網路服務之範圍。

【0004】本發明揭露了一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由本發明之網路服務擴展裝置或其等效裝置來執行。依據本發明之一實施例，該方法包含下列步驟：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線；以及經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【0005】本發明另揭露了一種網路服務擴展裝置，能夠擴展一無線網路服務裝置之網路服務之範圍。依據本發明之一實施例，該裝置包含：一無線網路中繼裝置，用來與該無線網路服務裝置建立連線，包含：一虛擬無線網路服務單元，係依據該無線網路服務裝置之連線設定而形成，用來與一無線網路需求裝置建立連線，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；以及一實質網路單元，用來與該虛擬無線網路服務單元以及該無線網路服務裝置建立連線，因此該無線網路中繼裝置藉由該虛擬無線網

路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【0006】有關本發明的特徵、實作與功效，茲配合圖式作較佳實施例詳細說明如下。

【圖式簡單說明】

【0007】

〔圖1〕為本發明之網路服務擴展裝置之一實施例的示意圖；

〔圖2a〕為圖1之無線網路中繼裝置之運作的一實施例的示意圖；

〔圖2b〕為圖1之無線網路中繼裝置之運作的另一實施例的示意圖；以及

〔圖3〕為本發明之網路服務擴展方法之一實施例的流程圖。

【實施方式】

【0008】以下說明內容之技術用語係參照本技術領域之習慣用語，如本說明書對部分用語有加以說明或定義，該部分用語之解釋係以本說明書之說明或定義為準。

【0009】本發明之揭露內容包含網路服務擴展裝置與方法，能夠擴展一網路服務之範圍。該裝置與方法可應用於一積體電路或一系統裝置，在實施為可能的前提下，本技術領域具有通常知識者能夠依本說明書之揭露內容來選擇等效之元件或步驟來實現本發明，亦即本發明之實施並不限於後敘之實施例。由於本發明之網路服務擴展裝置所包含之部分元件單獨而言可能為已知元件，因此在不影響該裝置發明之充分揭露及可實施性的前提下，以下說明對於已知元

件的細節將予以節略。此外，本發明之網路服務擴展方法可藉由本發明之網路服務擴展裝置或其等效裝置來執行，在不影響該方法發明之充分揭露及可實施性的前提下，以下方法發明之說明將著重於步驟內容而非硬體。

【0010】請參閱圖1，其係本發明之網路服務擴展裝置之一實施例的示意圖，於本實施例中，該擴展裝置10係一無線區域網路（Wireless Local Area Network, WLAN）裝置，例如一筆記型電腦、一手機、一平板電腦、一網路卡或一網路晶片，能夠無線連線至一無線網路服務裝置20（例如一無線網路接取點（Access Point, AP））並擴展其網路服務的範圍。如圖1所示，該網路服務擴展裝置10包含：一無線網路中繼裝置100，用來與該無線網路服務裝置20建立連線，包含一虛擬無線網路服務單元110以及一實質網路單元120，該無線網路中繼裝置100可以是一無線網路卡、一無線網路晶片或其等效裝置。所述虛擬無線網路服務單元110係依據前述無線網路服務裝置20之連線設定而形成

（Configured），具有與該無線網路服務裝置20之連線設定相同之設定，用來與一無線網路需求裝置30（例如一筆記型電腦、一手機或一平板電腦）建立連線，換句話說，只要該無線網路需求裝置30擁有連線至該無線網路服務裝置20之設定，即可連線至該虛擬無線網路服務單元110，本實施例中，該虛擬無線網路服務單元110係藉由無線網路中繼裝置100模擬該無線網路服務裝置20所形成。另外，所述實質網路單元120用來與該虛擬無線網路服務單元110以及該無線網路服務裝置20建立連線，因此，該無線網路中繼裝置100可藉由該虛擬無線網路服務單元110以及該實質網路單元120建立起該無線網路服務裝置20與該無線網路需求裝置30間的連結，本實施例中，該實質網路單元120係該無線網路中繼裝置100之固有架構。

【0011】承上所述，本實施例係假設：該無線網路需求裝置30無法直接或

穩定地連線至該無線網路服務裝置20，因此需透過該網路服務擴展裝置10來連線至該無線網路服務裝置20。換句話說，該無線網路需求裝置30所接收之該無線網路服務裝置20之訊號強度/穩定度會小於該無線網路需求裝置30所接收之該虛擬無線網路服務單元110之訊號強度/穩定度。由於該虛擬無線網路服務單元110與該無線網路服務裝置20之連線設定相同，因此無線網路需求裝置30會將該虛擬無線網路服務單元110視為該無線網路服務裝置20，且該無線網路需求裝置30只要擁有該無線網路服務裝置20之連線設定（例如一服務設定識別碼（Service Set Identifier, SSID）；一保密類型（Security Type）；以及一金鑰），即能連線至該虛擬無線網路服務單元110，再經由它連接該無線網路服務裝置20。詳言之，本實施例中，該虛擬無線網路服務單元110會發出一信標（Beacon）以供該無線網路需求裝置30得知該虛擬無線網路服務單元110之存在，之後該無線網路需求裝置30會發出一探詢要求（Probe Request）訊號，而該虛擬無線網路服務單元110會再針對該探詢要求訊號回應一探詢回應（Probe Response）訊號，進而建立兩者間的連線。

【0012】請繼續參閱第1圖，於該無線網路需求裝置30與該虛擬無線網路服務單元110建立連線後，若該無線網路需求裝置欲經由該無線網路服務裝置20輸出資料，會發送一傳送封包至該虛擬無線網路服務單元110，接著該虛擬無線網路服務單元110再經由該實質網路單元120將該傳送封包傳輸至該無線網路服務裝置20；另一方面，若該無線網路服務裝置20欲發送一接收封包屬於該無線網路需求裝置30，會將該接收封包傳輸至該實質網路單元120，該實質網路單元120再經由該虛擬無線網路服務單元110將該接收封包傳輸至該無線網路需求裝置30。上述封包傳送可藉由多種方式來實現，舉例而言，請參閱圖2a，該虛

擬無線網路服務單元110包含一虛擬實體層（Physical Layer, PHY Layer）112、一虛擬媒體存取控制層（Media Access Control Layer, MAC Layer）114、一虛擬階層3協定層（Layer-3 Protocol Layer）116以及一虛擬應用層（Application Layer）118，該實質網路單元120則包含一實質應用層122、一實質階層3協定層124、一實質媒體存取控制層126以及一實質實體層128，該虛擬實體層112用來從該無線網路需求裝置30接收該傳送封包，並依序經由該虛擬媒體存取控制層114、該虛擬階層3協定層116、該實質階層3協定層124、該實質媒體存取控制層126以及該實質實體層128將該傳送封包傳輸至該無線網路服務裝置20，其中該虛擬階層3協定層116及/或該實質階層3協定層124會依據傳送封包之資訊（例如來源欄位、目的欄位或特定標籤）來判斷該傳送封包之接收者是否為該無線網路中繼裝置100，若否即將該傳送封包轉發至該無線網路服務裝置20；類似地，該實質實體層128用來從該無線網路服務裝置20接收該接收封包，並依序經由該實質媒體存取控制層126、該實質階層3協定層124、該虛擬階層3協定層116、該虛擬媒體存取控制層114以及該虛擬實體層112將該接收封包傳輸至該無線網路需求裝置30，其中該實質階層3協定層124及/或該虛擬階層3協定層116會依據接收封包之資訊（例如來源欄位、目的欄位或特定標籤）來判斷該接收封包之接收者是否為該無線網路中繼裝置100，若否即將該接收封包轉發至該無線網路需求裝置30。另舉例而言，請參閱圖2b，本發明亦可不透過階層3協定層而直接轉發該傳送封包或接收封包，更精確地說，該傳送封包會依序經由該虛擬實體層112、該虛擬媒體存取控制層114、該實質媒體存取控制層126以及該實質實體層128而傳送至該無線網路服務裝置20，而該接收封包會依序經由該實質實體層128、該實質媒體存取控制層126、該虛擬媒體存取控制層114以及該虛擬實體層112而傳送至該無線網路需求裝置30。

【0013】請注意，前述應用層118、122屬於網路分層之一環，並未用於圖2a與圖2b之實施例。另外，前述虛擬實體層112之運作原理與實質實體層128相同；虛擬媒體存取控制層114之運作原理與實質媒體存取控制層126相同；且虛擬階層3協定層116之運作原理與實質階層3協定層124之運作原理相同。再者，由於該些實質單元124、126、128個別而言屬於本領域之習知技術，且本技術領域人士可依據本發明之揭露及當前技術來實現該些實質單元124、126、128以及虛擬單元112、114、116，因此在不影響本發明之充分揭露及可實施性的前提下，不必要之說明在此予以節略。

【0014】承前所述，本發明除可如圖1般模擬無線網路服務裝置20以延伸其網路服務之範圍，使無線網路需求裝置30得以經由本發明以相同的連線設定連線至該無線網路服務裝置20，亦可依循前揭方式來模擬更多不同的無線網路服務裝置，以支援更多的無線網路需求裝置，由於本技術領域具有通常知識者可依前揭內容瞭解相同/相似的模擬暨連線過程，並能自行採用現有或自設的規則來進行多連線操作（例如複數個虛擬裝置輪流進行連線或發送中斷要求（Interrupt Request）以要求連線等），故在不影響本發明之揭露與可實施性的要求下，冗餘之說明在此予以節略。

【0015】除前述之裝置外，本發明亦相對應地揭露了一種網路服務擴展方法，能夠擴展一網路服務（例如一無線區域網路服務）之範圍，係由前揭網路服務擴展裝置10或其等效裝置來執行。如圖3所示，本發明之一實施例包含下列步驟：

步驟S310：建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連線；

步驟S320：依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同。本實施例中，該連線設定例如是一服務設定識別碼；一保密類型；以及一金鑰；

步驟S330：建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線。本實施例中，步驟S330包含：令該虛擬無線網路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在；以及令該虛擬無線網路服務單元依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號；以及
步驟S340：經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。本實施例中，步驟S340包含：建立該虛擬無線網路服務單元與該實質網路單元間的連線；經由該虛擬無線網路服務單元與該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及經由該實質網路單元與該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【0016】承上所述，步驟S340之封包傳送可藉由多種方式來實現，舉例而言，將該傳送封包傳輸至該無線網路服務裝置之步驟包含：經由該虛擬無線網路服務單元之一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層3協定層與該實質網路單元之一實質階層3協定層、一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及將該接收封包傳輸至該無線網路需求裝置之步驟包含：經由該實質網路單元之該實質實體層、該實質媒體存取控制層以及該實質階層3協定層與該虛擬無線網路服務單元之該虛擬階層3協定層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。另舉例而言，步驟S340亦可不透過階層3協定層而直接轉發該

傳送封包或接收封包，亦即將該傳送封包傳輸至該無線網路服務裝置之步驟包含：經由該虛擬無線網路服務單元之虛擬實體層以及虛擬媒體存取控制層與該實質網路單元之實質媒體存取控制層以及實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及將該接收封包傳輸至該無線網路需求裝置之步驟包含：經由該實質網路單元之實質實體層以及實質媒體存取控制層與該虛擬無線網路服務單元之虛擬媒體存取控制層以及虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【0017】由於本技術領域具有通常知識者可藉由圖1至圖2b之裝置發明的揭露內容來瞭解圖3之方法發明的實施細節與變化，因此，為避免贅文，在不影響該方法發明之揭露要求及可實施性的前提下，重複之說明在此予以節略。請注意，前揭圖示中，元件之形狀、尺寸、比例以及步驟之順序等僅為示意，係供本技術領域具有通常知識者瞭解本發明之用，非用以限制本發明。另外，本技術領域人士可依本發明之揭露內容及自身的需求選擇性地實施任一實施例之部分或全部技術特徵，或者選擇性地實施複數個實施例之部分或全部技術特徵之組合，藉此增加本發明實施時的彈性。再者，前揭實施例雖以無線區域網路為例，然此並非對本發明之限制，本技術領域人士可依本發明之揭露適當地將本發明應用於其它類型的網路系統中。

【0018】綜上所述，本發明之網路服務擴展裝置與方法能夠模擬一無線網路服務裝置以延伸其網路服務之範圍，並能使一無線網路需求裝置經由本發明以相同的連線設定連線至該無線網路服務裝置，亦即只要該無線網路需求裝置擁有該無線網路服務裝置之連線設定，即能透過本發明之中繼來連接該無線網路服務裝置以上網，藉此解決該無線網路服務裝置之服務範圍不足或服務死角

等問題，並增加該無線網路需求裝置之連線機會。

【0019】雖然本發明之實施例如上所述，然而該些實施例並非用來限定本發明，本技術領域具有通常知識者可依據本發明之明示或隱含之內容對本發明之技術特徵施以變化，凡此種種變化均可能屬於本發明所尋求之專利保護範疇，換言之，本發明之專利保護範圍須視本說明書之請求項所界定者為準。

【符號說明】

【0020】

10 網路服務擴展裝置

20 無線網路服務裝置

30 無線網路需求裝置

100 無線網路中繼裝置

110 虛擬無線網路服務單元

112 虛擬實體層

114 虛擬媒體存取控制層

116 虛擬階層3協定層

118 虛擬應用層

120 實質網路單元

122 實質應用層

124 實質階層3協定層

126 實質媒體存取控制層

128 實質實體層

S310 建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的連

線

S320 依據該無線網路服務裝置之連線設定提供一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同

S330 建立該虛擬無線網路服務單元與一無線網路需求裝置間的連線

S340 經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結

【發明申請專利範圍】

【第 1 項】一種網路服務擴展方法，能夠擴展一網路服務之範圍，係由一網路服務擴展裝置來執行，包含下列步驟：

建立一無線網路中繼裝置之一實質網路單元與一無線網路服務裝置間的無線連線；

依據該無線網路服務裝置之連線設定提供該無線網路中繼裝置之一虛擬無線網路服務單元，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；

建立該虛擬無線網路服務單元與一無線網路需求裝置間的無線連線；以及

經由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【第 2 項】如請求項第 1 項所述之網路服務擴展方法，其中建立該虛擬無線網路服務單元與該無線網路需求裝置間的連線之步驟進一步包含：

令該虛擬無線網路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在；以及

令該虛擬無線網路服務單元依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號。

【第 3 項】如請求項第 1 項所述之網路服務擴展方法，其中建立該無線網路服務裝置與該無線網路需求裝置間的連線之步驟進一步包含：

建立該虛擬無線網路服務單元與該實質網路單元間的連線；

經由該虛擬無線網路服務單元與該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及

經由該實質網路單元與該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【第 4 項】如請求項第 3 項所述之網路服務擴展方法，其中將該傳送封包傳輸至該無線網路服務裝置之步驟包含：

經由該虛擬無線網路服務單元之一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層 3 協定層與該實質網路單元之一實質階層 3 協定層、一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及

將該接收封包傳輸至該無線網路需求裝置之步驟包含：

經由該實質網路單元之該實質實體層、該實質媒體存取控制層以及該實質階層 3 協定層與該虛擬無線網路服務單元之該虛擬階層 3 協定層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【第 5 項】如請求項第 3 項所述之網路服務擴展方法，其中將該傳送封包傳輸至該無線網路服務裝置之步驟包含：

經由該虛擬無線網路服務單元之一虛擬實體層以及一虛擬媒體存取控制層與該實質網路單元之一實質媒體存取控制層以及一實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及

將該接收封包傳輸至該無線網路需求裝置之步驟包含：

經由該實質網路單元之該實質實體層以及該實質媒體存取控制層與該虛

擬無線網路服務單元之該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

【第 6 項】如請求項第 1 項所述之網路服務擴展方法，其中該無線網路服務裝置之連線設定包含：一服務設定識別碼；一保密類型；以及一金鑰。

【第 7 項】如請求項第 1 項所述之網路服務擴展方法，其中該網路服務係一無線區域網路服務。

【第 8 項】一種網路服務擴展裝置，能夠擴展一無線網路服務裝置之網路服務之範圍，包含：

一無線網路中繼裝置，用來與該無線網路服務裝置建立無線連線，包含：

一虛擬無線網路服務單元，係依據該無線網路服務裝置之連線設定而形成，用來與一無線網路需求裝置建立無線連線，其中該虛擬無線網路服務單元之連線設定與該無線網路服務裝置之連線設定相同；以及

一實質網路單元，用來與該虛擬無線網路服務單元建立連線以及與該無線網路服務裝置建立無線連線，

其中該無線網路中繼裝置藉由該虛擬無線網路服務單元以及該實質網路單元建立該無線網路服務裝置與該無線網路需求裝置間的連結。

【第 9 項】如請求項第 8 項所述之網路服務擴展裝置，其中該無線網路需求裝置所接收之該無線網路服務裝置之訊號強度小於該無線網路需求裝置所接收之該虛擬無線網路服務單元之訊號強度。

【第 10 項】如請求項第 8 項所述之網路服務擴展裝置，其中該虛擬無線網

路服務單元發出一信標以供該無線網路需求裝置得知該虛擬無線網路服務單元之存在，並且依據該無線網路需求裝置之一探詢要求訊號發出一探詢回應訊號。

【第 11 項】如請求項第 8 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元經由該實質網路單元將該無線網路需求裝置之一傳送封包傳輸至該無線網路服務裝置；以及該實質網路單元經由該虛擬無線網路服務單元將該無線網路服務裝置之一接收封包傳輸至該無線網路需求裝置。

【第 12 項】如請求項第 11 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元包含一虛擬實體層、一虛擬媒體存取控制層以及一虛擬階層 3 協定層；該實質網路單元包含一實質階層 3 協定層、一實質媒體存取控制層以及一實質實體層；該虛擬實體層接收該傳送封包，並依序經由該虛擬媒體存取控制層、該虛擬階層 3 協定層、該實質階層 3 協定層、該實質媒體存取控制層以及該實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及該實質實體層接收該接收封包，並依序經由該實質媒體存取控制層、該實質階層 3 協定層、該虛擬階層 3 協定、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

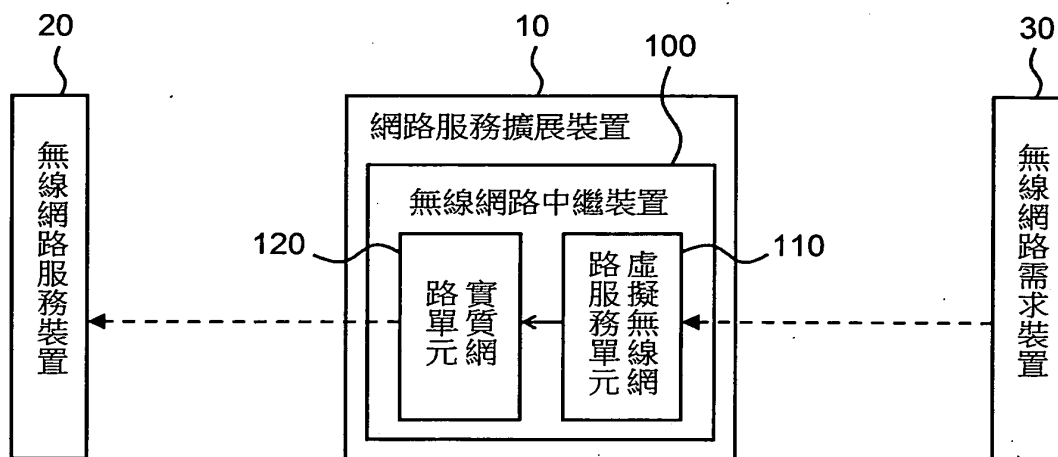
【第 13 項】如請求項第 11 項所述之網路服務擴展裝置，其中該虛擬無線網路服務單元包含一虛擬實體層以及一虛擬媒體存取控制層；該實質網路單元包含一實質媒體存取控制層以及一實質實體層；該虛擬實體層接收該傳送封包，並依序經由該虛擬媒體存取控制層、該實質媒體存取控

制層以及該實質實體層將該傳送封包傳輸至該無線網路服務裝置；以及該實質實體層接收該接收封包，並依序經由該實質媒體存取控制層、該虛擬媒體存取控制層以及該虛擬實體層將該接收封包傳輸至該無線網路需求裝置。

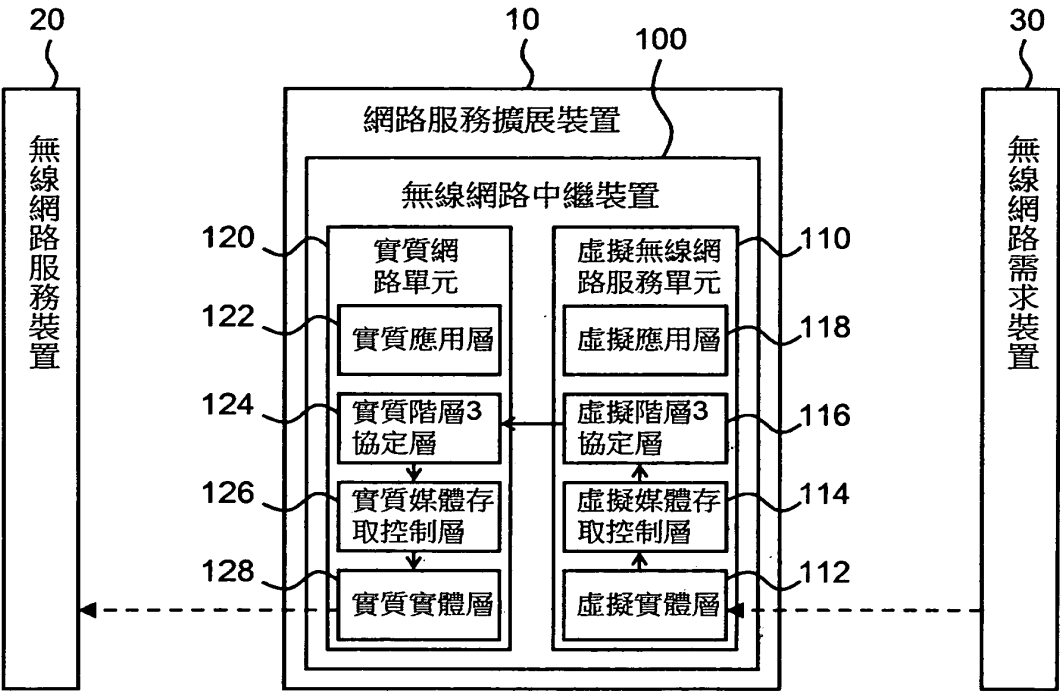
【第 14 項】如請求項第 8 項所述之網路服務擴展裝置，其中該無線網路服務裝置之連線設定包含：一服務設定識別碼；一保密類型；以及一金鑰。

【第 15 項】如請求項第 8 項所述之網路服務擴展裝置，其中該網路服務係一無線區域網路服務。

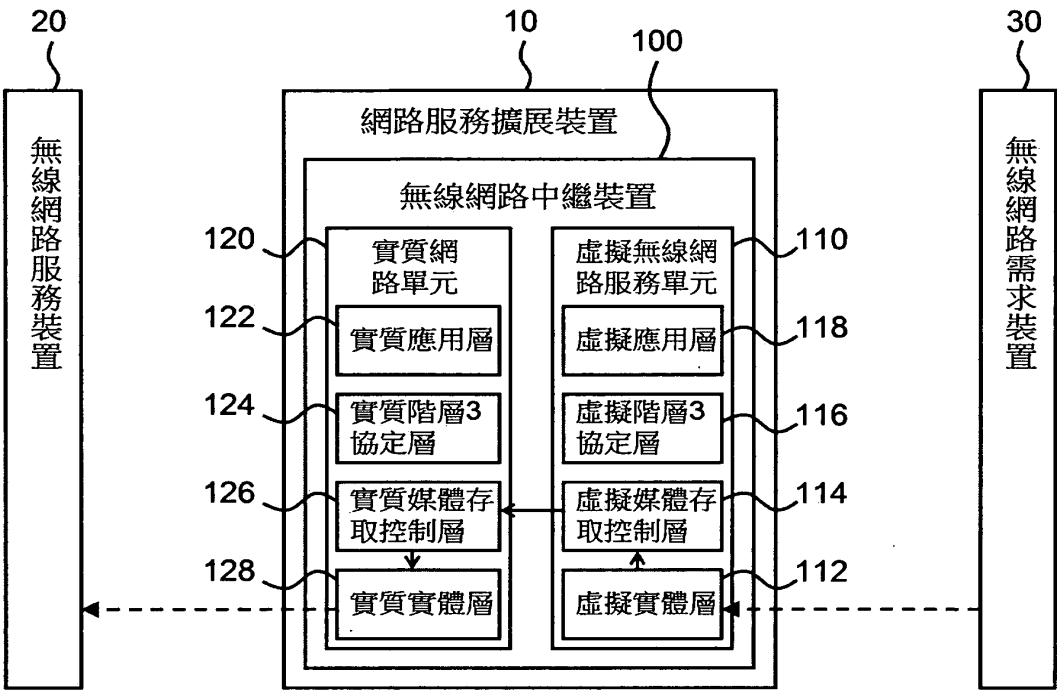
【發明圖式】



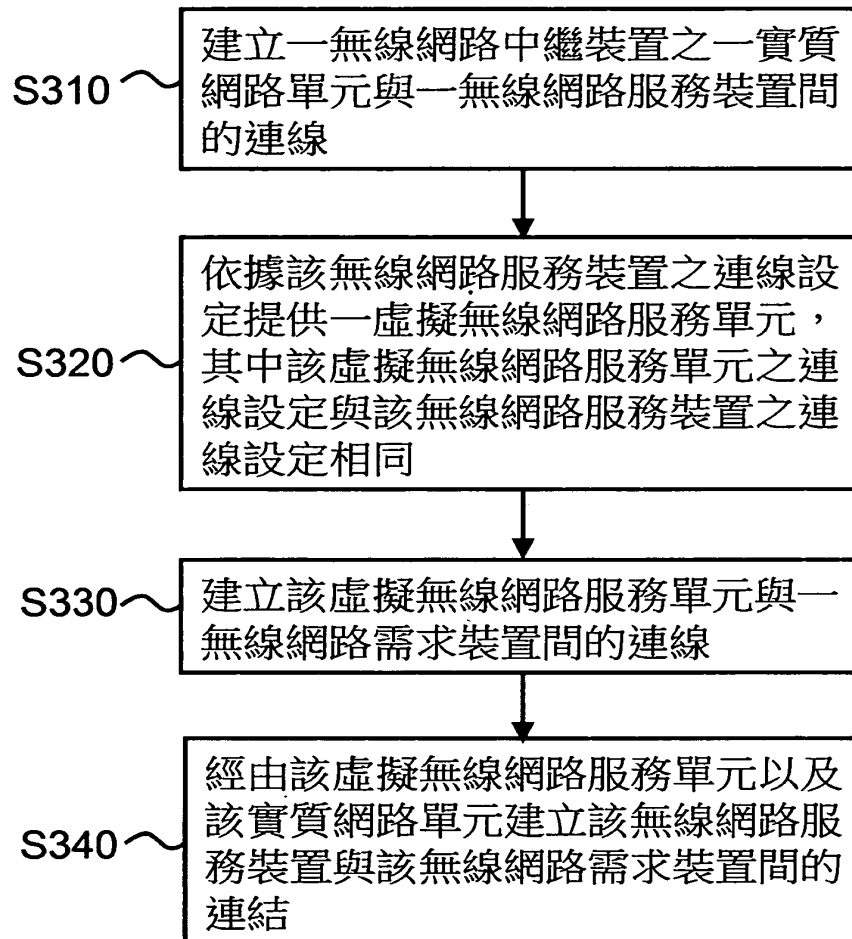
【圖1】



【圖2a】



【圖2b】



【圖3】

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: New Application
Confirmation No.:
First-Named Inventor: Sai C. Manapragada
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

INFORMATION DISCLOSURE STATEMENT TRANSMITTAL

1. List of All Patents, Publications, U.S. Applications, or Other Information

Pursuant to the provisions of 37 C.F.R. §§ 1.56, 1.97, and 1.98, applicant requests consideration of the references listed on the attached PTO/SB/08 form(s) [commonly referred to as a PTO-1449 form] and/or the additional information identified below.

2. Enclosed Legible Copies

2a. A legible copy of each foreign patent document and publication listed on the PTO/SB/08 form is enclosed:

- ☐ i. except, pursuant to MPEP 609.02, a copy is not provided for each reference previously cited by or submitted to the Patent Office in prior US Patent Application No(s). _____, filed _____, from which the present application claims priority under 35 U.S.C. § 120.
- ☐ ii. except, a copy is not provided for each cumulative reference and enclosed reference identified below:

☐ 2b. A copy of the specification and drawings for each cited unpublished U.S. application.

☐ 2c. A copy of a Search Report or Written Opinion from a foreign patent office is also enclosed.

- ☐ 2d. Consideration of the enclosed additional and/or below discussed information is requested.

3. Concise Explanation of Relevance for Non-English Language Information

For each non-English language reference listed on the attached PTO/SB/08 form(s), reference is made to:

- ☐ 3a. an English language translation submitted herewith,
- ☐ 3b. a foreign patent office Search Report (in the English language) submitted herewith,
- ☐ 3c. an English language translation of a foreign patent office Search Report submitted herewith,
- ☐ 3d. the concise explanation contained in the present application at page(s) _____,
- ☐ 3e. the concise explanation set forth in the attached English language abstract,
- ☐ 3f. a copy of a related patent publication (in the English language) cited herewith,

Foreign Patent Document	Corresponding English Language Patent Document

- ☒ 3g. the following concise explanation: The TW I500350B document itself contains an English version of the abstract.

4. Time for Filing

- ☒ 4a. This Information Disclosure Statement is submitted:
- ☒ i. for U.S. national applications or national stage PCT applications (not including CPAs and RCEs), within three months of filing or entry into national stage;
- ☒ ii. for U.S. national applications, national stage PCT applications, CPAs, or RCEs before the first Office Action on the merits;
and/or
- ☐ iii. before the mailing of an Office Action on the merits after the filing of a Request for Continued Examination (RCE) under § 1.114,

and thus no certification and/or fee is required.

- ☐ 4b. This information Disclosure Statement is submitted after three months from the filing date and after the first Office Action on the merits but prior to the mailing date of a final Office Action or Notice of Allowance, and thus:
 - ☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below, or
 - ☐ ii. the fee set forth in 37 C.F.R. § 1.17(p) is enclosed.
- ☐ 4c. This Information Disclosure Statement is submitted after the mailing date of a final Office Action or Notice of Allowance and prior to payment of the issue fee, and thus:
 - ☐ i. the statement specified in 37 C.F.R. § 1.97(e) is provided below and the fee set forth in 37 C.F.R. § 1.17(p) is enclosed, or
 - ☐ ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.
- ☐ 4d. This Information Disclosure Statement is submitted after payment of the issue fee, and thus:
 - i. a Petition to Withdraw from Issue pursuant to 37 C.F.R. § 1.313(c)(2) has been filed, and
 - ii. a Request for Continued Examination (RCE) and fee of 37 C.F.R. § 1.17(e) has been filed.

5. Certification- Statement Under 37 C.F.R. 1.97(e)

- ☐ 5a. It is hereby certified that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.
- ☐ 5b. It is hereby certified that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

The filing of this Information Disclosure Statement shall not be construed as an admission that the information cited is, or is considered to be, material to patentability as defined

in § 1.56(b). It is believed that no additional fees are required. Should any other fee be required, however, please charge such fee to Deposit Account No. 23-3030, but not to include any payment of issue fees.

Respectfully submitted,

By /Blake R. Hartz, Reg. No. 73453/
Blake R. Hartz, Reg. No. 73453
Woodard, Emhardt, Henry, Reeves & Wagner, LLP
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
Telephone: (317) 634-3456 Fax: (317) 637-7561
Email: bhartz@uspatent.com



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
18/448,281

RECEIPT DATE / TIME
08/11/2023 11:38:51 AM ET

ATTORNEY DOCKET #
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 # 62601310

FILING DATE -

CUSTOMER # 30565

FIRST NAMED INVENTOR Sai C. Manapragada

CORRESPONDENCE ADDRESS -

AUTHORIZED BY Blake Hartz

Documents

TOTAL DOCUMENTS: 30

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Application Data Sheet.pdf	4	Application Data Sheet	25 KB
Warning: This is not a USPTO supplied ADS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.			
IDS Transmittal.pdf	4	Transmittal Letter	24 KB
Oath Declaration.pdf	1	Oath or Declaration filed	196 KB
General POA.pdf	1	Power of Attorney	305 KB
Specification_Claims_Abstact-APP.TEXT.docx	26	Application body structured text document	70 KB

Warning: Bookmarks were found and have been removed.

SB08.pdf	5	Information Disclosure Statement (IDS) Form (SB08)	877 KB
Statement Under 37 CFR 3_73c.pdf	2	Power of Attorney	451 KB
Track One Request.pdf	1	Track One Request	296 KB
Drawings.pdf	11	Drawings-only black and white line drawings	1227 KB
npl_2013 March 19 beyond-802-11ac-a-very-high-capacity-wlan.pdf	12	Non Patent Literature	138 KB
npl_2013 July 15 hew-discussion-on-potential-techniques-for-hew.pdf	13	Non Patent Literature	191 KB
for_TWI500350B.pdf	24	Foreign Reference	1097 KB
npl_2011 WiSP-A-protocol-for-overcoming-MAC-overheads-using-packet-size-dependent-channel-widths.pdf	9	Non Patent Literature	617 KB
npl_2013 May 9 discussions-on-11ac-phy-efficiency.pdf	11	Non Patent Literature	314 KB
npl_2013 Sept 16 hew-dl-mu-mimo-transmission-with-unequal-bandwidth.pdf	5	Non Patent Literature	49 KB
Specification_Claims_Abstract.pdf	26	Auxiliary PDF of Application	77 KB
npl_2013 Nov 11 hew-	11	Non Patent Literature	56 KB

discussion-on-ofdma-in-hew.pdf

npl_2013 Nov 12 11-13-1331-02-0hew-proposed-direction-and-priorities-for-hew.pdf	17	Non Patent Literature	192 KB
npl_2012 J uly A-Channel-Splitting-Strategy-for-Reducing-Handoff-Delay-in-Internet-Based-Wireless-Mesh-Networks.pdf	13	Non Patent Literature	1584 KB
npl_2013 Sept 18 hew-discussion-on-access-mechanism-for-hew.pdf	10	Non Patent Literature	54 KB
npl_2013 Oct 16 An-Efficient-Cooperative-Retransmission-MAC-Protocol-for-IEEE-802.11n-Wireless-LANs-3.pdf	9	Non Patent Literature	262 KB
npl_2013 September 16 hew-multicat-transmission-for-hew.pdf	10	Non Patent Literature	83 KB
npl_2014 J uly 14 ax-envisioning-11ax-phy-structure-part-i.pdf	11	Non Patent Literature	185 KB
npl_E ng Abstract TWI500350B.pdf	2	Non Patent Literature	62 KB
npl_2014 J uly 9 ax-envisioning-11ax-phy-structure-part-ii.pdf	12	Non Patent Literature	76 KB
npl_J an 13 2013 Publication 1687-1499-2013-135.pdf	17	Non Patent Literature	1369 KB

npl_80211ac-2013.pdf	425	Non Patent Literature	4107 KB
npl_Performance_analysis_of_OFDMA_in_LTE.pdf	7	Non Patent Literature	5027 KB
npl_2012 OFMDA LTE Master's Thesis.pdf	74	Non Patent Literature	12702 KB
npl_Reference 10.pdf	12	Non Patent Literature	6410 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Application Data Sheet.pdf	272C112E78BF17D332105110687893ECBC3457ED33048D91C4 A23DB5527833315B6C01B5869767E2E4C93CC02CF76BB1554 22453814CB489BF31BE9A80879B60
IDS Transmittal.pdf	C36CED0CDD89075A155ED6F162F03F0E5868F3AB37B9AE2 13A443FE115FC28228C600DAF197E95391C876BDA7B3BBA3C B81A30401D75D2A6ED08AC8281BFC3C
Oath Declaration.pdf	9BA9631F8AFF266661D46D7EEC95129A9A368EF1E5ED22463 D6A690DA52332ADD71C28ECA167E0B4B5169863560A6FA6BD A77975F93479EE8D5E601BCFE951E9
General POA.pdf	6196807BB5FED014BD32FA6FAAABD254F8C3754BBC4A0E46 8D29133B3AEFE4766E96468860809FB772C797368229E1DB5E 23C2C195C7D9988C51CC0507238A8B
Specification_Claims_Abstract-APP.TEXT.docx	BE461A5C0BA5B4ADC5BB4C992CE6F237B49D86525B54CE0F 686175DE76363FA3F4A33F570402CC83979F28F313D96A0701 B9BDC966DB197F58CFD8E00E9DE043
SB08.pdf	219370C3A9B01F4302D65E98E622DCE30D718395DC8929A649 619C179651A264ED78D7B1A6D5F51190A54FDB412C91CC3D4 CA043FBD0CD012BC32BFE475CD93D

Statement Under 37 CFR 3_73c.pdf	5A26197293EC5975C00772F2875F3D7A7B547E97F371C035B9 49487C01FF04DF0A74D6852A39B227F54FD856F9F6D918FBB4 47CD43121EAA7CA50505F1D82340
Track One Request.pdf	4B90C274304266ECCB4D2BADC64CF46C3E69036B85780FF54 C5B1CA1B71C604436B4CB6A41A0B82DD5E5BA3E310438DBB E63E260BC5840F36AC34596A2BF787B
Drawings.pdf	31032E235A524B730658805C23AE57A81AA7190188E6C5D9EC BB807FF09A7719B9933ABAA502EA2346E572694D0EF5A5FB0 D7096CCA03C5F7E68F4DECB53BEF0
npl_2013 March 19 beyond- 802-11ac-a-very-high-capacity- wlan.pdf	9F085867BDA21190385406970D3C334FACD5A66C35DF163F25 0D3C7C6D163D127CE4AB777840C821184931D46CBF90FBFBA 4C23F17B84EC72EC7AE3F0C24376C
npl_2013 July 15 hew- discussion-on-potential- techniques-for-hew.pdf	BC34B3734A2F68E38302904CF0FA40DEAE5100041B07A3DCE 04B59D9BEDAA579D1924F2EB0F1C7D81BBE25ADE144DA5BC 4181B74018FF966BC0CE6A6E9F8B22A
for_TWI500350B.pdf	2A000ADDC8412D9E5F3D239BC2BB1B135699922BB9A65C99B 427F1248730557060442A6877F014E1118A515B156CE79ABDFF D22505CC9A24DE8E89CAD361ACDD
npl_2011 WiSP-A-protocol-for- overcoming-MAC-overheads- using-packet-size-dependent- channel-widths.pdf	A48832E58768E2755F8D0BB61A43AE75A3611A3A776F4A1BF0 DE2CC98CE23F06D17EA4DA4AD3758744A2737818F87339C74 82B6E8549753CA6971C6226697F03
npl_2013 May 9 discussions-on- 11ac-phy-efficiency.pdf	E74FDD326ACEA3D29C6BEFACE28A38530E1E7D13715A6691 4C1E3341EE6590BC1580831E68B3D318CCEEB76850D530630 BEE0A1A33C550616E73A638C8A92961
npl_2013 Sept 16 hew-dl-mu- mimo-transmission-with- unequal-bandwidth.pdf	19E03ADEDAFB8A5C5D2C26CB7AEF11DA9CCD35D02AB1116 544AB3DCA2010C39AD5384547DC7874F5C8EC75C0ED5AE70 E9AFAF0AC53CFA85B866ACC65DCF76462
Specification_Claims_Abtract.p df	FEFFC866260AFEE4BA4F79C0C4BE9136A6C78951382A78CB8 4AFCDF6792C9F31587B7D645881D61061E423227167658786B 4C45B64EEDB31E6B707C4C07E2D75

npl_2013 Nov 11 hew-discussion-on-ofdma-in-hew.pdf	5DFA22F587A184A597B34832FCE32A743252965679B136B381 93F8175493004D265C6E5B554985BAF7D98CB5DD9C49BF168 8E0FCC0F25F51C485DEE9BAD6F96E
npl_2013 Nov 12 11-13-1331-02-0hew-proposed-direction-and-priorities-for-hew.pdf	601D6BA15F858CA86097F071EBE11F30A7C6CE6D789332E89 73F7874BBCE8D9201C987C86FFC1893433011C65F5FBEDDB3 575B05E3E37786CB19C34910F054D0
npl_2012 J uly A-Channel-Splitting-Strategy-for-Reducing-Handoff-Delay-in-Internet-Based-Wireless-Mesh-Networks.pdf	7E20E028E9EBCBC4F25854C055631EEA30E4F5D370A7CCDD AA77C63F189E2D7CFD5D837B537562C8216D5FEC1E6EB8785 CFA0D544DCD16E9E1F0E979A7918041
npl_2013 Sept 18 hew-discussion-on-access-mechanism-for-hew.pdf	CE4E2EF7A953FFCEDAAF7B511A6D93E35E422D55305D38147 30B37073F49458298C71A947368A7EFD5EF2B0CA88915701CC F830E43ED4918AFDFD6E5A17AD720
npl_2013 Oct 16 An-Efficient-Cooperative-Retransmission-MAC-Protocol-for-IEEE-802.11n-Wireless-LANs-3.pdf	CB7D637C1185C0101205BB858C5562FF30EF75BFFB7C8272D 9B0C3104ED48C671F27093C8FE4C46F2928C4210EA4954F770 6AF1C3173A688C889DC0D079529ED
npl_2013 September 16 hew-multicat-transmission-for-hew.pdf	E51E2A58C69BC72A416E9051C05D5BF0C43E005557BC4322D C5B00CE1F48A1DA23076436D99AD93EAFCA40DBF37DAF97E7 EE180138AD96FE455CEE3E1226DE86B
npl_2014 J uly 14 ax-envisioning-11ax-phy-structure-part-i.pdf	B963B4763E98556CD02A7029CD0C3F8678A843736FFE9BC7E F6D36096481430F5265F24AB4800B22D2CB012864111DB9CAC 7E821B881AB75D61A9FA8FAAD03E0
npl_Eng Abstract TWI500350B.pdf	6898E7CAF03CA3488DC69E57288573F6BC41ABEF1B0006320 E5439DC3EB8F6878F48A8AC1736C1FD4744800C4A0CB422CA 5F42F5B4EA0E0AF753DAB665273993
npl_2014 J uly 9 ax-envisioning-11ax-phy-structure-part-ii.pdf	9FC232726897C2527248F09B8CD59837615DFFC93ED8D63152 8C3A6943DD77DB70D757AD71D38F3875213059832FA6A2F287 DD6FC2255DBCDCB637F1AB9B11BB
npl_J an 13 2013 Publication 1687-1499-2013-135.pdf	E0ABF7B6E016FA7404BB54CE1BFED7204F5D191ED88500EA9 04DFCEF241D0CBBC6AE24DE087E915CAB857B06A29979CA8

9D3CEABADE2D64333DCF6A991CF1851

npl_80211ac-2013.pdf	152C5B7E98E5DE608C85C57ED69109B40A39C580F84A14A92 A59946DFB9FD799A50FB1906CEDC91D386157AD0030C6D25A C7F5BF7F08EE1911E667FBAACB472E
npl_Performance_analysis_of_ OFDMA_in_LTE.pdf	545016E766232F2FAA6B3A5E79B5C2932E65299D6C61780387 FE02332481A44AFEDB5AC4E6B809E83E524A29C2DEB5BC28 35FE9FAD974C5B436C69ADD21AD09B
npl_2012 OFMDA LTE Master's Thesis.pdf	AE607AD3B61ED2BB2336645F4ADA8E618C56076DBBB4B287 CF8763B52EBA5074A903C88A7BA701C637CDB93BFE5D821C 93F35FF66850342FB62ED3432CD179C8
npl_Reference 10.pdf	DDE455A473686A48E280237782A435AF1FCA7A7057B9CB61F 03CFC50184079599A920361DA081CFCE223489BDA84CA0ABE 6D905FB8F7780DE9156AD04267D1D2

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.

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 <i>(Use as many sheets as necessary)</i>				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				
Sheet	2	of	5			

U.S. PATENT DOCUMENTS					
Examiner Initial *	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code ² (if known)			
	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	Damjanovic et al.	

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

Examiner Signature	Date Considered
-----------------------	--------------------

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

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

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

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786.9199) and select option 2.

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 <i>(Use as many sheets as necessary)</i>				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
Sheet	4	of	5	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		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 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 and select option 2.

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 <i>(Use as many sheets as necessary)</i>				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
Sheet	5	of	5	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 Technology, (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		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 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 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)Applicant/Patent Owner: XiFi Networks R&D Inc.Application No./Patent No.: / Filed/Issue Date: /Titled: METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL LAYERSXiFi Networks R&D Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 064462, Frame 0164, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2. 020505-000006

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Blake R. Hartz, Reg. No. 73453/

August 11, 2023

Signature _____

Date _____

Blake R. Hartz

73453

Printed or Typed Name _____

Title or Registration Number _____

[Page 2 of 2]



UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ELECTRONIC PAYMENT RECEIPT

APPLICATION #
18/448,281

RECEIPT DATE / TIME
08/11/2023 11:38:51 AM ET

ATTORNEY DOCKET #
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 # 62601310

AUTHORIZED BY Blake Hartz

CUSTOMER # 30565

FILING DATE -

CORRESPONDENCE
ADDRESS -

FIRST NAMED
INVENTOR Sai C. Manapragada

Payment Information

PAYMENT METHOD
CARD / 1649

PAYMENT TRANSACTION ID
E20238AB40505047

PAYMENT AUTHORIZED BY
W. Pat Moore

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	56.00	1	56.00
2817	REQUEST FOR PRIORITIZED EXAMINATION	1680.00	1	1680.00
2111	UTILITY PATENT APPL. SEARCH FEE	280.00	1	280.00
4011	BASIC FILING FEE- UTILITY	64.00	1	64.00
2311	EXAMINATION OF ORIGINAL PATENT APPLICATION	320.00	1	320.00

2202	EACH CLAIM IN EXCESS OF 20	40.00	10	400.00
TOTAL AMOUNT:				\$2,800.00

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

30565

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

30565

OR



Firm or individual name

Address

City

State

Zip

Country

Telephone

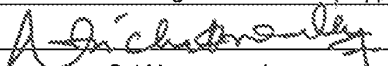
Email

Assignee name and address:
 XiFi Networks R&D Inc.
 21214 Chelton Beach Drive
 Cypress, TX 77433
 United States

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature		Date	July 29, 2023
Name	Sai Manapragada	Telephone	(510) 543-9655
Title	CEO		

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Sai C. Manapragada	Nonprovisional Application Number (if known):	
Title of Invention:	METHOD AND APPARATUS FOR PROCESSING BANDWIDTH INTENSIVE DATA STREAMS USING VIRTUAL MEDIA ACCESS CONTROL AND PHYSICAL L		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:

I. ☒ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

- i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
- ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

- i. A request for continued examination has been filed with, or prior to, this form.
- ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
- iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
- iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
- v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Blake R. Hartz, Reg. No. 73453/	Date August 11, 2023
Name (Print/Typed) Blake R. Hartz	Practitioner Registration Number 73453
Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.*	
☒ *Total of <u>1</u> forms are submitted.	