(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2007 (27.12.2007)

PCT

(10) International Publication Number
WO 2007/149598 A1

(51) International Patent Classification:
H04Q 7/38 (2006.01)

(21) International Application Number:
PCT/US2007/060486

(22) International Filing Date: 12 January 2007 (12.01.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/758,846 13 January 2006 (13.01.2006) US
11/621,875 10 January 2007 (10.01.2007) US

(71) Applicants *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI). **NOKIA INC.** [US/US]; 6000 Connective Drive, MS 1-4-755, Irving, Texas 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **EDNEY, Jonathon, P.** [GB/GB]; 31 High Street, Willingham Cambridgeshire CB4 5ES (GB). **FACCIN, Stefano** [US/US]; 3421 Dartmoor Drive, Dallas, Texas 75229 (US).

(74) Agents: **JEANG, Wei Wei** et al.; Haynes and Boone, LLP, 901 Main Street, Suite 3100, Dallas, Texas 75202-3789 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

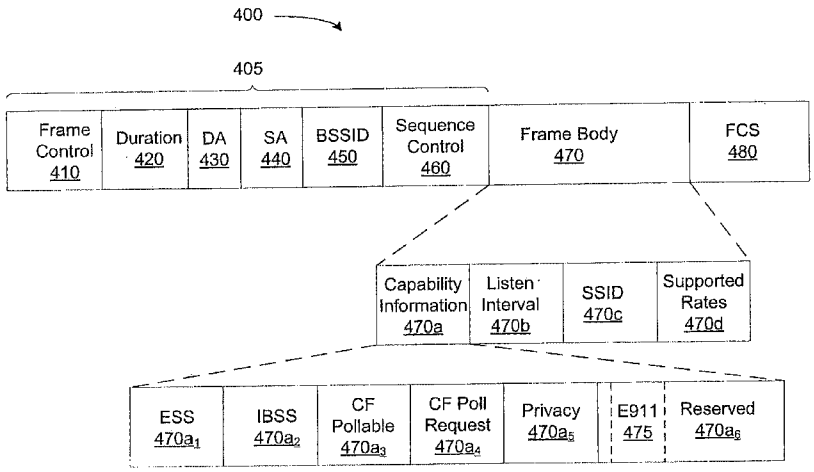
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEM AND METHOD FOR PROVISIONING OF EMERGENCY CALLS IN A SHARED RESOURCE NETWORK



(57) **Abstract:** A system and method for provisioning emergency services in a wireless local area network is provided. A station may assert an emergency service in a network by generating an association request that includes an indication of a request for an emergency service. The association request is transmitted to a network access point, and the station may be associated with the access point without engaging in an authentication procedure. Additionally, a network access point is provided that facilitates provisioning of emergency services to authenticated or unauthenticated network stations. An access point receives an association request that includes an indication of a request for an emergency service, and transmits an association response to a station that originated the association request. The originator of the association request may be associated with the access point without the access point engaging in an authentication procedure with the requesting station. Additionally, the access point may segregate emergency service traffic from general-purpose traffic to prohibit exploitation of the emergency service to fraudulently access other network services.

WO 2007/149598 A1

SYSTEM AND METHOD FOR PROVISIONING OF EMERGENCY CALLS IN A SHARED RESOURCE NETWORK

FIELD OF THE INVENTION

The present invention relates to shared resource network technologies and, more particularly, to mechanisms for enabling provisioning of emergency calls for users. Still more particularly, the present invention provides a system and method for provisioning emergency calls to authenticated and unauthenticated users in a wireless local area network.

BACKGROUND

Wireless local area networks (WLANs) are becoming increasingly popular for both business and residential applications. For instance, many companies are deploying WLANs in place of, or as an enhancement to, the corporate local area network. Additionally, many service industry businesses, e.g., restaurants and hotels, have deployed WLANs to provide customers with access to the Internet or other data networks.

Because a radio link is utilized for communication channels rather than utilization of a wireline connection, provisioning of emergency services in a WLAN similar to those commonly provided by fixed networks presents various technical challenges. For example, access to WLANs may involve various association and authentication procedures with access points to prohibit unauthorized user access to the WLAN. It is desirable to provide emergency services to user stations even in the event the user is not authorized to access the WLAN for general communication purposes. However, no mechanisms are currently available for enabling a WLAN station to determine if a WLAN access point is adapted to provide emergency services, such as enhanced 911 (E911) emergency services. Moreover, provisioning of unauthenticated WLAN station access to a WLAN presents security issues, such as the exploitation of the WLAN access point and the potential access to non-emergency services.

SUMMARY

It would be advantageous to provide a system and method for provisioning of emergency services in a wireless local area network. It would be further advantageous to provide for emergency service provisioning to unauthenticated wireless local area network stations. It would still be further advantageous to provide mechanisms that allow a wireless local area network station to identify access points that are adapted to provide emergency services. It would still be further advantageous to provide emergency services to unauthenticated wireless local area network stations in a manner that avoids exploitation of the wireless local area network access point.

Embodiments of the present invention provide a system and method for asserting emergency services in a wireless local area network. A station may assert an emergency service in a network by generating an association request that includes an indication of a request for an emergency service. The association request is transmitted to a network access point, and the station may be associated with the

access point without engaging in an authentication procedure. Mechanisms are provided for segregating emergency service traffic from other general purpose traffic to prohibit fraudulent exploitation of network infrastructure.

BRIEF DESCRIPTION OF THE DRAWINGS

Aspects of the present disclosure are best understood from the following detailed description when read with the accompanying figures.

Figure 1 is a simplified block diagram of an exemplary network environment in which embodiments disclosed herein may be implemented;

Figure 2 is a diagrammatic representation of an embodiment of a service indication information element that facilitates provisioning of emergency calls in a shared resource network;

Figure 3 is a diagrammatic representation of an embodiment of a basic service set identifier information field that facilitates advertisement of E911 capabilities;

Figure 4 is a diagrammatic representation of an embodiment of an association request frame that may be generated by a station for asserting an emergency service in a network;

Figure 5 is a diagrammatic representation of an embodiment of a virtual local area network table depicted in Figure 1 that is maintained, or otherwise accessible, by an emergency services compliant access point that facilitates segregation of emergency service traffic from non-emergency service traffic;

Figure 6 is a flowchart of an embodiment of an access point processing routine that facilitates provisioning of emergency services; and

Figure 7 is a flowchart of an embodiment of an access point processing subroutine for processing a request for emergency services from a currently associated station.

DETAILED DESCRIPTION

It is to be understood that the following disclosure provides many different embodiments, or examples, for implementing different features of various embodiments. Specific examples of components and arrangements are described below to simplify the present disclosure. These are, of course, merely examples and are not intended to be limiting. In addition, the present disclosure may repeat reference numerals and/or letters in the various examples. This repetition is for the purpose of simplicity and clarity and does not in itself dictate a relationship between the various embodiments and/or configurations discussed.

Figure 1 is a simplified block diagram of an exemplary network 100 environment in which embodiments disclosed herein may be implemented. Network 100 is an example of a shared resource network. For example, network 100 may be implemented as a wireless local area network (WLAN) conforming to the Institute of Electrical and Electronics (IEEE) 802.11 standards.

In the illustrative example, network 100 comprises two basic service sets (BSSs) 10-11 although any number of BSSs may be included in network 100. BSSs 10-11 provide respective coverage areas (illustratively designated with dashed lines) in which WLAN stations (STAs) 20-23 may communicate

via a wireless medium with one another or with other communication or computational devices in other external networks that interface with network 100. STAs 20-23 each have an associated address, such as one of respective Media Access Control (MAC) addresses MAC:A-MAC:D. A Media Access Control address is uniquely associated with the device hardware, e.g., a network interface card such as secure digital input/output card, a compact flash card, a miniPCI port card, or a PCMCIA card. The MAC address uniquely identifies the device within network 100. MAC addresses are typically implemented as a predefined length binary number, such as a 48-bit value. In the illustrative example, MAC addresses designated as alphabetic values are provided for illustrative purposes and are representative of binary physical addresses. Additionally, each of STAs 20-23 may have a logical, e.g., Internet protocol (IP) address, associated therewith. BSSs 10-11 are communicatively interconnected by a distribution system (DS) 30. DS 30 enables mobile device support by providing requisite logical services for handling address to destination mapping and integration of multiple BSSs. Each BSS includes an access point (AP) that provides access to DS 30. In the illustrative example, each of BSSs 10-11 have a respective AP 40-41. DS 30 provided by APs 40-41 and BSSs 10-11 facilitate creation of a wireless network of arbitrary size and complexity, and the collection of DS 30 and BSSs 10-11 is commonly referred to as an extended service set network. Logical integration between network 100 and non-IEEE 802.11 LANs, e.g., LAN 50, may be provided by a portal 60. Various other configurations of network 100 are possible. For example, coverage areas provided by BSSs 10 and 11 may partially overlap or may be collocated. Moreover, embodiments of the invention may be deployed in a WLAN comprising a single independent BSS. Additionally, wireless virtual local area networks (VLANs) may be configured in network 100. To this end, one or more APs, such as AP 40, may include or interface with a VLAN table 70. A VLAN may be configured to facilitate segregation of emergency traffic from general purpose traffic (i.e., non-emergency traffic) as described more fully hereinbelow.

Provisioning of emergency services may be provided by an emergency network 90 that is interconnected with LAN 50. Emergency network 90 may include a public safety answering point (PSAP) 95 at which emergency personnel may be connected with an emergency call. In the illustrative example, AP 40 interconnects with emergency network 90 by way of LAN 50. For example, AP 40 may interconnect with a router 80 that is communicatively coupled with PSAP 95. Various PSAPs may be disposed in emergency network 90, and any number of network components may be used to connect AP 40 with an appropriate PSAP. Depiction of a coupling between AP 40 and PSAP 95 by way of router 80 is for illustrative purposes only.

Each of STAs 20-23 may be implemented as a respective data processing system adapted for communication in a wireless network, such as a wireless laptop computer, a personal digital assistant, a cellular telephone, or other device capable of wireless data communications. A STA may comprise a processing unit, such as a general purpose microprocessor and/or an application specific integrated circuit, a memory device, such as a random access memory, a read-only memory, or another storage device for holding machine-readable data, a communication interface, such as an expansion slot and wireless communication card or a wireless communication interface integrated with the STA hardware,

and various other components and peripheral devices. A wireless communication interface of a STA may be, for example, implemented as a secure digital input/output (SDIO) port and accompanying SDIO WLAN card, a compact flash (CF) port and CF WLAN card, a miniPCI port and miniPCI WLAN card, a Personal Computer Memory Card International Association (PCMCIA) port and PCMCIA WLAN card, or other suitable wireless communication devices.

Aspects of the present invention may be implemented in software, hardware, firmware, or a combination thereof. The various elements of the system, either individually or in combination, may be implemented as a computer program product tangibly embodied in a machine-readable storage device for execution by a processing unit. Various steps of embodiments of the invention may be performed by a computer processor executing a program tangibly embodied on a computer-readable medium to perform functions by operating on input and generating output. The computer-readable medium may be, for example, a memory in an AP or a transportable medium such as a compact disk, a floppy disk, or a diskette, such that a computer program embodying the aspects of the present invention can be loaded onto a computer. The computer program is not limited to any particular embodiment, and may, for example, be implemented in an operating system, application program, foreground or background process, driver, or any combination thereof, executing on a single computer processor or multiple computer processors. Additionally, various steps of embodiments of the invention may provide a data structure generated, produced, received, or otherwise implemented on a computer-readable medium, such as a memory.

While the descriptions of a shared resource network, devices operating therein, and wireless medium transmissions made within the shared resource network are provided herein according to IEEE 802.11 protocols, functionality, and nomenclature, such examples are illustrative only and implementations of the invention are not limited to any particular network, network-compliant device, or network communication formats or protocols. Furthermore, descriptions of the invention provided herein in relation to implementations in an IEEE 802 conformant network are illustrative only and are provided only to facilitate an understanding of the invention. Embodiments of the present invention may be implemented on other network architectures and devices that utilize shared resources for effecting data communications.

In accordance with embodiments disclosed herein, E911 capable network components, such as AP 40 shown in Figure 1, may advertise the E911 capabilities to STAs within network 100 by one or more of various mechanisms. For example, an AP may advertise E911 capabilities in a beacon frame, a probe response frame, a neighbor information element, or another suitable data structure. The receipt, or lack thereof, of the E911 capability advertisement by a STA allows the STA to identify whether the AP supports emergency calls. Additionally, the AP may also advertise whether quality of service (QoS) mechanisms are supported for unauthenticated E911 calls.

In accordance with an embodiment, the E911 capability may be advertised in one or more of existing information elements by an otherwise unused or free bit. In accordance with another embodiment, an E911 advertisement may be made through the introduction of a service indication information element (IE) as described below.

Figure 2 is a diagrammatic representation of an embodiment of a service indication information element 200 that facilitates provisioning of emergency calls in a shared resource network. In the illustrative example, service indication information element 200 comprises a data structure of two octets including an E911 bit field 210. E911 bit field 210 may be set to a particular value, e.g., "1", to indicate the AP transmitting IE 200 is E911-capable. Additionally, IE 200 may include an optional E911 QoS bit field 220 that may be set to a particular value, e.g., "1", to indicate that the transmitting AP supports quality of service mechanisms for unauthenticated E911 calls. Other data may be included in field 230.

In accordance with another embodiment, a reserved bit of an information field in a BSSID may be set to advertise E911-capabilities of an AP. Additionally, another reserved bit may be set to indicated QoS support of E911 calls as described below.

Figure 3 is a diagrammatic representation of an embodiment of a basic service set identifier (BSSID) information field 300 that facilitates advertisement of E911 capabilities. Exemplary information field 300 comprises a two octet data structure that includes a reachability bit field 310, a robust security networks (RSN) bit field 320, a key scope bit field 330, a capabilities bit field 340, and a reserved bit field 350. Reachability bit field 310 comprises a two-bit field that indicates whether the AP represented by the BSSID is reachable by a STA for pre-authentication purposes. RSN bit field 320 comprises a single bit field that indicates whether the AP represented by the BSSID matches the RSN IE capabilities of the current AP. Key scope bit field 330 comprises a single bit field that indicates whether the AP represented by the BSSID has the same authenticator identity as the AP sending the information field. Capabilities field 340 comprises a five-bit field that indicates various capability information, e.g., spectrum management, QoS, radio measurement, etc., of the AP represented by the BSSID.

In accordance with an embodiment, a bit 350a of reserved bit field 350 may be set to indicate the AP supports E911 calls. Additionally, another bit 350b of reserved bit field 350 may be set to indicate QoS support of E911 calls. Information field 300 may be included in a neighbor list entry of a neighbor list component of a neighbor report element that may be transmitted by an AP for receipt by STAs in network 100.

In another embodiment, domains, such as a security domain, a roaming domain, or the like, may be introduced in network 100. In such a network configuration, an embodiment may be implemented to provide E911 capability advertisements in an information element configured to describe the particular domain. Alternatively (or in addition thereto) reserved bit field mechanisms may be implemented in a manner similar to that described above with reference to Figure 3 for providing E911 capability advertisements.

A STA may implement any one or more of various mechanisms for discovering E911 calls within network system 100. If a STA is unassociated or unauthenticated, the STA may attempt discovery of an E911-capable AP by passive or active scanning. In a passive scanning mode, a STA may evaluate beacon frames for an indication of E911 capabilities. In an active scanning mode, a STA may generate and transmit a probe request, and evaluate any received probe response for an indication of E911 capabilities therein. If a STA is associated or authenticated, the STA already has information regarding the E911

capabilities of the AP with which the STA is associated. In another implementation, a STA may evaluate information in a neighbor report to identify whether an AP has E911 capabilities. For example, if a STA needs to identify a target AP for roaming during an E911 call, a neighbor report may be evaluated to identify a suitable candidate for handover to maintain the call. In another scenario, a STA may be involved in a regular (non-E911 call), and may evaluate a neighbor report for E911 capabilities of candidate APs to ensure that a selected AP for handover supports E911 calls. In other implementations, APs identified in a neighbor report as supporting E911 calls may be given precedent over non-E911 call compliant APs for handover purposes.

In accordance with an embodiment, an unauthenticated STA asserts an access attempt to the emergency service by way of an indicator included in an association request frame generated and transmitted by the STA. In one implementation, the indicator may be comprise a bit set to a value, e.g., "1," that indicates a request to access emergency service. For example, the bit may comprise a reserved bit in the capability information field of the association request frame. In another implementation, the bit may comprise a bit in an information field that is included within the association request, e.g., in a manner similar to E911 bit field 210 shown in Figure 2.

Additionally, other bit(s) or indicator(s) may be included in an association request. For example, additional bits or indicators may be included in the association request to specify a particular emergency service in the event that a plurality of emergency services may be supported. In this instance, multiple bits of the capabilities field may be designated for emergency service designations. An AP, in response to receipt of an association request, returns an association response that includes an indication of whether the AP supports the requested emergency service(s). Such an indication in the association response may be provided by designation of one or more bits of an association response to emergency service capability indicators, by return of an information element that provides an indication of the supported emergency service(s), or the like.

Advantageously, an AP that supports the requested emergency service may accept the association of any STA (assuming protocol compatibility) thereby providing emergency service to both authenticated and unauthenticated STAs. Moreover, the need to perform a 4-way handshake with an unauthenticated STA is averted because no keys are required to be created for authentication. Thus, no encryption keys are required to be setup between an unauthenticated STA and the AP.

Figure 4 is a diagrammatic representation of an association request frame 400 that may be generated by a STA for asserting an emergency service in a network. Association request frame 400 comprises a MAC header 405 that includes a frame control field 410, a duration field 420, a destination address field 430, a source address field 440, a basic service set identification field 450, and a sequence control field 460 that each may include subfields thereof and may be formatted in accordance with the IEEE 802.11 standard. Association request frame 400 may include a frame body field 470 that includes a capability information subfield 470a, a listen interval subfield 470b, a service set identifier subfield 470c, and a supported rates subfield 470d. Additionally, association request frame 400 may include a frame check sequence (FCS) field 480.

Capability information subfield 470a may include an extended service set (ESS) subfield $470a_1$, an independent basic service set subfield $470a_2$, a coordination function (CF) pollable subfield $470a_3$, a coordination function poll request subfield $470a_4$, a privacy subfield $470a_5$, and a reserved subfield $470a_6$. In accordance with embodiments disclosed herein, a STA desiring emergency services may assert a request therefor by including an indicator of a requested emergency service within reserved subfield $470a_6$. For example, an E911 bit 475 may be included within reserved field $470a_6$ that may be interpreted by a receiving AP as a request for an emergency service. The AP may then invoke an association service to associate the transmitting STA to the AP without the invocation of an authentication service. In a similar manner, a QoS bit may be included in reserved subfield $470a_6$.

It is desirable to avoid exploitation of wireless local area network infrastructure, such as access points, from fraudulent unauthenticated users. To this end, embodiments disclosed herein may provide for the segregation of emergency service traffic from other non-emergency traffic.

In accordance with embodiments disclosed herein, emergency service traffic may be bridged to a common network entity dedicated to emergency services to facilitate segregation of emergency traffic from other network traffic. In one implementation, a particular VLAN configured in network 100 is dedicated to emergency service traffic. For example, a pre-established tunnel may be associated with the VLAN dedicated to emergency service traffic.

Figure 5 is a diagrammatic representation of VLAN table 70 depicted in Figure 1 that is maintained, or otherwise accessible, by an emergency services compliant AP. Table 70 maps or otherwise logically associates identifiers of STAs to one or more particular VLANs. An identifier of a STA that is mapped to a particular VLAN may, for example, comprise a MAC address of the STA. Table 70 may be implemented as a lookup table comprising a plurality of records 520 and fields 530. Table 70 may be stored in a storage medium, such as a random access memory, dynamic random access memory, or the like, of an AP, such as AP 40 shown in Figure 1.

Each record 520a-520f, or row, comprises associated data elements in respective fields 530a-530b. In the present example, field 530a stores physical addresses of STAs. Thus, for example, field 530a stores various MAC addresses of STAs within, or that may have been within, BSS 10. Field 530b stores VLAN identifiers to which a STA with a MAC address specified in a common record is associated. For example, field 530b of record 520a indicates a VLAN "01" to which the STA having MAC address "A" is associated. That is, STA 20 depicted in Figure 1 is assigned to a VLAN having an identifier "01." In a similar manner, STAs having MAC addresses "B" – "F" are assigned to one of VLANs having a VLAN identifier of "01," "02," or "03."

In accordance with an embodiment, a particular VLAN may be dedicated to servicing emergency service traffic. For example, assume the VLAN "01" is dedicated to emergency service traffic. Accordingly, STAs having MAC addresses "A" and "D" have asserted an emergency service in a respective association request transmitted to the servicing AP, and all traffic for STAs having MAC addresses of "A" and "D" is segregated from other general-purpose traffic, e.g., traffic bridged to VLANs "2" and "3." Thus, all data frames generated by a STA that has asserted an emergency service call

during association are bridged to the VLAN "01" dedicated to emergency service traffic. In this manner, all emergency traffic, whether from an authenticated or unauthenticated user, is segregated from non-emergency traffic, and exploitation of other network services by an AP fraudulently asserting an emergency service to gain network access to other non-emergency services is advantageously thwarted.

If an emergency service is asserted by an authenticated and associated station, the AP may disassociate the STA and, subsequently, re-associate the station to facilitate emergency service provisioning in accordance with an embodiment. For example, assume STA 21 (having MAC address "B") is engaged in a general purpose session within network 100 and is assigned to VLAN "02" as depicted in Figure 5. If a user of STA 21 attempts to assert an emergency service by transmitting an association request with an asserted emergency service request indicator, AP 40 may invoke a disassociation service to terminate the current association, and complete an association service with the requesting STA. In this implementation, the assignment of STA 21 to VLAN "02" may be terminated, and STA 21 may be reassigned to VLAN "01" (that is, the VLAN dedicated to emergency service traffic). Accordingly, additional security to network 100 is provided by prohibiting a single STA from concurrent assignment to a general purpose VLAN and a VLAN allocated for emergency service traffic.

Other embodiments may, however, permit an authenticated STA to be assigned to multiple VLANs if network 100 is configured to support the concurrent assignment of multiple VLANs to a STA. In this manner, a faster connection with the emergency service network may be provided by allowing invocation of the association service in response to the service request from an authenticated station without first requiring a disassociation service to complete. For example, if authenticated STA 21 is engaged in a general purpose session and is assigned to VLAN "02" when a user attempts assertion of an emergency service, AP 40 may, upon recognition of the emergency service request, invoke an association service to assign STA 21 to VLAN "01" dedicated to emergency service traffic. In this implementation, assignment of STA 21 to VLAN "01" may be made without terminating the assignment of STA 21 to VLAN "02." Thus, STA 21 may be assigned to one or more general purpose VLANs and a VLAN dedicated to emergency service traffic. Advantageously, AP 40 is not required to complete a disassociation service with STA 21 prior to connecting STA 21 with emergency network 90.

In accordance with another embodiment, emergency service traffic segregation may be implemented by dedicating one or more network components to servicing such traffic. For example, one or more routers or other network devices, such as router 80, may be dedicated to only handling emergency service traffic. In the illustrative example of Figure 1, AP 40 may forward all emergency service traffic to router 80 upon recognition of the traffic as related to an emergency service. For example, AP 40 may evaluate an association request for inclusion of an emergency service request indicator (such as assertion of E911 bit 475), and complete the association (assuming the STA is unassociated) with the requesting STA. Emergency related traffic from the newly associated STA is then forwarded to router 80 upon completion of the association service. Router 80, in turn, may convey the emergency service data to emergency network 90. Accordingly, traffic from a STA asserting an

emergency service may be routed to a router dedicated to emergency services thereby segregating emergency service traffic from other general purpose traffic.

In the event that a STA requesting an emergency service is associated and authenticated (that is, the STA is in a local state 3), a security association is already established between the AP and requesting STA at the time the emergency service request is made. In this situation, the AP may evaluate the STA requesting the emergency service as both associated and authenticated. The AP may then tear-down or otherwise delete the existing security association of the requesting STA and notify the STA accordingly, e.g., by way of an association response or other association acknowledgement message. Responsive to termination of the association, the STA may then generate and transmit another association request with an emergency service request indicator. The AP, on receipt of the association request, may complete the association without engaging the STA in authentication procedures, and emergency service data is then forwarded to the router dedicated to emergency service traffic.

Figure 6 is a flowchart of an embodiment of an access point processing routine that facilitates provisioning of emergency services. The AP processing routine is invoked (step 602), and the AP awaits receipt of an association request (step 604). On receipt of an association request, the AP evaluates whether an emergency service is requested (step 606). For example, the AP may evaluate a particular bit field, such as reserved subfield $470a_6$ of request frame 400 depicted in Figure 4 to determine if E911 bit 475 is asserted. If an emergency service is requested, the AP may then evaluate whether the requesting STA, that is the STA that originated the received association request, is currently associated with the AP (step 608). In the event that the STA is already associated with the AP (and is thus already authenticated), the AP may optionally delete an existing security association, e.g., a security association resulting from an 802.1x authentication service, of the STA (step 610). The AP may then proceed to segregate emergency service related traffic of the STA from other general purpose network traffic (step 613), and the AP processing routine cycle may end (step 618). In the event that the requesting station is evaluated as not currently associated with the AP at step 608, the AP processing routine may proceed to invoke an association service (step 611), and may optionally invoke an 802.11 MAC authentication service (step 612). Emergency service related traffic of the newly associated STA may be segregated from other general-purposed traffic according to step 613.

Returning again to step 606, the AP processing routine may invoke an association service (step 614) in the event that an emergency service is not requested. Upon completion of the association service, an authentication service may be invoked (step 616). For example, the authentication service may be implemented as an 802.11 MAC authentication. The AP processing routine cycle may then end according to step 618.

Figure 7 is a flowchart of an embodiment of an access point processing subroutine for processing a request for emergency services from a currently associated STA. In the embodiment depicted in Figure 7, the servicing AP and network 100 (or a portion thereof) is configured to segregate emergency service traffic from general purpose traffic by way of a router dedicated to emergency service traffic. The processing steps depicted in Figure 7 generally correspond to steps 610 and 613 shown in Figure 6 when

the AP processing routine of Figure 6 is implemented for segregating emergency traffic by way of a dedicated network router.

The AP invokes a security association deletion service (step 702), e.g., upon recognition that a received association request includes a request for an emergency service and is originated by a STA that is currently associated. The security association deletion service may provide the deletion of the security association of the requesting STA. A security association deletion notice or other indicator may then be generated by the AP (step 704) and transmitted to the STA (step 706). Alternatively, the security association deletion notice generated by the AP and transmitted to the STA may be implemented as an association response. The AP then forwards any traffic received from the STA to a router dedicated to emergency service traffic (step 708).

In accordance with embodiments disclosed herein, fast BSS transition is supported during E911 calls or other emergency services provided in network 100. Because STAs may access E911 services without authenticating with an AP, no authentication and key derivation functions are performed, and thus delays typically associated with security and QoS functions are averted. Accordingly, a STA can roam from one AP to another AP during an E911 call by simply repeating the initial connect procedure.

In another embodiment, interoperability with fast BSS transition enabled systems may be implemented by allowing a STA to decide whether fast transition abilities are desired. In this implementation, when a STA makes an initial connection for E911 service, pre-authentication and keying models are performed by the STA prior to a transition, e.g., in accordance with the IEEE 802.11r standard. If a STA is not to perform fast transitions, the STA may assert an E9111 connection without any authentication procedures. To implement such a mechanism, a pre-shared key (PSK) mechanism may be deployed wherein a pre-shared key is provided to STAs. Such a mechanism would allow the use of fast BSS transition procedures of unauthenticated STAs in general accordance with those specified in IEEE 802.11r.

As described, embodiments disclosed herein provide a system and method for asserting emergency services in a wireless local area network. A station may assert an emergency service in a network by generating an association request that includes an indication of a request for an emergency service. The association request is transmitted to a network access point, and the station may be associated with the access point without engaging in an authentication procedure. Additionally, a network access point is provided that facilitates provisioning of emergency services to authenticated or unauthenticated network stations. An access point receives an association request that includes an indication of a request for an emergency service, and transmits an association response to a station that originated the association request. The originator of the association request may be associated with the access point without the access point engaging in an authentication procedure with the requesting station. Additionally, the access point may segregate emergency service traffic from general-purpose traffic to prohibit exploitation of the emergency service to fraudulently access other network services.

Embodiments disclosed herein may be implemented as an executable instruction set embodied in hardware, software, firmware, or a combination thereof and may comprise computer-executable

instructions or code that may be fetched from a memory and executed by a processing unit of a data processing system. Computer-executable instructions that implement embodiments disclosed herein may be maintained or executed, in whole or in part, within a WLAN STA, an expansion card interfaced therewith, a WLAN AP, or a combination thereof. The instruction set is preferably maintained on any one of various computer-readable mediums. In the context of this document, a "computer-readable medium" can be any means that can contain, store, communicate, propagate or transport the instruction set for use by or in connection with an instruction execution system, apparatus, or device. The computer-readable medium can be, for example, but is not limited to, an electronic, magnetic, optical, electro-magnetic, infrared, or semi-conductor system, apparatus, device, or propagation medium now known or later developed.

Although embodiments of the present disclosure have been described in detail, those skilled in the art should understand that they may make various changes, substitutions and alterations herein without departing from the spirit and scope of the present disclosure. Accordingly, all such changes, substitutions and alterations are intended to be included within the scope of the present disclosure as defined in the following claims.

WHAT IS CLAIMED IS:

1. A method of asserting an emergency service in a network, comprising:

generating an association request that includes an indication of a request for an emergency service;

transmitting the association request to a network access point; and

receiving an association response without engaging in an authentication procedure.

2. The method of claim 1, further comprising receiving an emergency service advertisement that includes an indicator of an emergency service capability.

3. The method of claim 2, wherein receiving an emergency service advertisement further comprises receiving an information element that includes the indicator implemented as a bit field.

4. The method of claim 1, further comprising receiving an emergency service advertisement in a beacon frame.

5. The method of claim 1, further comprising receiving an emergency service advertisement in a probe response frame responsive to transmitting a probe request frame.

6. The method of claim 1, further comprising receiving an emergency service advertisement in a neighbor report.

7. A method of providing an emergency service in a network, comprising:

receiving an association request that includes an indication of a request for an emergency service; and

transmitting an association response to a station that originated the association request without engaging in an authentication procedure.

8. The method of claim 7, further comprising transmitting an emergency service advertisement that includes an indicator of an emergency service capability.

9. The method of claim 8, wherein transmitting an emergency service advertisement further comprises transmitting an information element that includes the indicator implemented as a bit field.

10. The method of claim 7, further comprising transmitting an emergency service advertisement in a beacon frame.

11. The method of claim 7, further comprising transmitting an emergency service advertisement in a probe response frame responsive to receiving a probe request frame.

12. The method of claim 7, further comprising transmitting an emergency service advertisement in a neighbor report.

13. The method of claim 7, further comprising:

evaluating a station that originated the association request as currently associated; and

deleting an existing security association of the station.

14. The method of claim 7, further comprising assigning a station that originated the association request to a virtual local area network dedicated to emergency service traffic.

15. The method of claim 7, further comprising :

transmitting emergency service related traffic originated by a station that transmitted the association request over a pre-established tunnel from an access point to an emergency network; and

receiving, by the access point, emergency service related traffic originated by an entity in an emergency network over a pre-established tunnel between the access point and the emergency network.

16. A device adapted to perform communications in a network, comprising:

a memory adapted to store a set of executable instructions; and

a processing unit adapted to, responsive to execution of the set of executable instructions, generate an association request that includes an indication of a request for an emergency service, transmit the association request to a network access point, and receive an association response without engaging in an authentication procedure.

17. The device of claim 16, wherein the processing unit receives an emergency service advertisement that includes an indicator of an emergency service capability.

18. The device of claim 17, wherein the emergency service advertisement comprises an information element that includes the indicator implemented as a bit field.

19. The device of claim 17, wherein the processing unit receives the emergency service advertisement in a beacon frame.

20. The device of claim 17, wherein the processor receives the emergency service advertisement in a probe response frame responsive to transmitting a probe request frame.

21. The device of claim 16, further comprising a wireless network interface implemented as one of a secure digital input/output card, a compact flash card, a miniPCI port card, and a PCMCIA card.

22. The device of claim 16, wherein the processor receives an emergency service advertisement in a neighbor report.

23. A device adapted to provide an emergency service in a network, comprising:
a wireless interface;
a memory adapted to store a set of executable instructions; and
a processing unit adapted to receive an association request on the wireless interface, wherein the association request includes an indication of a request for an emergency service, and, responsive to execution of the set of executable instructions, transmit an association response without engaging in an authentication procedure.

24. The device of claim 23, wherein the processing unit transmits an emergency service advertisement that includes an indicator of an emergency service capability.

25. The device of claim 24, wherein the emergency service advertisement comprises an information element that includes the indicator implemented as a bit field.

26. The device of claim 23, wherein the processing unit transmits an emergency service advertisement in a beacon frame.

27. The device of claim 26, wherein the processing unit transmits an emergency service advertisement in a probe response frame responsive to receiving a probe request frame on the wireless interface.

28. The device of claim 26, wherein the memory includes a data structure adapted to associate a station with a virtual local area network, and wherein the processing unit assigns a station that originated the association request to a virtual local area network dedicated to emergency service traffic.

29. The device of claim 23, wherein the processing unit transmits an emergency service advertisement in a neighbor report.

30. The device of claim 23, wherein the processing unit evaluates a station that originated the association request as currently associated and, responsive thereto, deletes a security association of the station.

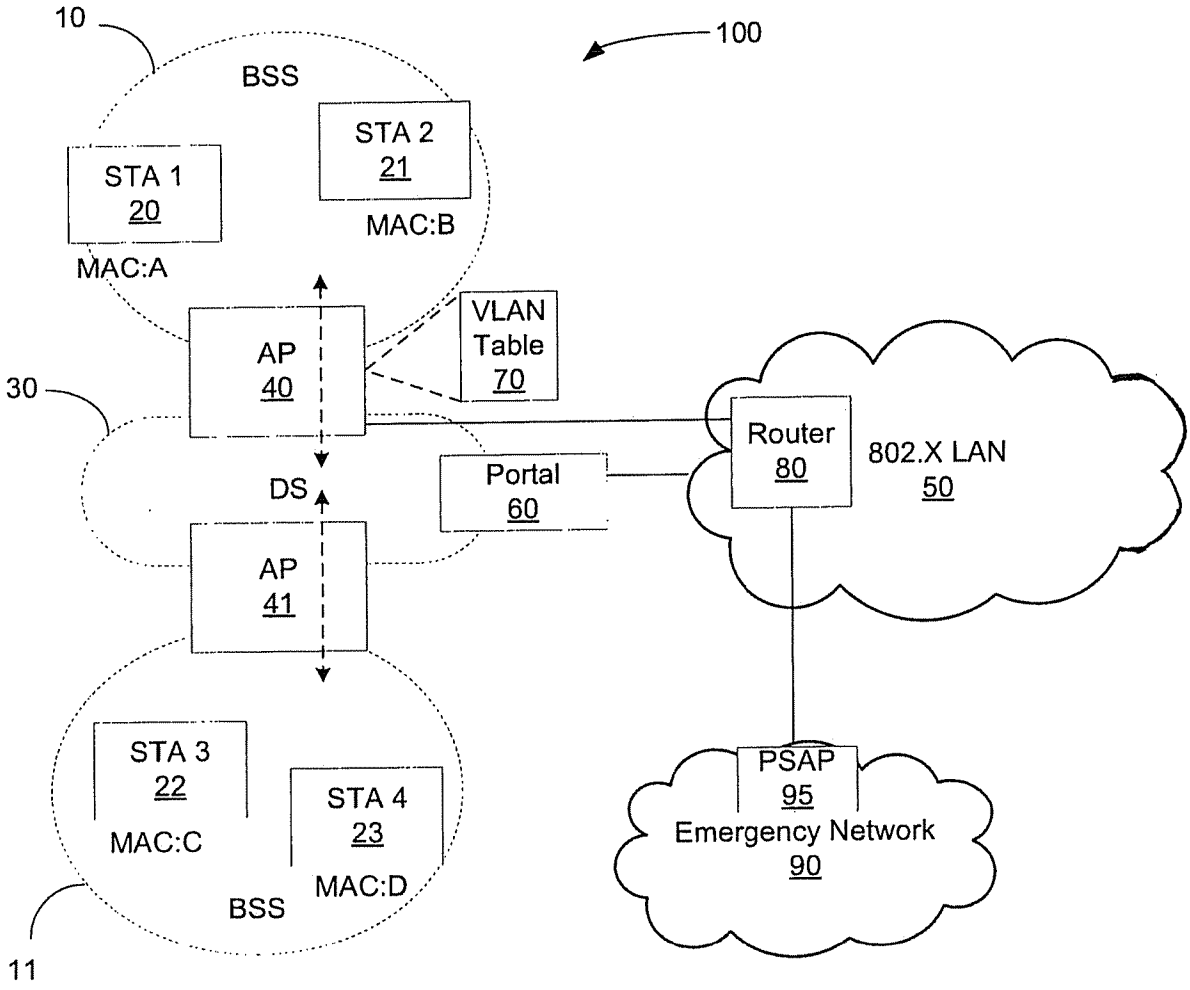

10
100
BSS
STA 2
21
MAC:B
STA 1
20
MAC:A
VLAN
Table
70
AP
40
30
Router
80
802.X LAN
50
DS
Portal
60
AP
41
STA 3
22
MAC:C
STA 4
23
MAC:D
BSS
PSAP
95
Emergency Network
90
11

Figure 1

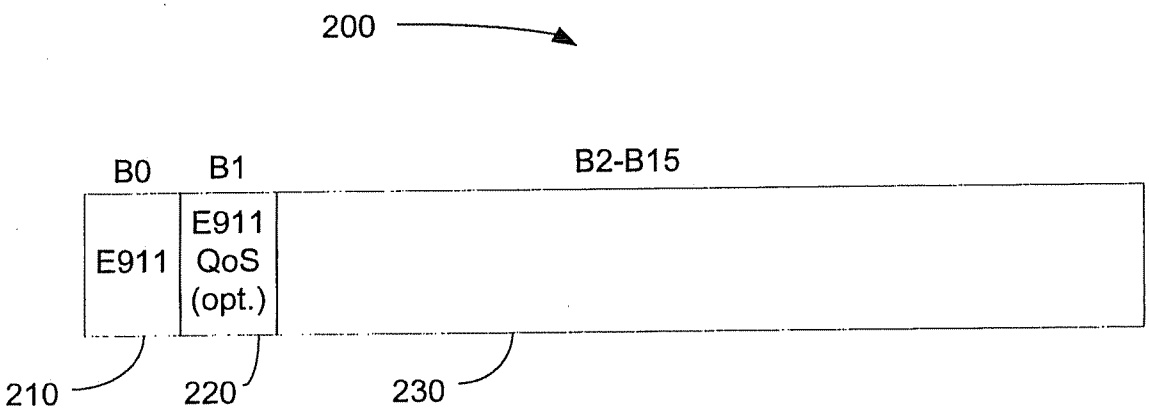


Figure 2

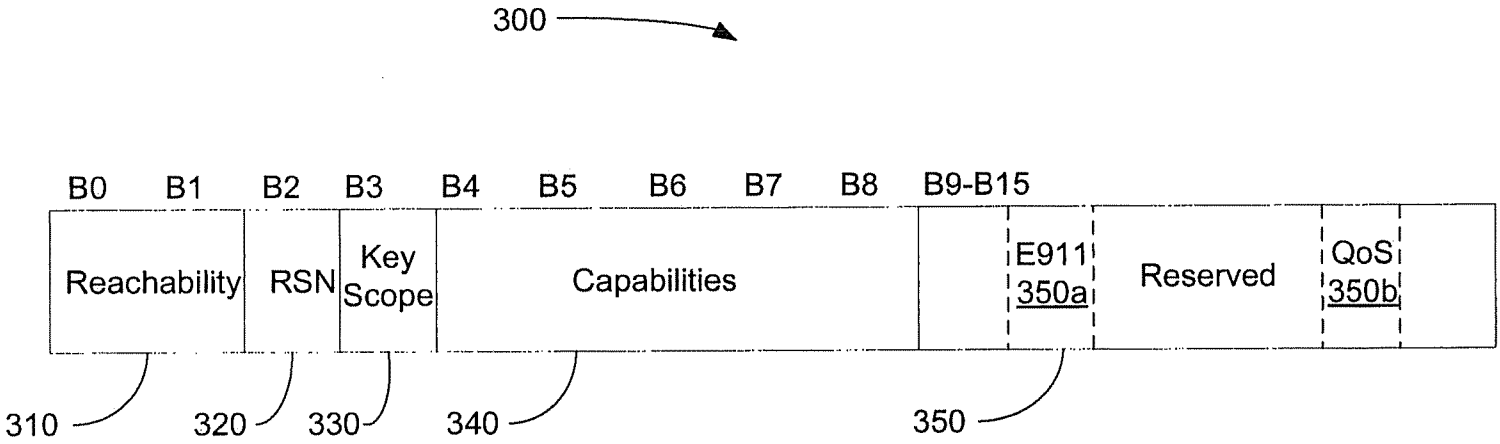


Figure 3

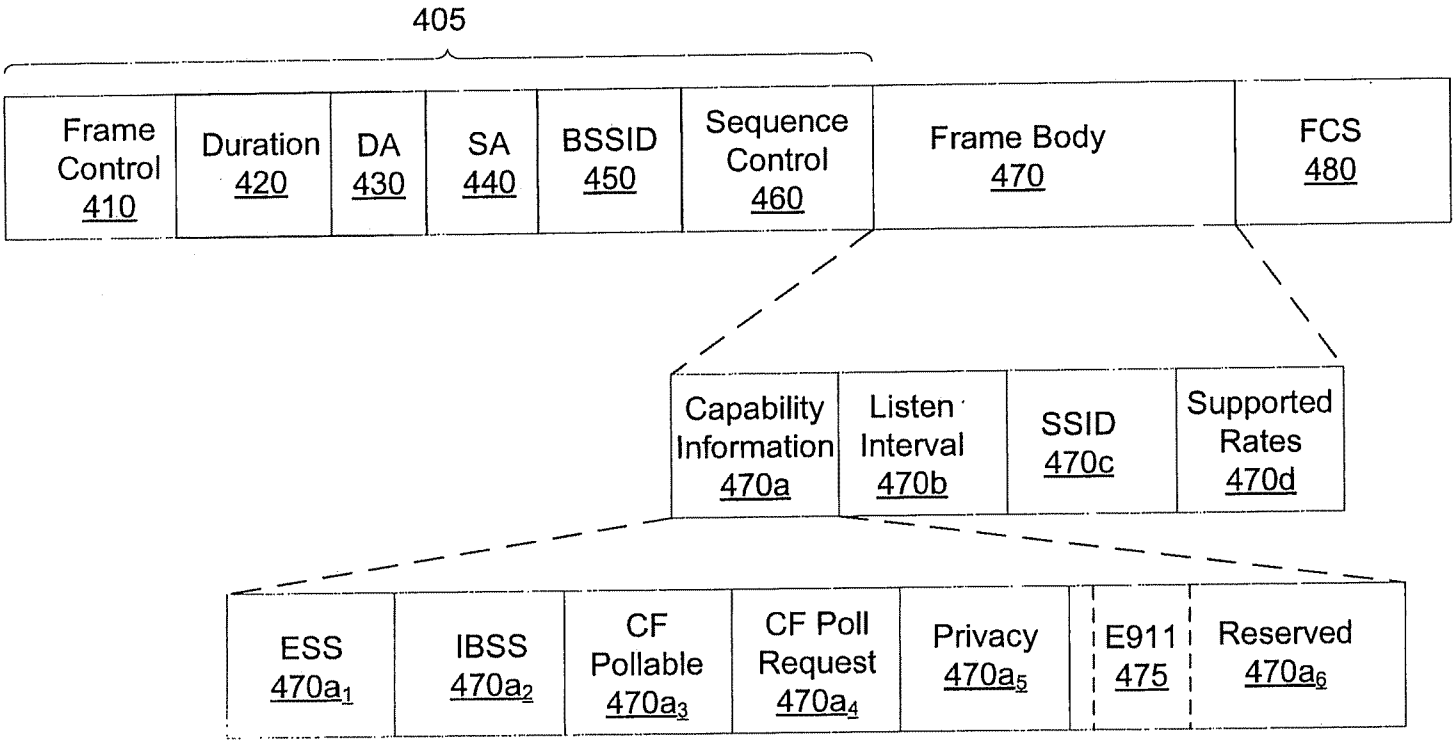


Figure 4

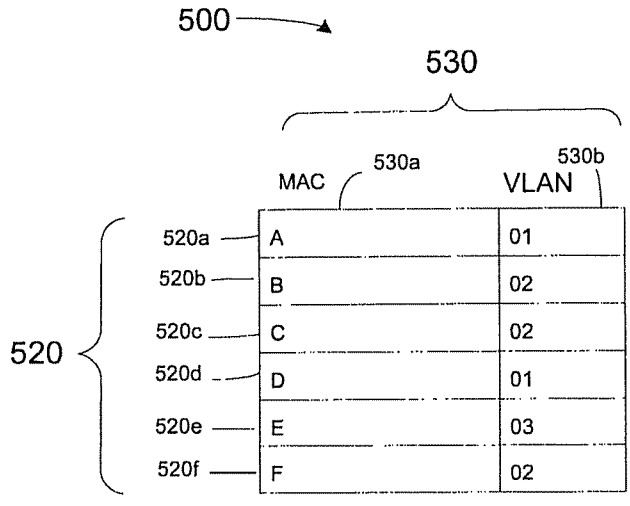


Figure 5

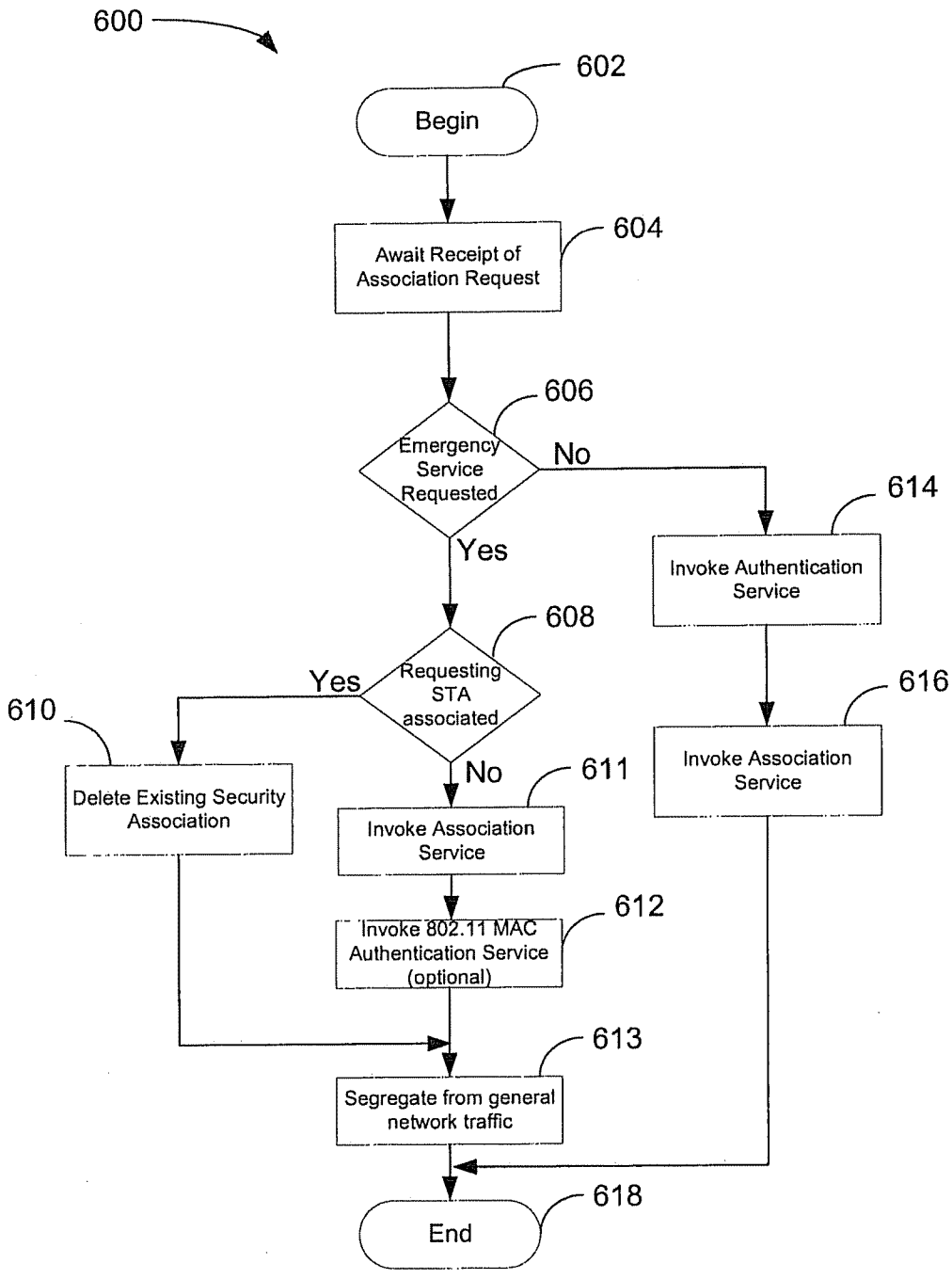

600
602
Begin
604
Await Receipt of Association Request
606
Emergency Service Requested
No
Yes
614
Invoke Authentication Service
608
Requesting STA associated
Yes
No
610
Delete Existing Security Association
611
Invoke Association Service
616
Invoke Association Service
612
Invoke 802.11 MAC Authentication Service (optional)
613
Segregate from general network traffic
618
End

Figure 6

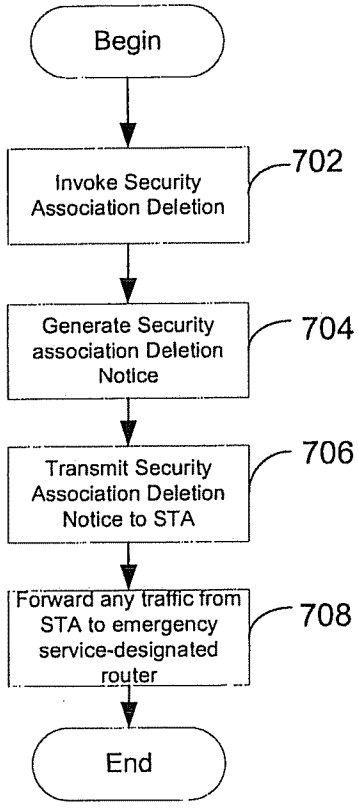

Begin
Invoke Security Association Deletion
702
Generate Security association Deletion Notice
704
Transmit Security Association Deletion Notice to STA
706
Forward any traffic from STA to emergency service-designated router
708
End

Figure 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/060486

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/38

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)
H04Q H04L

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 practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 2005/112488 A (INTERDIGITAL TECH CORP [US]; RUDOLF MARIAN [CA]; RAHMAN SHAMIN ABKAR [) 24 November 2005 (2005-11-24) paragraph [0003] paragraphs [0009] - [0018] paragraphs [0039] - [0045] paragraphs [0054], [0056], [0061] paragraph [0065] paragraphs [0073] - [0081] paragraph [0102]	1-13, 15-27, 29,30 14,28

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 September 2007	08/10/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hegeman, Hans

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/060486

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2004/013986 A (CISCO TECH IND [US]) 12 February 2004 (2004-02-12)	14,28
A	page 1, lines 24-30 page 2, lines 7-13 page 2, lines 25-27 page 3, lines 26-28 page 6, lines 5-11 page 7, lines 15-17	1,7,15, 16,23
P,X	EP 1 653 668 A (CIT ALCATEL [FR]) 3 May 2006 (2006-05-03) paragraphs [0015] - [0019] paragraphs [0024] - [0028]	1-12,14, 16-29
X	MOULY ET AL: "The GSM System for Mobile Communicatons - Communication Management" GSM SYSTEM FOR MOBILE COMMUNICATIONS. COMPREHENSIVE OVERVIEW OF THE EUROPEAN DIGITAL CELLULAR SYSTEMS, ÄS.L.Ü : CELL & SYS, 1992, pages 501-565, XP002103158 ISBN: 2-9507190-0-7 pages 532-533	1,7,16, 23
X	3GPP: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions (Release 7)" 3GPP TS 23.167 V1.0.0 (2005-11), [Online] 12 December 2005 (2005-12-12), XP002452155 Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Specs/archive/23_series/23.167/23167-100.zip> [retrieved on 2007-09-21] page 13, lines 7-29	1,7,16, 23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/060486

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005112488 A	24-11-2005	AR 049271 A1	12-07-2006
		AU 2005242239 A1	24-11-2005
		CA 2565561 A1	24-11-2005
		CN 2834037 Y	01-11-2006
		EP 1747687 A2	31-01-2007
		KR 20060045962 A	17-05-2006
		KR 20060092934 A	23-08-2006
		TW 288740 Y	11-03-2006
WO 2004013986 A	12-02-2004	AU 2003254133 A1	23-02-2004
		CA 2526978 A1	12-02-2004
		EP 1529352 A1	11-05-2005
		US 2005185626 A1	25-08-2005
		US 6950628 B1	27-09-2005
EP 1653668 A	03-05-2006	CN 1770716 A	10-05-2006
		WO 2006045791 A1	04-05-2006
		US 2006088020 A1	27-04-2006