

LOCATION AWARENESS IN WIRELESS NETWORKS

FIELD OF THE INVENTION

The present invention relates generally to location awareness in wireless networks and more particularly to identifying and communicating with proximate wireless stations. The present invention also relates generally to communications between stations in wireless networks
5 and more particularly to establishing wireless direct links between proximate stations.

BACKGROUND OF THE INVENTION

Various wireless standards, such as Institute of Electrical and Electronics Engineers (IEEE) standards 802.11a/b/c/e/g/i (referred to collectively as IEEE 802.11), provide for wireless connectivity between a wireless station and an infrastructure network (e.g., the Internet) via an
10 access point. Processes covered by these standards include the association of a wireless station with an access point, the transmission of data from wireless station to infrastructure network, and vice versa, via the access point, communication between wireless stations via an access point, and the like.

Some wireless standards, such as the direct link protocol (DLP) proposed for inclusion in
15 IEEE 802.11e, provide a technique for initiating direct communications between wireless stations without the access point acting as an intermediary for the forwarding the data frames. The direct communications are commonly referred to as a wireless "direct link." These conventional direct link processes, however, require active cooperation from the access point in initiating and establishing the direct link. It will be appreciated that the access point may be
20 configured to prevent the establishment of a direct link or may be incapable of supporting direct link capabilities (e.g., modulation type) preferred by the wireless stations. Wireless stations using conventional direct link techniques therefore may be unable to establish a direct link or may restricted to establishing and using a direct link with capabilities limited to the supported capabilities of the access point.

25 While providing for the establishment of a direct link in limited instances, conventional wireless techniques fail to provide an adequate technique for identifying nearby wireless stations with which a direct link may be established. Further, conventional wireless standards fail to

provide processes that allow a wireless user to identify nearby users of wireless stations with whom the wireless user may want to meet or converse.

Accordingly, techniques for establishing a direct link independent of an access point and for identifying proximate wireless stations users would be advantageous.

5 **SUMMARY OF THE INVENTION**

The present invention mitigates or solves the above-identified limitations in known solutions, as well as other unspecified deficiencies in known solutions. A number of advantages associated with the present invention are readily evident to those skilled in the art, including economy of design and resources, transparent operation, cost savings, etc.

10 Still further features and advantages of the present invention are identified in the ensuing description, with reference to the drawings identified below.

BRIEF DESCRIPTION OF THE DRAWINGS

15 The purpose and advantages of the present invention will be apparent to those of ordinary skill in the art from the following detailed description in conjunction with the appended drawings in which like reference characters are used to indicate like elements, and in which:

Figure 1 is a top view of an exemplary building having wireless network access provided by a plurality of access points in accordance with at least one embodiment of the present invention.

20 Figure 2 is a schematic diagram illustrating an exemplary wireless station for identifying proximate wireless stations in accordance with at least one embodiment of the present invention.

Figure 3 is a flowchart illustrating an exemplary operation of the wireless station of Figure 2 in accordance with at least one embodiment of the present invention.

25 Figure 4 is a schematic diagram illustrating an exemplary technique for identifying proximate wireless stations using direct polling in accordance with at least one embodiment of the present invention.

Figure 5 is a schematic diagram illustrating an exemplary technique for identifying proximate wireless stations using proximity information maintained by an access point in accordance with at least one embodiment of the present invention.

5 Figure 6 is a schematic diagram illustrating an exemplary technique for identifying proximate wireless stations using proximity information maintained by a proximity server associated with an extended service set (ESS) in accordance with at least one embodiment of the present invention.

10 Figure 7 is a schematic diagram illustrating an exemplary technique for identifying proximate wireless stations using proximity information maintained by a proximity server associated with an infrastructure network in accordance with at least one embodiment of the present invention.

Figures 8, 9 and 10A-10D are block diagrams illustrating various tables of proximity information that may be maintained by a proximity server in accordance with at least one embodiment of the present invention.

15 Figures 11, 12A-12C and are schematic and flow diagrams illustrating an exemplary technique for identifying wireless stations within a transmission/reception range of another wireless station in accordance with at least one embodiment of the present invention.

20 Figure 14 is a schematic diagram illustrating a technique for obtaining one or more user identifications (IDs) associated with a proximate wireless station in accordance with at least one embodiment of the present invention.

Figure 15 is a schematic diagram illustrating an exemplary table of information related to associates of a user of a wireless station in accordance with at least one embodiment of the present invention.

25 Figure 16 is a flow diagram illustrating an exemplary technique for notifying a wireless station user of one or more proximate wireless station users using the table of Figure 15 in accordance with at least one embodiment of the present invention.

Figure 17 is a flow diagram illustrating exemplary techniques for communicating with a proximate wireless station in accordance with at least one embodiment of the present invention.

Figure 18 is a schematic diagram illustrating an independent link protocol (IDL)P technique for establishing a wireless direct link between proximate wireless stations in accordance with at least one embodiment of the present invention.

Figure 19 is a schematic diagram illustrating an exemplary IDLP frame used by the technique of Figure 18 in accordance with at least one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The following description is intended to convey a thorough understanding of the present invention by providing a number of specific embodiments and details involving the identification of, and communication with, proximate wireless stations. It is understood, however, that the present invention is not limited to these specific embodiments and details, which are exemplary only. It is further understood that one possessing ordinary skill in the art, in light of known systems and methods, would appreciate the use of the invention for its intended purposes and benefits in any number of alternative embodiments, depending upon specific design and other needs.

For ease of illustration, the various techniques of the present invention are discussed below in the context of IEEE 802.11-based wireless networking. However, those skilled in the art, using the teachings provided herein, may advantageously implement the disclosed techniques in other wireless networks. Accordingly, reference to techniques and components specific to IEEE 802.11, such as a media access control (MAC) addresses, applies also to the equivalent technique or component in other wireless network standards unless otherwise noted.

Referring now to Figure 1, an exemplary implementation of one or more techniques is illustrated in accordance with at least one embodiment of the present invention. Figure 1 depicts a top view 100 of a building, where the building may include any of a variety of structures, such as, for example, an airport, a shopping mall, a factory, a business office, a school campus, a residence, and the like. Situated at various points within the buildings interior are a plurality of access points 102-118 (illustrated as AP 1-AP 9, respectively) having coverage areas 122-138, respectively. The access points 102-118 typically are connected via a backbone network (not illustrated) to form one or more extended service sets (ESSs). The backbone network in turn

typically is connected to an infrastructure network, such as, for example, a wide area network (WAN), metropolitan area network (MAN), the Internet, etc. Thus, wireless network access to the infrastructure network may be provided to one or more wireless stations 140-172 (illustrated as S₁-S₁₇, respectively) that are positioned within one or more of the coverage areas 122-138.

5 The wireless stations 140-172 include devices enabled to communicate wirelessly using one or more protocols supported by one or more the access points 102-118. Such protocols may include, for example, the IEEE 802.11 protocols (802.11a/b/e/g/i, etc. Examples of wireless-enabled devices may include notebook (or "laptop") computers, handheld computers, desktop computers, workstations, servers, portable digital assistants (PDAs), cellular phones, etc.

10 In conventional wireless applications, a wireless station typically is unaware of the position or proximity of wireless stations and is further unaware of the one or more user IDs associated with the users of nearby wireless stations. In many instances, however, a user of a wireless station may desire to receive notification of other users of proximate wireless stations. Particularly, a certain user may want to be notified of other users with whom the certain user has
15 some sort of association (i.e., "associates" of the certain user). Accordingly, in one embodiment of the present invention, one or more of the wireless stations 140-172 may be adapted to identify proximate wireless devices and determine one or more user IDs associated with the user or users of the proximate wireless devices. A user's ID may include, for example, a login ID supplied by the user to enable the user's use of the wireless station, an email address associated with the user
20 and used by an email client operating on the wireless station, a user ID associated with one or more software programs operating on the wireless station, such as an instant messenger client, and the like.

 After determining the user ID(s) associated with a nearby station, the wireless station may automatically notify the user of the wireless station. Alternatively, in one embodiment, a
25 filtering process may be performed to determine whether the user should be notified of a proximate station user. The filtering process may include, for example, comparing the user ID with a list of associate user IDs or applying one or more notification filter rules that govern the notification process. Examples of notification filter rules may include rules that prevent or allow

notification of proximate users during certain time periods, at certain locations, or in other situations. Exemplary filtering processes are discussed in greater detail herein.

5 The user of the wireless station may be notified of proximate users in a variety of manners. For example, a pop-up window could be displayed on a display screen of the station that informs the user of the proximity of the identified proximate user and also may provide additional related information, such as, for example, a value representing the degree of proximity (e.g., a physical distance value). The pop-up window could be displayed in conjunction with a communications program operating on the wireless station, such as an email client or an instant messaging program. Notification also may be provided by, for example, automated speech
10 output by a speaker of the station, transmitting an email to an email client operating on the wireless station, etc.

After receiving notification of proximate users or associates, a user may take any of a variety of actions, such as initiating communications with a proximate user via their respective wireless stations, attempting to locate the proximate user for a face-to-face meeting, etc.
15 Communications between nearby wireless stations may be accomplished via conventional wireless techniques where data communications between two wireless stations are communicated via one or more access points and/or the backbone network. Alternatively, in one embodiment, if the nearby wireless stations are within each other's transmission range, a wireless direct link may be established between the nearby wireless stations whereby data is
20 communicated directly between the wireless stations without assistance or interference from an access point.

After establishing a direct link with the proximate station, various types of information may be transmitted over the direct link. For example, the proximate users could establish an instant messaging session using the direct link, transmit email directly without routing the emails
25 through the infrastructure network, conduct a videoconference over the direct link, and the like. As another example, if one station belongs to a business and the other station to a potential customer, the direct link formed between the stations could be used to send advertisements, promotionals, coupons, and the like, from the business to the potential customer. Thus,

advertising could be targeted by the business to potential customers that are within a certain proximity of the business.

As described above, a user of a wireless station may be interested in learning of other users of wireless stations within a certain proximity. The proximity may be defined by the user, an access point, or a third party based at least in part on equipment capabilities and the desires of the user and/or administrator of the wireless network. Various exemplary definitions of proximity are described in the following using Figure 1 for illustrative purposes. For ease of reference, the one or more conditions that define a proximity in a particular instance are collectively referred to herein as a proximity definition.

In at least one embodiment, wireless stations associated with a same access point (i.e., in a same basic service set or BSS) may be classified as proximate to each other. For example, the user of wireless station 144 may want be notified only of those wireless stations that are in the same coverage area 128 of access point 108 to which wireless station 144 is associated. In this case, wireless stations 146 and 148 may be considered as proximate to wireless station 144. In another embodiment, a user of certain wireless station may consider only those wireless stations that are associated with the same access point or another access point having a coverage area that overlaps or is immediately adjacent to the coverage area of the access point associated with the certain wireless station. For example, under this classification of proximity, wireless stations 156, 158 and 170 may be considered proximate to wireless station 160 because the access points 114, 118 associated with one or more of the wireless stations 156, 158 and 170 have coverage areas 134 and 138, respectively, which overlap or are immediately adjacent to coverage area 136 of access point 116. Further, in one embodiment, wireless stations may be considered proximate when they are associated with the same ESS. To illustrate, assume that access points 102-108 form an ESS that spans rooms A and B. In this case, wireless stations 140-150 and 172 may be considered proximate to each other as each is associated with an access point that is a member of the same ESS.

As described above, a proximity definition may be based at least in part on the physical proximity or logical proximity of the access points to which the wireless stations are associated.

In other circumstances, however, a proximity definition may be substantially based on the physical proximity, or physical distance, between wireless stations. In one embodiment, proximity may be defined as a physical distance from a certain wireless station. For example, the user of the wireless station 152 may consider only those wireless stations within an area 180 described by a radius 182 as proximate wireless stations. Under this exemplary proximity definition, wireless stations 150, 154 and 166 would be proximate wireless stations while wireless station 156 would not even though it is associated with the same access point 112 as the wireless station 152. The dimensions of the proximate area may be defined in part by features of the area where the wireless station is located (e.g., the walls or ceiling), by the transmission/reception range of the wireless station (e.g., radius 182 may represent the maximum transmission range), or by the coverage areas of nearby access points.

Rather than, or in addition to, basing proximity on a distance from the wireless station, features of the room or building where the wireless station is located may be used to aid in defining proximity. For example, the contours of room A may set the boundary for an area considered proximate by a user of a wireless station located in room A. In another example, the wireless stations located in either room A or room B may be considered proximate to each other because rooms A and B are adjacent and wireless stations in either room B or room C may be considered proximate to each other because Rooms B and C are adjacent. Wireless stations in room A, however, may not be considered proximate to wireless stations in room C, and vice versa, in this example because the areas of room A and C are not adjacent.

In other embodiments, proximity may be defined based on both physical proximity of the wireless stations and the proximity of access points. For example, wireless stations may be considered to be proximate when they are located in the same room and are associated with the same ESS or are associated with access points having overlapping or adjacent coverage areas. Although various exemplary proximity definitions have been disclosed, other definitions of proximity may be utilized based on the teachings provided herein without departing from the spirit or the scope of the present invention.

Referring now to Figures 2 and 3, an exemplary wireless station 202 for implementing the various techniques described herein and an exemplary method 300 for its use are illustrated in accordance with at least one embodiment of the present invention. The wireless station 202 includes a radio frequency (RF) transceiver 204, one or more processors 206, a proximity
5 identification module 208, a notification module 210 and a link module 212. The wireless station 202 further may include one or more software applications 214, 216. The software applications 214, 216 may include, for example, communications based applications such as an email client, an instant messaging client, videoconferencing software, and the like. The wireless station 202 further may include a global positioning system (GPS) receiver 218 for determining
10 the position of the wireless station 202.

In at least one embodiment, data and other signaling is communicated between the wireless device 202 and one or more access points 220 or other wireless stations 222, 224 as frames represented by RF energy transmitted by and received via the RF transceiver 204. Incoming data from the RF transceiver 204 may be processed by the processor 206 using one or
15 more protocol stacks 226, such as, for example, an Internet Protocol (IP) stack. The resulting extracted data may be used by the proximity identification module 208, the notification module 210, the link module 212 and/or one or more of the software applications 214, 216 as described herein. Similarly, data generated by one or more of the modules 208-212 and/or software applications 214, 216 may be encapsulated or otherwise processed by the processor 206 using
20 the one or more protocol stacks 226 and transmitted to the access point 220 or wireless stations 222, 224 via the transceiver 204.

In at least one embodiment, the modules 208-210 are at least partially implemented as software executed by one or more processors 206 to perform the associated function. In other embodiments, some or all of the modules 208-210 may be implemented as hardware, firmware,
25 or a combination thereof. For example, the modules 208-212 may be implemented as a software application installed on and executed by the wireless station 202 to perform the proximity detection, notification, and link establishment techniques described herein. Alternatively, the modules 208-212 may be implemented as software "plug-ins" for implementation in conjunction with another software application, such as an email client application.

Referring to Figure 3, an exemplary method 300 illustrating an operation of the wireless station 202 is illustrated. The method 300 initiates at step 302 wherein the proximity identification module 208 identifies wireless stations proximate the wireless station 202 under one or more proximity definitions. In one embodiment, the proximity identification module 208 identifies proximate wireless stations using a direct polling approach as described with reference to Figure 4. In another embodiment, the proximity identification module 208 identifies proximate wireless stations based at least in part on proximity information provided by the access point 220 or a proximity server implemented by, or connected to, the access point 220 as described with reference to Figures 6-10D. Alternatively, the proximity identification module 208 may identify proximate wireless stations using an automatic peer discovery technique as described with reference to Figures 12-14B. Other techniques for identifying proximate wireless stations may be implemented without departing from the spirit or the scope of the present invention.

At step 304, the proximity identification module 208 determines one or more user IDs associated with the identified proximate wireless stations. A user ID may include, for example, a login ID used to access the wireless station, an email address associated with a user of the wireless station, a user ID provided by the user in response to a request for identification, a user ID provided specifically for proximate identification purposes, etc. In one embodiment, the user ID of the user of a proximate wireless station may be received by the proximity identification module 208 as data transmitted by the proximate wireless station in response to a identification request transmitted by the proximity identification module 208. Alternatively, the user ID of a user of a proximate wireless station may be provided by the proximity server or the access point 220.

As noted above, in some instances the user of the wireless station 202 may want to be notified of a proximate station user only under certain conditions. For example, one condition may be that the proximate station user be associated in some way with the user of the wireless station 202, i.e., the proximate station user is an associate of the user of the wireless station 202. An associate may include, for example, a family member, a friend, a co-worker, a business associate, a fellow club member, etc. Accordingly, at step 306, the user IDs of proximate

wireless stations may be compared to a list of user IDs related to identified associates of the user of the wireless station 202. In the event that the user ID of a proximate wireless station substantially matches a user ID on the list of associate IDs, the proximity identification module 208 may identify the user of the proximate wireless station as an associate. In other
5 embodiments, however, the user of the wireless device 202 may opt to receive notification of proximate users regardless of an association, or lack thereof, with the user of the wireless device 202. In this case, step 306 may be omitted.

At step 308, the notification module 210 notifies the user of the wireless station 202 of the proximity of nearby station users. The notification module 210 may notify the user by, for
10 example, displaying a display window having proximate user information on a display screen of the wireless station 202 for observation by the user, by playing an automated voice output identifying proximate users, by sending an email to an email client operating on the wireless station 202, etc.

In certain instances, however the notification module 210 performs a filtering process
15 before notifying the user of proximate users. The filtering process may include subjecting the user IDs associated with the proximate wireless stations to one or more notification filter rules set by the user of wireless station 202. The one or more notification filter rules may include, for example, conditions relating to the time of notification, the place of notification, the means of notification, and the like. For example, the wireless station 202 may include a notebook
20 computer and the user of the wireless station may work at an office with other workers having similarly configured notebook computers. The user therefore may not desire to receive notification of the proximity of associates at the office due to user's preexisting awareness that the other workers are proximate due to their co-employment at the same office. Accordingly, the user may set a notification filter rule whereby no notification is given for proximate users
25 identified as coworkers when the wireless station 202 is within the confines of the user's office.

After notifying the user of proximate users, the user may be provided with the choice of whether to initiate a direct link with one or more proximate wireless stations. If the user does not want to establish a direct link, the user may so indicate at step 310 and the method 300

terminates at end step 312. Otherwise, the user may select one or more proximate users with whom the link module 212 may attempt to establish a direct link.

At step 314, the link module 212 may initiate the one or more direct link techniques to establish a direct link with the wireless station(s) of the selected proximate user(s). Any of a variety of techniques may be used to establish a direct link, two of which are discussed with reference to Figures 17-19. After a direct link is established at step 316, the user may communicate with the proximate user, and vice versa, via the direct link at step 318. Such communications may include instant messaging, direct email, video conferencing, etc.

Referring now to Figure 4, an exemplary direct polling technique 400 for identifying proximate wireless stations is illustrated in accordance with at least one embodiment of the present invention. In the illustrated example, the proximity identification module 208 of station 202 generates and provides for transmission a poll frame 402 having a broadcast or multicast MAC address in its destination address field. The poll frame 402 further may include, for example, data identifying the frame as a request for wireless devices to identify themselves upon receipt of the poll frame 402. In this case, the proximate wireless stations 222, 224 may prepare and transmit poll response frames 404 and 406, respectively, for receipt by the wireless station 202. The poll response frames 404 and 406 may include, for example, data representing the MAC address of the proximate wireless station sending the poll response frame, an indicator of the type of wireless station (e.g., PDA, notebook computer, cell phone, etc.), one or more user IDs associated with the wireless station, and the like.

It will be appreciated that the receipt of a poll response frame from a wireless station indicates a strong possibility that the wireless station is nearby. Based on this possibility, upon receipt of a broadcast response frame, the proximity identification module 208 may insert relevant data from the poll response frame into a response table 408 maintained at the wireless station 202. In other embodiments, rather than transmitting a poll response frame in response to a poll frame 402, the wireless stations 202, 222, and 224 may be adapted to periodically transmit a beacon frame, similar to the poll response frames 404 and 406, identifying the MAC address, type, user ID, etc., of the wireless station transmitting the beacon frame. Upon receipt of a

beacon frame from another wireless station, the receiving wireless station may add information from the beacon frame to the response table 208.

In the illustrated example, the response table 408 includes an entry for each broadcast response frame received, the entry including the MAC address (column 410), type (column 412) and user ID (column 414) associated with the wireless station transmitting the response frame. Information from the response table 408 therefore may be used by the proximity identification module 408 and notification module 410 to identify proximate station users and to provide notification of their proximity.

Referring now to Figure 5, an exemplary technique for identifying proximate wireless stations based on proximity information provided an access point is illustrated in accordance with at least one embodiment of the present invention. IEEE 802.11 and other wireless standards describe an association process whereby a wireless station that enters the coverage area of an access point may identify itself to the access point and request that the access point handle incoming and outgoing frames on behalf of the wireless station. In at least one embodiment, the access point and wireless device may be adapted to provide proximity information during or in response to the association process.

To illustrate, the access point 502 may be adapted to maintain an association table 504 that stores information relating to wireless stations associated with the access point 502. This information may include, for example, the MAC address of the wireless station, the type of wireless station, user ID(s) associated with the wireless station, etc.

When wireless device 506 enters the coverage area of the access point 502 (already associated with wireless stations 508 and 510), the wireless station 506 may transmit an association request frame 512 to the access point 502 requesting association with the access point 502. Information related to the wireless device 506 may be transmitted as part of the association request 512 or in subsequent frame(s). Upon receipt of the frame(s) containing information related to wireless station 506, the access point 502 may use this information to create an entry 514 in the associates table 504 for the wireless station 506.

As described in IEEE 802.11, the access point 502 conventionally responds to an association request frame 512 with an association response frame 516 indicating whether the association request of the wireless station 202 is successful, and if so, the association response frame 516 also generally includes an association ID for use by the wireless station 506. In one embodiment; the access point 502 may further respond to a successful association request by transmitting a proximity listing 518 to the wireless station 506 as part of the association response frame 516 or as one or more separate frames. The proximity listing 518 preferably includes information related to other wireless stations 506 and 508 associated with the access point 502, such as, for example, the proximate stations' MAC addresses, user IDs, type, GPS position, etc. The information presented in the proximity listing 518 may be culled from the associates table 504 maintained by the access point 502. The proximity identification module 208 may store part or all of the information of the proximity listing 518 in the response table 408 or similar table for use in identifying and providing notification of proximate users.

Referring now to Figure 6, an exemplary system 600 and technique for providing proximity information in an ESS is illustrated in accordance with at least one embodiment of the present invention. System 600 includes a backbone network 602 connecting a plurality of access points 604-610 to form an ESS. The backbone network 602 is further connected to an infrastructure network 612 (e.g., the Internet) to provide network connectivity between wireless stations 614-624 and the infrastructure network 612.

The system 600 further includes a proximity server 630 operably connected to the access points 604-610 via the backbone network 602. In at least one embodiment, the notification server 630 may be adapted to monitor the physical and/or logical locations of wireless stations associated with the ESS. To facilitate this monitoring process, the proximity server 630 may be adapted to maintain, or have access to, a proximity database 632 storing various information related to the locations, positions, identities, types, connection capabilities, etc. of the wireless stations 614-624. Various examples of information that may be stored in the proximity database 632 are discussed below with reference to Figures 8, 9, and 10A-D.

Information stored in the proximity database 632 may be provided directly by the wireless stations 614-634, provided by the access points 604-610, or the proximity database 632 may obtain information from other sources. To illustrate, when a wireless station associates with one of the access points 604-610, the access point may obtain information related to the workstation as described with reference to Figure 5 and provide this information to the proximity server 630. Alternatively, the address of the proximity server 630 may be provided to the wireless station during, for example, the association process and the wireless station may provide the proximity server with the information directly.

To receive information from the proximity server 630 identifying proximate wireless stations, a wireless station (e.g., wireless station 620) may be adapted to transmit a proximity request 640 to the proximity server 630. In instances where the address of the proximity server 630 is known to the wireless station 620, the wireless station 620 may transmit the proximity request 640 directly to the proximity server 630 via the access point 608. In instances where the wireless station 620 is unaware of the proximity server 630, the wireless station 620 may transmit the proximity request 640 for receipt by the access point 608. The access point 608, knowing the address of the proximity server 630, then may forward the proximity request 640 to the proximity server 630.

The proximity request 640 may include various information useful to the proximity server 630 in identifying proximate stations and providing their relevant information. The information in the proximity request 640 may include, for example, information associated with the wireless station 620 such as its MAC address, one or more user IDs, a BSSID, position coordinates provided by the GPS receiver 218 (Figure 2), etc. The information in the proximity request 640, in one embodiment, may also include a desired proximity definition, such as a maximum proximity radius, a limitation to a same room, BSS, set of BSSs, etc.

Using the information of the proximity request 640 and the proximity database 632, the proximity server 630 may identify proximate stations using a default proximity definition or a proximity definition provided by the wireless device 620. After identifying proximate stations, the proximity server 630 may identify information in the proximity database 632 corresponding

to the identified proximate stations and provide some or all of this information to the wireless station 620 as a proximity listing 642. The proximity identification module 208 (Figure 2) of the wireless station 620 may process the information of the proximity listing 642 as appropriate and provide relevant portions to the notification module 210 (Figure 2) for use in notifying the user of the wireless station 620 of nearby wireless station users.

Referring now to Figure 7, an exemplary system 700 and technique for providing proximity information for multiple ESSs are illustrated in accordance with at least one embodiment of the present invention. System 700 includes the backbone network 602 connecting a plurality of access points 604-610 to form an ESS. The backbone network 602 is further connected to the infrastructure network 612 (e.g., the Internet) to provide network connectivity between wireless stations 614-624 and the infrastructure network 612. The infrastructure network 612 is further connected to one or more other ESSs, such as ESS 702 having access points 706, 708 and ESS 710 having access points 712, 714.

System 600 of Figure 6 depicts a system whereby proximity information may be provided to a wireless station in an ESS by a proximity server 630 that is associated with the ESS. In certain instances, it may be advantageous to maintain a proximity server 720 capable of providing proximity information for a plurality of ESSs. For example, as noted above, multiple ESSs may be present in a building. In this case, a useful proximity definition may span multiple ESSs. Accordingly, the proximity station 720 may be adapted to maintain a proximity database 722 (analogous to proximity database 632, Figure 6) for the wireless stations associated with multiple ESSs. The station-related information populating the proximity database 722 may be provided by, for example, the access points 604-610, 706, 708, 712 and 714 when a wireless station associates with one of the access points. Examples of information maintained in the proximity database 722 are discussed with reference to Figures 8, 9 and 10A-10D.

To obtain proximity information, the wireless station 620 can transmit a proximity request 740 (analogous to proximity request 640, Figure 6) to the proximity server 720. The proximity request 740 may include a proximity definition that provides, for example, a definition of proximity that spans multiple ESSs. In response to the proximity request 740, the proximity

server 722 may identify proximate wireless stations using proximity database 722 and provide information relevant to identified proximate wireless stations as proximity listing 742 (analogous to proximity listing 642, Figure 6) for use by the wireless device 620.

Referring now to Figures 8, 9 and 10A-10D, examples of information maintained in proximity databases 632 (Figure 6) or proximity database 722 (Figure 7) are illustrated in accordance with at least one embodiment of the present invention.

Figure 8 illustrates an exemplary table 800 whereby information related to wireless stations (e.g., stations 614-624, Figure 6) of an ESS may be stored by, for example, MAC address of the wireless stations (column 802), MAC address of the access point associated with the corresponding wireless station (column 804), the device type (column 806), and one or more user IDs associated with the corresponding work station (column 808).

As noted above, proximity may be limited to a BSS or a group of adjacent BSSs. Under this proximity definition, the proximity server 630/720 may identify a wireless stations proximate to a certain wireless station by identifying entries in the table 800 having an AP MAC address (or BSSID) common to the certain wireless station. To illustrate, to identify stations proximate to the wireless station having MAC address MAC 4, the proximity server 630/720 can analyze the table 800 to identify other wireless stations associated with the same access point identified by MAC address AP MAC 3. In the illustrated example, the proximate wireless station would include the station having MAC address MAC 5. The proximity server 630/72 then may select information associated with the identified proximate stations, such as the device type (column 806) and the user ID(s) (column 808).

In certain instances, proximity may be defined as wireless stations within the same ESS as a certain wireless device. Accordingly, Figure 9 illustrates an exemplary table 900 organized by ESS (column 902) and then classified by access point (column) 904 and subclassified by wireless station (column 906). Using table 900, the proximity server 630/720 may identify wireless stations in a same BSS or, alternatively, in the same ESS for proximity identification purposes.

Figures 10A and 10B illustrate exemplary tables 1000 and 1010, respectively, that may be used by the proximity server 630/720 to identify proximate workstations when proximity is based at least in part on the relation of wireless stations to the topography of an area or the room boundaries of a building. Table 1000 of Figure 10A illustrates a table whereby access points
5 (columns 1002) are organized based on the room (column 1006) in which the access points are located. Table 1000 may include additional information related to the access points, such as their MAC addresses (column 1006), their position coordinates (not shown), etc. In instances where proximity is limited to the same room, enclosure or area as a certain wireless station, the proximity server 630/720 may use table 1000 to identify access points located in the same room
10 and consequently identify wireless stations in the same room based on their association with an access point in that room.

In other instances, proximity may be limited to adjacent rooms. Figure 10B illustrates an exemplary table 1010 that may be used by the proximity server 630/720 to identify adjacent rooms. The table 1010 may include, for example, columns 1012 and 1014 listing possible
15 pairings of rooms and column 1016 listing a proximity value (column 1016) used to identify the degree of proximity between the pair of rooms. For example, referring to Figure 1, room A is adjacent to room B and room B is adjacent to room C, so the pairings (room A, room B) and (room B, room C) may be assigned a proximity value of 1 to identify them as immediately adjacent. However, room A and room C are only connected via room B, so the pairing (room A,
20 room C) may be assigned a proximity value of 2 to identify that they are indirectly connected by a third room (room B).

Rather than identifying wireless stations as being located in a certain room based on their association with a particular access point, position coordinates of the wireless stations may be used to identify their location within a building and, therefore, their proximity to a certain
25 wireless device. To illustrate, exemplary table 1020 of Figure 10C lists wireless stations by an identifier, such as a MAC address (column 1022), and the corresponding position coordinates (e.g., latitude X_k , longitude Y_j) of the wireless stations (column 1024). The position coordinates for a wireless station may be supplied by the GPS receiver 218 (Figure 2) of the wireless station. To illustrate, the proximity identification module 208 (Figure 2) may be adapted to transmit the

position coordinates supplied by the GPS receiver to the access point or proximity server on a periodic basis or in response to a poll transmitted by the access point. In other embodiments, the position of the wireless station may be determined one or a plurality of access points using well known wireless triangulation methods.

5 Using table 1020, the proximity server 630/720 may identify wireless stations occurring within a certain proximity of another wireless station, where the proximity may be defined as, for example, an area occurring within a certain radius of the wireless station. If proximity is defined as, for example, the confines of a particular room or building, the proximity server 630/720 may use exemplary table 1030 of Figure 10D to identify proximate wireless stations based on their
10 position. In the illustrated example, table 1030 includes one or more entries having an identifier (column 1032) identifying a certain room, area or building and a boundary description (column 1034) describing the boundaries of the room, area or building using for example, the position coordinates of certain features of the boundaries (e.g., corners of a room). Accordingly, the proximity server 630/720 may identify wireless stations within a certain room, area or building
15 by identifying those wireless stations having position coordinates that fall within the described boundary for the room/area/building.

 In addition to receiving location-related information from the wireless stations and/or access points, the proximity server 630/720 could be adapted to obtain location-related information by performing an Internet Protocol (IP) traceroute. The resulting traceroute
20 information typically provides information about the networks between the wireless station and the proximity server (or other Internet host). The traceroute path provides value in two ways. First, it can provide an indication of relative degree of “closeness.” If two users are connected to the same service provider, but not on the same local subnet, they might share a common router on the path back to the central server. An example might be two users in different terminals at an
25 airport equipped with a wireless LAN infrastructure. A common network router in a traceroute path does not guarantee physical proximity, but there frequently is a correlation due to the way networks are deployed and the way blocks of IP addresses are often assigned. The proximity server 630/720 may report the possible proximity back to both users. The second value of the traceroute function is to prevent “false positive” proximity indications due to the common use of

network address translation (NAT) in wireless access areas. Where low-cost wireless routers are use, there is a very high probability that a wireless user will be issued an IP address of the form 192.168.0.X. This private address space provides no location information. However, the traceroute can identify the next router in the path and identify a public IP address that the router is connecting to the Internet with and, therefore, additional location information can be derived. Furthermore, third party services are available that provide location information for most IP addresses on the Internet.

Referring now to Figure 11, 12A-12C and 13A-13B, an exemplary automatic discovery technique for identifying proximate wireless stations is illustrated in accordance with at least one embodiment of the present invention. Rather than relying on proximity information from a proximity server or an access point, the proximity identification module 208 (Figure 2) of a wireless station may be adapted to identify proximate wireless stations directly by monitoring frames transmitted by wireless stations within a transmission/reception area of the wireless station. In this instance, the proximity may be defined, for example, as those wireless stations within transmission/reception range.

To illustrate with reference to Figure 11, a plurality of wireless devices 1102-1110 may be located within one of coverage areas 1112 and 1114 of access points 1116 and 1118, respectively. By monitoring frames transmitted by or to wireless stations within a transmission/reception range 1120 (defining transmission/reception area 1122), the wireless station 1106 may identify proximate stations within its transmission/reception range, i.e., wireless stations 1104, 1108, using the automatic discovery technique described below.

As provided by IEEE 802.11 and related standards, frames typically contain several address fields inside the MAC header, depending on their type (control, data, or management). The first address field, denoted herein as address field A1, indicates the MAC address of the immediate receiver of the frame. The second address field, denoted herein as address field A2, contains the MAC address of the transmitter of the frame. The third address field, denoted herein as address field A3, contains either the MAC address of the ultimate source of the frame (for downlink frames), the MAC address of the ultimate destination (for uplink frames), or the

BSSID (for direct link and ad hoc frames). Acknowledgement (ACK) frames typically only have address field A1. Therefore, it will be appreciated that three types of frames may exist within the transmission/reception range of a wireless station: 1) a frame intended for receipt by the wireless station (e.g., a frame having the MAC address of the wireless station as its destination address), referred to herein as a “receipt intended frame”; 2) a frame overheard by the wireless station but intended for receipt by another wireless station (e.g., a frame having a MAC address of another wireless station as its destination address), referred to herein as an “overheard frame”; and 3) a frame transmitted by the wireless station for receipt by another station (e.g., a frame having the MAC address of the certain wireless station as the source address), referred to herein as an “originating frame.”

Figures 12A-12C illustrate various exemplary methods 1200A, 1200B and 1200C for monitoring frames transmitted within the transmission/reception range of a wireless station (e.g., wireless station 1106) to identify potential proximate stations using the address fields A1, A2 and A3 of the frames. Exemplary method 1200A describes a method for monitoring overheard frames, exemplary method 1200B describes a method for monitoring receipt intended frames and exemplary method 1200C describes a method for monitoring originating frames.

Method 1200A initiates at step 1202 wherein the wireless station 1106 overhears a frame transmitted by another station. The proximity identification module 208 (Figure 2) may identify the frame as an overheard frame by, for example, noting that the MAC address in address field A1 does not match the MAC address of the wireless station 1106. At step 1204, the MAC address stored in address field A1 of the frame is stored in peer list 1 (PL1) maintained by the proximity identification module 208. At step 1206, the MAC address stored in address field A2 is stored in a peer list 2 (PL2) maintained by proximity identification module 208. Method 1200B initiates at step 1208 when a the wireless station 1106 receives a receipt intended frame, i.e., a frame having the wireless station 1106 as the ultimate destination. The proximity identification module 208 may identify the frame as such by noting that the MAC address in address field A3 matches the MAC address of the wireless station 1106. At step 1210, the MAC address in address field A3 is stored in a peer list 3 (PL3) maintained by proximity identification module 208. Method 1200C initiates at step 1212 when the wireless station 1106 transmits a

frame. At step 1214, the proximity notification module 208 stores the MAC address of address field A3 of the transmitted frame in PL3.

In methods 1200A-1200C, filtering of frames that contain a BSSID, multicast address or broadcast address preferably is performed to prevent the storage of such in PL1, PL2 or PL3.

5 Furthermore, PL1, PL2 and PL3 preferably are aged or periodically refreshed to maintain the accuracy of the lists. PL1 and PL2 may be pre-populated when stations periodically transmit a null frame at a low PHY rate; a station's own MAC address stored in address fields A1 and A2 (i.e. Null-to-self). The peer lists may also be pre-populated when other stations join and authentication or association request/response frames are received. Address information from
10 probe request/response frames preferably is not added to the peer lists because such frames do not indicate the presence of a station on that channel.

As a result of methods 1200A-1200C, PL1, PL2 and PL3 are populated with the MAC addresses of wireless stations overheard by wireless station 1106 or in communication with the wireless station. To identify wireless stations that potentially are within transmission/reception
15 range of the wireless station 1106, the proximity identification module 208 may implement exemplary method 1300A of Figure 13A and method 1300B of Figure 13B.

Method 1300A initiates at step 1302 wherein PL1 and PL3 are compared to identify MAC addresses that occur in both PL1 and PL3. A MAC address stored in PL3 implies that wireless station 1106 is either receiving data from that MAC address or it is sending data to that
20 MAC address, so the wireless station having the MAC address might be a potential peer. The occurrence of the same MAC address in PL1 and PL3 indicates that wireless station 1106 overheard a frame being transmitted to another station that is not in communication with the wireless station 1106, which in turn implies that that other station is nearby and potentially inside the same BSS. This is, however, no guarantee that the two stations are within
25 transmission/reception range because no frame was received from that address. Accordingly, at step 1304, the proximity identification module 208 may transmit a test frame directly (i.e., bypassing the access point) to the wireless station having the MAC address occurring in both PL1 and PL3. The test frame may include, for example, a null frame or randomly generated

frame. At step 1306, the proximity identification module 208 waits for an ACK frame from the other wireless station in response to the test frame. If no ACK frame is received, the other wireless station is marked as out of transmission/reception range of the wireless station 1106 at step 1308. If an ACK frame is received, the proximity identification module 208 at step 1310
5 may mark the other wireless station as within the transmission/reception range of the wireless station 1106 and therefore proximate to the station 1106 if proximity is defined as such.

If no ACK frame received, a direct link may still be set up even though direct communications may not be possible. The direct link communications may be relayed by the access point but it may still be possible to use a subset of the extra capabilities in this context. To
10 illustrate, two stations may be in the same BSS but outside of direct link range. In this case, they typically need the access point to relay their traffic because direct transmission is not possible. However, it may be useful to setup an "indirect" direct link in this case by allowing the stations to use a subset of the performance enhancements provided by a direct link. These performance enhancements may include those features which are transparently forwarded by the access point,
15 such as compression, concatenation, encryption, etc.

In this situation, stations which are not within transmission/reception range of each other but which are associated with the same access point may trigger a direct link setup procedure with access point. Similarly, if two stations are engaged in a direct link and they move out of range, the direct link may be logically maintained by routing traffic via the AP and reducing the
20 capability set to match the capabilities of the AP. An indirect direct link (e.g., a long-distance direct link or extended direct link) may require that an additional capability be added to the IDLP signaling. If the long range capability is present in both peer stations, this may imply that the direct link is not ended when a direct transmission fails, but only when the idle timeout passes or when a teardown occurs.

25 Instead of using a test frame, the first data frame transmitted over the direct link formed between the wireless station 1106 and the other station (as described below) may also function as the test frame. When an ACK frame in response to the first data frame exceeds the retry limit, the direct link may be discarded and the other wireless station marked as out of

transmission/reception range. This alternate test process, however, may introduce duplicates at the receiving station so the use of a separate test frame is preferable. Note that the Direct Link typically must be established on a logical level before the test frame is used to test the link.

Method 1300B initiates at step 1312 wherein PL2 and PL3 are compared to identify
5 MAC addresses that occur in both PL2 and PL3. The same MAC address showing up in both PL2 and PL3 implies that wireless station 1106 overheard a frame from another station with which it is currently exchanging traffic. The occurrence of the MAC address of the other wireless station in PL2 indicates that a direct radio connection exists and, therefore, the other wireless station is proximate to wireless station 1106 under a proximity defined by the reception radius
10 1120 (Figure 11). Accordingly, due to the high probability that the other wireless station is within transmission/reception range of the wireless station 1106, the proximity identification module 208 may identify the other wireless station as within transmission/reception range and proximate at step 1314 without transmitting a test frame.

In certain instances, the technique described with reference to Figures 1200A-1300B
15 may be simplified by collapsing PL1 and PL2 into a Nearby Node List (NNL) where $NNL = PL1 \cup PL2$. PL3 then becomes a Peer List (PL) that contains the addresses of peer stations. When the same MAC address occurs in both PL and NNL, the station having the MAC address may be marked as a potential proximate station, but this procedure should include a directed test frame to assess the quality of the radio link between the wireless station 1106 and the other station. The
20 technique may be simplified further by identifying any station having a MAC address in the NNL as a potentially proximate station. The actual proximity of the potentially proximate station then may be verified by, for example, transmitting a test frame to the potentially proximate station.

Referring now to Figure 14, exemplary techniques for determining one or more user IDs
25 associated with an identified proximate wireless station are illustrated in accordance with at least one embodiment of the present invention. For the following, assume a wireless station 1402 has identified a wireless station 1404 as proximate under a default proximity definition or a proximity definition defined by a user of the wireless station 1404. Prior to notifying the user of

the wireless station 1402 of the proximate wireless station 1404, the proximity identification module 208 or notification module 210 (Figure 2) may attempt to obtain one or more user IDs 1406 associated with the user of the wireless station 1404.

5 In one embodiment, the wireless station 1404 may directly supply the desired user ID information 1406 to the wireless device 1402 using, for example, a frame transmitted over a wireless direct link formed between the stations 1402 and 1404 (the formation of direct links are discussed in detail below) by transmitting the user ID information 1406 to the wireless device 1402 as a broadcast or multicast frame. Alternatively, user ID information 1406 may be supplied to an access point 1408 associated with the wireless station 1404 or a proximity server 1410
10 (analogous to proximity server 630/720) responsible for providing proximity information to wireless station 1402. The wireless device 1402, in turn, may request the information from the access point 1408 or the proximity server 1410 using one or more techniques described above.

Referring now to Figures 15 and 16, an exemplary technique for filtering proximate station users for notification purposes is illustrated in accordance with at least one embodiment
15 of the present invention. As noted above, the notification module 210 of a wireless station may perform a filtering process to determine whether the user of the wireless station should be notified of a proximate user. In at least one embodiment, this filtering process includes maintaining an associates table 1502 of user IDs of associates of the user of the wireless station. The associates table 1502 may include a variety of information, such as, for example, a name of
20 the associate (column 1504), user ID(s) of the associate (column 1506), an associate type (column 1508), notification filter rules to be applied to the associated (column 510, rules table 1512), etc.

Information populating the associates table 1502 may be derived from any of a variety of sources. For example, the notification module 210 may be adapted to facilitate the input of
25 associate information directly by the user (user input 1514). Associate information also may be obtained from other information sources, such as the email list of an email client 1516, (e.g., the contacts list information from a Microsoft® Outlook® software program), information from an

electronic rolodex 1518, an electronic phone list 1520 maintained in, for example, a cell phone or PDA, or user information from a instant messaging client 1522.

Figure 16 illustrates an exemplary method 1600 for filtered notification of proximate users using the associates table 1502 of Figure 15. The method initiates at step 1602 wherein the user IDs associated with proximate stations are determined as described above. At step 1604, the user ID obtained from a proximate station is compared with the user IDs (column 1506) of the associates table 1502. In the event that a user ID from a proximate station does not substantially match a user ID in the associates table 1502 (step 1606), the consideration of the user ID for notification purposes may terminate at step 1608 and the next user ID, if any, may be considered for notification purposes.

In the event that the user ID from a proximate station substantially matches a user ID in the associates table 1502, the user ID from the proximate station may be identified as belonging to an associate. Accordingly, at step 1610 the notification module 210 may apply one or more notification filter rules in determining the manner in which the user is notified. The notification rules applicable to a particular associate may be determined from the associates table 1502 or other filter rule source or a default set of notification filter rules may be applied.

The notification filter rules preferably provide guidelines for proximity notification under various conditions. For example, the user may desire to be notified of proximate business associates only during normal business hours (e.g., 9 AM - 5 PM, Monday-Friday). Accordingly, the user may set a rule whereby the notification module 210 is prevented from notifying the user of a proximate business associate during non-business hours. In another example, it may be appropriate to prevent notification of proximate associates in circumstances where their proximity to the user may already be assumed. For example, the user may set a rule whereby notification of proximate co-workers is deactivated within the user's place of work. Other filter rules may be utilized by those skilled in the art using the teachings provided herein without departing from the spirit or the scope of the present invention.

In at least one embodiment, a user may desire notification of proximate wireless users regardless of any association between the user and the proximate users. In this case, after

determining the user IDs of a proximate station at step 1602, the notification module 210 may be adapted to automatically notify the user without comparing the user ID to the associates table 1502 or applying notification filter rules.

5 If notification of a proximate associate is appropriate (step 1612) after applying the relevant notification filter rules, the notification module 210 may notify the user of the wireless station that the associate is nearby at step 1614. Various methods may be used to notify the user. For example, the notification module 210 may prompt the display of a window on a display screen of the user's wireless station that contains text or other graphical representations that notify the user of the proximate associate and provide information about the proximate user.
10 Notification also may be performed by providing speech output via a speaker of the wireless station, the speech output informing the user of the proximate user and providing information about the proximate user. Information about the proximate user may include, for example, the name of the proximate user, the user ID, a telephone number or email address associated with the proximate user, a position (e.g., position coordinates, location within a particular room/area, etc.)
15 of the proximate wireless station, and the like.

In at least one embodiment, the notification also presents the user with the option of initiating a wireless direct link with the proximate station if the proximate station is within transmission/reception distance of the user's station. Alternatively, the user's wireless station could be configured to automatically initiate a wireless direct link with a proximate station. The
20 initiation and establishment of a wireless direct link is discussed in detail below.

Referring now to Figure 17, an exemplary process 1700 for selecting a communication method between proximate wireless stations is illustrated in accordance with at least one embodiment of the present invention. After receiving an indication from a user of a wireless station that communications with a proximate station are desired (step 1702), the link module
25 212 (Figure 2) of the wireless station may attempt to establish communications with the proximate station either via conventional means or via a direct link. In the event that the proximate station is out of transmission/reception range or the proximate station is incapable of or prevented from forming a direct link, at step 1704 the link module 212 may establish

communications with the proximate station in a conventional manner whereby frames are transmitted to the proximate station, and vice versa, via the access points, backbone network, and/or infrastructure network to which the wireless station and proximate station are connected.

5 Otherwise, if a wireless direct link is feasible between the proximate stations, a direct link may be initiated by the wireless station using any of a variety of direct link establishment techniques. For example, in instances wherein the access point is enabled to facilitate the establishment of a wireless direct link between stations, the wireless station may initiate a direct link at step 1706 using the Direct Link Protocol (DLP) technique described in U.S. Patent Application No. 60/388,569 filed June 12, 2002, the entirety of which is hereby incorporated by
10 reference.

Where the access point is prevented from facilitating a direct link between the proximate stations or where the proximate stations may be capable of a PHY rate that is not supported by the access point, the wireless station may initiate a direct link at step 1708 using an Independent Direct Link Protocol (IDLDP) technique as described below with reference to Figures 18 and 19.

15 Direct links offer a number of advantages over conventional communications between stations using an access point as an intermediary. For one, direct links typically are more efficient as the access point is eliminated as an intermediary hop. Furthermore, the bandwidth allocated to a particular wireless station may be limited due to the volume of traffic handled by the access point or the access point may not support a PHY rate of which the proximate stations
20 are capable. To illustrate, the access point may support only IEEE 802.11b with a maximum rate of 11 megabits per second (Mbps), whereas the proximate stations may support IEEE 802.11g with a maximum rate of 54 Mbps. With a direct link, however, active involvement by the access point is removed from the process and a higher data rate therefore may be established between the two proximate stations.

25 After a direct link has been established between the proximate stations at step 1710, the users of the proximate stations may initiate communications via the direct link at step 1712. The communications carried over the direct link may serve a variety of purposes. When the users of the proximate stations are associates, the communications may include, for example, instant

messages or direct emails transmitted between the users for the purpose of setting up a time and or place for the users to meet face-to-face. The users may establish a videoconference over the direct link to allow for interactive audio and video communications. Alternatively, the direct link may be established for establishing a relationship between the proximate users. For
5 example, a wireless station may include a workstation operated by a business, where the workstation is adapted to transmit one or more advertisements, coupon offers or other business communications to the users of proximate stations over direct links established with the proximate stations. The users may consider the business communications in view of the proximity of the business and may choose to visit the business.

10 Referring now to Figures 18 and 19, the IDLP technique for establishing a wireless direct link between proximate wireless stations is illustrated in accordance with at least one embodiment of the present invention. As noted above, U.S. Patent Application No. 60/388,569 discloses a DLP technique for use with IEEE 802.11e that uses MAC management frames to establish a direct link between stations. The DLP technique provides for the transmission of a
15 protocol message from a station to an access point. The access point, in turn, sends the protocol message to the proximate station. The proximate station responds with a message to the access point, which then sends a message to the initiating station to establish a direct link. Because the messages are in the form of MAC management frames, the access point interprets these messages and forms new messages for the receiving station as a result.

20 In certain instances, however, the access point may not be enabled to process MAC management frames in accordance with the DLP technique or the access point may be configured to prevent the establishment of a direct link between proximate stations by analyzing incoming frames to eliminate those MAC management frames that may be used to initiate a direct link. Accordingly, in at least one embodiment, the IDLP technique described herein
25 overcomes the limitations of the access point by initiating and establishing a direct link without active cooperation by the access point. The access point's active cooperation may be bypassed by encapsulating the IDLP signaling messages at the logical link control (LLC) level instead of the MAC level. The LLC encapsulated signaling messages may be transmitted as MAC data frames which typically are transparently forwarded by the access point regardless of the LLC

type. As a result, both the setup and capabilities (e.g., PHY rate) become independent of the limitations of the access point. To illustrate, two IDLP-enabled wireless stations may negotiate and setup a direct link implementing, for example, IEEE 802.11g orthogonal frequency division multiplexing (OFDM) modulations even though the access point is only capable of supporting
5 Barker and complementary code keying (CCK) modulations as set forth in IEEE 802.11b.

To illustrate an exemplary operation of a IDLP direct link setup, Figure 18 depicts proximate wireless stations 1802 and 1804 associated with access point 1806. After determining that a direct link is possible between the wireless devices 1802, 1804 (e.g., they are within transmission/reception range of each other), the wireless station 1802 may transmit a setup
10 request frame 1810 to the access point 1806. To avoid a situation where an IDLP setup procedure is started by both stations 1802 and 1804, the stations 1802 and 1804 may adhere to a convention that only the station with the lowest MAC address shall start an IDLP setup procedure. The setup request frame 1810 preferably includes a MAC data frame having the MAC address of the wireless station 1804 as the destination address. The setup request frame
15 1810, in at least one embodiment, further includes direct link information encapsulated at the LLC layer as discussed below with reference to IDLP frame 1900 of Figure 19. The direct link information may include, for example, proposed link capabilities, such as proposed IEEE 802.11 characteristics (e.g., supported rates) and vendor-specific features (e.g., compression). In one embodiment, the direct link information further may include encryption key information, as
20 discussed below.

The access point 1806 receives the setup request frame 1810 and because it appears to be a typical MAC data frame to the access point 1806, the access point 1806 sends the setup request frame 1810 to the wireless station 1804 as a unicast frame. The wireless station 1802 preferably is prevented from entering a power save mode after transmitting the setup request frame 1810.

25 Upon receiving the setup request frame 1810, in at least one embodiment, the wireless station 1804 transmits a IDLP probe frame 1812 directly to the wireless station 1802. The IDLP probe frame 1812 may include, for example, a random 1500-byte data frame having the MAC address of the wireless station 1802 in both address fields A1 and A2 (discussed above). Upon

receipt of the IDLP probe frame 1812, the wireless station 1802 preferably is adapted to immediately send an ACK frame to the wireless station 1804 rather than processing the IDLP probe frame 1812 by the protocol stack 226 (Figure 2) before sending an ACK frame.

5 If the wireless station 1804 does not receive an ACK frame from the wireless station 1802 in response to the IDLP probe frame 1812, the wireless station 1804 may transmit a IDLP teardown response to abort the direct link establishment process. Otherwise, if the ACK frame is received, the wireless station 1804 may consider the proposed capabilities presented in the setup request frame 1810. If the proposed capabilities are acceptable to the wireless station 1804, the wireless station 1804 may transmit a setup response frame 1814 to the wireless station 1802 via
10 the access point 1806. If the setup request frame 1810 advertises multiple capabilities of the same sort (for instance a selection of supported compression algorithms), the wireless station 1804 may choose and select one of these and indicate its selection in the setup response. As with the setup request frame 1810, the setup response frame 1814 may include an IDLP frame encapsulated at the LLC layer to appear as a typical MAC data frame to the access point 1806 so
15 that the access point 1806 forwards the setup request frame 1814 to the wireless station 1802 with minimal modification.

Upon receipt of the setup response frame 1814, the wireless station 1802 enables itself to receive frames directly from wireless station 1804 and transmits a setup confirm frame 1816 to the wireless station 1804 via access point 1806. The setup confirm frame 1816 confirms the
20 successful negotiation of the capabilities of the direct link between the stations 1802 and 1804 and notifies the station 1804 to enter direct link mode. As with frames 1810 and 1814, the setup confirm frame 1816 may include an LLC encapsulated frame that appears as a MAC data frame to the access point 1806 so that it is forwarded with minimal processing by the access point 1806.

25 After setup confirm frame 1816 has been received by the wireless station 1804, a direct link is established between the wireless stations 1802, 1804 and each station therefore may transmit data frames 1818 directly to the other station without the access point 1806 acting as an intermediary.

When the direct link is to be terminated, one of the wireless stations 1802 and 1804 may transmit an IDLP teardown request frame 1820 to the other either directly via the direct link or via the access point 1806. The receipt of the IDLP teardown request frame 1820 directs the receiving wireless station to cease direct transmission of frames to the other workstation. The receiving wireless station may then transmit a teardown response frame (not shown) to the other station to acknowledge receipt of the teardown request.

Figure 19 illustrates an exemplary LLC-encapsulated IDLP frame 1900 that may be used as the setup request frame 1810, setup response frame 1814, setup confirm frame 1816 or teardown request frame 1820. In the illustrated example, the IDLP frame 1900 is similar to a MAC data frame in that it includes a MAC header field 1902 in accordance with one or more wireless standards, an Organizationally Unique Identifier (OUI) protected protocol field 1904, an OUI field 1906, and an LLC type field 1908. The IDLP frame 1900 further includes an IDLP version field 1910, and IDLP type field 1912, a MAC address field 1914, a BSSID field 1916, a capability information field 1918 and an information elements field 1920.

The LLC type field 1908, in one embodiment, includes a value (e.g., 0x0003) identifying the frame 1900 as an IDLP frame. Accordingly, upon receipt of the frame 1900, an IDLP-enabled wireless station may note the IDLP identifier in the LLC type field 1908 and process the frame 1900 in accordance with the IDLP techniques described above. The IDLP version field 1910 contains a value indicating the IDLP version applicable to the frame 1900. The IDLP type field 1912 contains a value indicating the type of IDLP frame as shown by table 1922. The MAC address field 1914 stores the MAC address of the station transmitting the frame 1900 and the BSSID field 1916 stores the BSSID with which the transmitting station is associated.

As noted above, the setup request frame 1810, the setup response frame 1814 and setup confirm frame 1816 are used to negotiate the capabilities of the proposed direct link.

Accordingly, the capability information field 1918 may include data related to the capabilities, such as PHY rate, compression types, encryption capabilities, etc. The probe frame 1812 and teardown request/response frames typically do not convey link characteristic information. These

frames therefore may omit the capability information field 1918 and information elements field 1920.

Security via encryption is frequently provided in Wireless Fidelity Protected Access (WPA) or similar environments, such as IEEE 802.11i. Pairwise encryption keys established by WPA or the like may be used to secure the IDLP setup messages. The encryption key for protecting subsequent station-to-station IDLP data therefore can simply be transferred over the WPA protected link, as the entire IDLP Setup Request/Response exchange is protected by the pairwise key between the stations and the access point. In one embodiment, the information elements field 1920 may be used to transport the key material to be used on the direct link. This information preferably is provided only in the setup request frame 1810. A key material type field preceding the key material in the information elements field 1920 may be used to indicate the type and context of the key material present in the information elements field 1920. There is one simple key material type indicating that the direct link uses the same cipher suites as used on the pairwise links between a station and the access point and only key material is provided. Other types may indicate specific cipher suites to be used on the direct link. To illustrate, if TKIP is being used on pairwise links between stations and the access point in the network and both stations intend to use TKIP for the direct link as well, providing key material only suffices and the cipher suite will default to the cipher suite used between the station and the access point. However, if for example the stations wish to use the stronger AES (advanced encryption standard) algorithm for their direct link (this may not even be available on the access point), cipher suites need to be negotiated explicitly along with provision of key material.

Referring now to the documents attached as Appendices A-C, additional features associated with location awareness and the establishment of a direct link are disclosed.

Other embodiments, uses, and advantages of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. The specification and drawings should be considered exemplary only, and the scope of the invention is accordingly intended to be limited only by the following claims and equivalents thereof.

APPENDIX A

INDEPENDENT DIRECT LINK PROTOCOL SUMMARY:

Independent Direct Link Protocol

5 Abbreviations

	ACK.....	Acknowledgement
	AP.....	Access Point
	BSS.....	Basic Service Set
	BSSID.....	Basic Service Set Identifier
10	CCK.....	Complementary Code Keying
	DL.....	Direct Link
	DLP.....	Direct Link Protocol
	IDLP.....	Independent Direct Link Protocol
	IE.....	Information Element
15	IEEE.....	Institute of Electrics and Electronics Engineers
	LLC.....	Logical Link Control
	MAC.....	Media Access Control
	OFDM.....	Orthogonal Frequency Division Multiplexing
	TKIP.....	Temporal Key Integrity Protocol
20	Tx.....	Transmit
	UUI.....	Organizationally Unique Identifier
	PHY.....	Physical Layer
	Rx.....	Receive
	WiFi.....	Wireless Fidelity
25	WPA.....	WiFi Protected Access

Introduction – 802.11e Direct Link Protocol (DLP)

30 The current state of the art in IEEE 802.11e (currently only available in draft) is a Direct Link Protocol which uses MAC management frames to set up direct links between stations in an infrastructure network. The IEEE 802.11e DLP lets client stations set up a Direct Link with a peer client station, by sending a protocol message to the AP, which in sends a protocol message to the peer client. The peer client responds with a message to the AP, which sends a message to the initiator client and the Direct Link is a fact. The AP interprets these messages and forms new messages as a result.

35 With Direct Link, peer-to-peer traffic is much more efficient, because the AP is eliminated as an intermediate hop.

Invention –Independent Direct Link Protocol (IDLDP)

40 This invention is an enhancement to IEEE 802.11e DLP, which allows the Direct Link to be set up without cooperation of the AP. This is achieved by encapsulating the IDLP signaling messages at the LLC level, instead of at the MAC level (the LLC layer is the protocol layer on top of the MAC layer). The LLC encapsulated signaling messages are transmitted as MAC Data

frames, which are transparently forwarded by the AP, irrespective of the LLC type. This makes the Direct Link signaling independent of the AP, hence the name Independent Direct Link Protocol (IDLP). This is clarified in Table 1.

LLC	IDLP Signaling Messages	Not interpreted by the AP
MAC	DLP Signaling Messages	Interpreted by the AP

Table 1. Layering for DLP and IDLP signaling messages.

Transparent signaling through LLC encapsulation allows for Direct Links to be set up also if the AP itself does not support the Direct Link capability. The Direct Link may use capabilities (like PHY rates) which the AP does not support. In other words, by using IDLP, both the setup and capabilities of the Direct Link become independent of the AP. As an example, two IDLP capable clients may negotiate and setup an IDLP link and 802.11g OFDM modulations, while both clients are associated with an 802.11b AP. (802.11b does not include OFDM modulations, but only Barker and CCK)

The AP may always filter IDLP messages if it wishes to avoid the use of Direct Links inside the BSS. But this requires knowledge of the fact that IDLP exists.

If security is enabled in the infrastructure network, the Direct Link security credentials can be exchanged by the IDLP clients, using the LLC encapsulated IDLP signaling messages. The credentials are transmitted with the security of the BSS, so the security of the Direct Link will be as strong as the security of the BSS.

IDLP Frame Formats

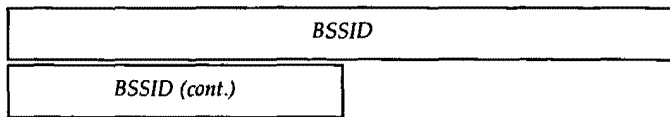
The generic LLC GlobespanVirata encapsulation frame is defined as follows.

802.11 MAC Header	AA-AA-03	00-10-91	<i>LLC Type</i>
<i>n</i>	3	3	2

The 802.11 MAC header is followed by an GlobespanVirata-specific LLC encapsulation using the GlobespanVirata OUI. The *LLC Type* indicates what type of GlobespanVirata-specific LLC-encapsulated frame this is. For IDLP, this is 0x0003.

The generic IDLP frame is using LLC encapsulation and is defined as follows:

<i>IDLP Version</i>	<i>IDLP Type</i>	<i>MAC Address</i>
<i>MAC Address (cont.)</i>		



5

The *IDLP Version* currently defined is 1. The *IDLP Type* can have the following values:

0	IDLP Setup Request
1	IDLP Setup Response
2	IDLP Setup Confirm
3	IDLP Probe
4	IDLP Teardown Request
5	IDLP Teardown Response
6-FF	Reserved

10 The *MAC Address* is the MAC address of the sending station. The *BSSID* indicates the BSSID the sending STA is associated with.

The generic IDLP frame format is used for IDLP Probes, IDLP Teardown Requests/Responses.

15 IDLP Setup Requests/Responses/Confirms are effectively used to create a virtual association between two STAs, and therefore these need to advertise and negotiate particular IDLP link characteristics. Characteristics can include both 802.11 characteristics (e.g., supported rates), and Intersil-specific features (e.g. compression).

20 Therefore these frames have more elaborate formats, defined as follows:

<i>IDLP Version</i>	<i>IDLP Type</i>	<i>MAC Address</i>
<i>MAC Address (cont.)</i>		
<i>BSSID</i>		
<i>BSSID (cont.)</i>		<i>Capability Info</i>
<i>Information Elements (variable length)</i>		

25

30

IDLP Security

Security is only provided in WPA or similar (802.11i) environments. Pairwise keys established by WPA secure the IDLP setup messages. The key for protecting subsequent STA-to-STA IDLP data can simply be transferred over this link, as the entire IDLP Setup Request/Response

35

exchange is protected by the pairwise key between IDLP STA1 and the AP and IDLP STA2 and the AP.

A GlobespanVirata Key Information Element has been defined that transports the key material to be used on the direct link. This information element shall be provided in the IDLP Setup Request frame only. A *key material type* field preceding the key material in the IE indicates the type and context of the key material present in the IE. There is one simple *key material type* indicating that the direct link uses the same cipher suites as used on the pairwise links between STA and AP; other types may indicate specific cipher suites to be used on the direct link.

For TKIP, the first 128 bits of the key material shall denote the TKIP encryption key; the next 64 bits shall denote the Michael Tx key of the sender of the IDLP Request; the last 64 bits denote the Michael Rx key of the sender of the IDLP Request.

IDLP Protocol Overview

The IDL protocol consists of several signaling messages, which are summarized below. A possible protocol for the setup and teardown of a Direct Link based on IDLP are shown in Figure 1.

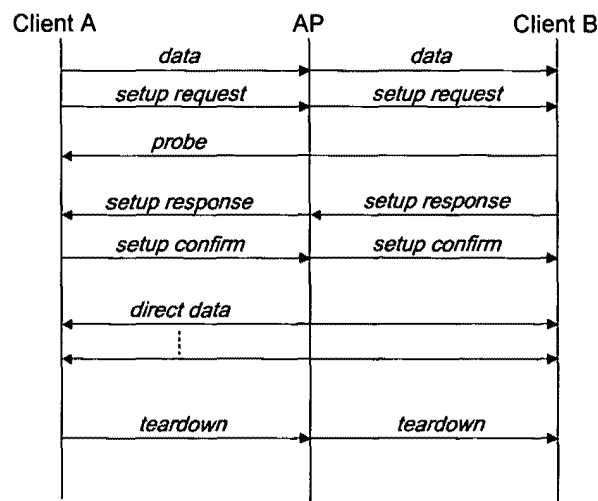


Figure 1. Overview of Direct Link setup and teardown. The MAC ACK frames were omitted, for clarity.

IDLP setup request

- Client A sends an IDLP setup request to Client B when a Data frame is sent to Client B and Client B occurs in the peer list
- The IDLP setup request is sent as a unicast frame via the AP
- The IDLP setup request contains capabilities and possibly key material
- Client A shall not go into power save after transmitting an IDLP setup request

IDLP probe (optional)

- Client B sends an IDLP probe is sent when an IDLP setup request was received (Client A will not be in power save, because it just started the IDLP negotiation)
- 5 • The IDLP probe is a random 1500 Byte Data frame
- The IDLP probe is sent directly from peer to peer
- The IDLP probe frame will not be sent up the stack, but it will be auto-ACKed
- If the IDLP probe succeeds (i.e. an ACK is received), Client B responds with an IDLP setup response
- 10 • If the IDLP probe fails, Client B sends an IDLP teardown response

IDLP setup response

- Client B sends an IDLP setup response to Client A if the capabilities in the request are acceptable and the IDLP probe succeeded
- 15 • After transmission of the setup response, Client B enables the reception of directed traffic from Client A
- After receiving the setup response, Client A enables the transmission and reception of directed traffic from Client B

20 **IDLP setup confirm**

- Client A sends an IDLP setup confirm to Client B to confirm the successful negotiation
- After receiving the setup confirm, Client B enables the transmission of directed traffic to Client A

25 **IDLP teardown**

- When a Direct Link must be ended, Client A or Client B transmits an IDLP teardown.
- The transmission of a teardown disables direct transmission and direct receipt.

Note that nodes A and B could both be the initiator of the direct link setup procedure.

30

APPENDIX B

AUTOMATIC PEER DISCOVERY PROTOCOL SUMMARY:

Abbreviations

5	A1.....Address 1
	A2.....Address 2
	A3.....Address 3
	Ack.....Acknowledgement frame
	AP Access Point
	BSS Basic Service Set
10	BSSID Basic Service Set Identifier (MAC Address of AP)
	D.....Destination
	DA.....Destination Address
	Data.....Data Frame
	DL Direct Link
15	DLP Direct Link Protocol
	F1 Frame 1
	F2 Frame 2
	F3 Frame 3
	F4 Frame 4
20	IDLP.....Independent Direct Link Protocol
	DS Distribution System
	IEEE.....Institute of Electrics and Electronics Engineers
	LLC Logical Link Control
	PDLP Proprietary Direct Link Protocol
25	MAC Media Access Control
	NNL Nearby Node List
	PL.....Peer List
	PL1 Peer List 1
	PL2 Peer List 2
30	PL3 Peer List 3
	PHY.....Physical Layer
	S Source
	SA Source Address
35	WDS.....Wireless Distribution System

Introduction – 802.11e Direct Link Protocol

40 The current state of the art in the IEEE 802.11e draft is a Direct Link Protocol which uses MAC management frames to set up direct links between stations in an infrastructure network. The need for such a protocol is justified by the fact that peer-to-peer traffic between nodes inside the same network can be transmitted directly, instead if via the AP. This creates a considerable efficiency gain.

45 DLP allows clients to set up a Direct Link with a peer client station, but DLP does not indicate when a client should attempt to do so.

Invention – Automatic Peer Discovery Procedure

This invention describes how the presence of peer nodes can be automatically detected, and when a Direct Link setup handshake should be started as a result of that. As a background, it is important to realize that 802.11 frames contain several address fields inside the MAC header,

depending on their type (Control, Data, Management). The first address field (A1) always indicates the immediate receiver of the frame. The second address field, denoted A2, contains the transmitter of the frame. The third address field (A3) contains either the ultimate source of the frame (for downlink or From-DS frames), the ultimate destination (for uplink, or To-DS frames), or the BSSID (Direct Link and Ad Hoc frames). The address fields present in Data and ACK frames is shown in Table 2.

Frame	Address Fields
Data (From-DS, To-DS, Direct)*	A1, A2, A3
ACK	A1

Table 2. Address fields in Data and ACK frames. (* AP-AP WDS frames are not considered.)

Then automatic peer discovery procedure described in this invention matches source and destination addresses from frames that are received or transmitted. The mechanism is designed such that a Direct Link setup will always be started after the transmission of a single frame from one peer to another, through the AP. This peer-to-peer transmission requires the transmission of 4 frames between the Source (S), the Access Point (AP) and the Destination (D), as shown in Table 3.

Frame	Type	From	To
F1	Data	S	AP
F2	Ack	AP	S
F3	Data	AP	D
F4	Ack	D	AP

Table 3. Frame transmissions required to transmit a single MPDU peer-to-peer without Direct Link.

A client obtains information from frames that are received, including frames which are not destined for that station. A1 contains the address of a station that might be in the vicinity, because a frame is transmitted to it. A2 contains the address of a station which is in the vicinity and within reach, because it is transmitting the frame. A3 inside frames with matching A1 (i.e. the frame is destined for that station) identifies a source which may potentially be a peer node, but it may also be a node somewhere on the wired side of the network. If a frame is transmitted, the Destination Address (DA) may be a peer node, but it may also be a node somewhere on the wired side.

To find potential peer-to-peer connections, the address information should be stored in three Peer Lists. Address information should be stored in PL1, PL2 and PL3 in the following way:

1. the station overhears a frame (i.e. A1 does not match the own MAC address)
 - Store A1 in PL1
 - Store A2 in PL2
2. the station receives a frame (i.e. A1 matches the own MAC address)
 - Store A3 in PL3

3. the station transmits a frame

- Store the DA in PL3

5 Addresses must not be stored if they are the BSSID or if they are a broadcast or a multicast address. Filtering the BSSID avoids that a direct link is set up with the AP, while Broadcast and Multicast addresses must be filtered because they do not designate a specific station.

Note that PL3 may contain a mixture of source and destination addresses.

10

Peer List entries should be aged and removed after a certain age, if they are not refreshed.

When the station finds the same address in PL3 and either PL1 or PL2, it shall start the Direct Link setup procedure for that address. No action shall be taken based on single entries.

15

This can be understood as follows. When an address shows up in PL3, this implies that the station is either receiving data from that address or it is sending data to that address, so this address might be a potential peer. The occurrence of the same address in PL1 indicates that the station overheard a frame being transmitted to that same station, which is an indication that that station is nearby and potentially inside the same BSS. There is no guarantee that the two stations are within reach, because no frame was received from that address, but a Direct Link setup procedure should be started to find. The Direct Link procedure should be started with a directed test frame in this case, which will establish whether direct connectivity is possible. When the test frame is acknowledged, the station must start the Direct Link setup procedure. Note that direct connectivity may only be possible at a lower PHY rate than the PHY rate that was previously used to transmit to the AP.

20
25

The same address showing up in both PL3 and PL2 implies that the station overheard a frame from a station with which it is currently exchanging traffic. The occurrence in PL2 indicates that a direct radio connection exists, and the station may start the Direct Link setup procedure without sending a test frame first.

30

Summary

In summary,

35

- $A \in \{PL3 \cap PL1\}$: A is a potential peer but that it is not known whether a Direct Link is possible from a radio link perspective. Send a test frame directed to A first and start the Direct Link setup if an acknowledgement is received (for the first try or for the subsequent retries).
- $A \in \{PL3 \cap PL2\}$: A is a potential peer, with a high probability for a good radio connection. Start the Direct Link setup procedure without sending a test frame.

40

Instead of using a test frame in the $\{PL3 \cap PL1\}$ case, the first Data frame that is to be transmitted over the Direct Link may also function as the test frame. When the Data test frame exceeds the retry limit, the Direct Link is discarded and the Data frame may be retransmitted via

45

the AP. (This may introduce duplicates at the receiver, however, so the use of a separate test frame is recommended. A Null frame could serve as a test frame.)

- 5 Peer lists may be pre-populated when stations periodically transmit a Null frame at a low PHY rate, with $A1 = A2 =$ own MAC address (i.e. Null-to-self). The addresses from the Null frame will be inserted into the peer list by as many Direct Link capable clients as possible.

- 10 The peer lists may also be pre-populated when other stations join and authentication or association request/response frames are received. Address information from Probe Request/Response frames should not be added to the peer lists, because such frames do not indicate the presence of a station on that channel.

Simplified Procedure

- 15 It is possible to simplify this procedure by collapsing PL1 and PL2 into a Nearby node List (NNL = $PL1 \cup PL2$). PL3 then becomes the Peer List (PL), which contains the addresses of peer nodes. When the same address occurs in both PL and NNL, a Direct Link setup procedure may be started, but this procedure should include a directed test frame:

- 20
 - $A \in \{PL \cap NNL\}$: A is a potential Direct Link peer, but that it is not known whether a Direct Link is possible from a radio link perspective. A Direct Link setup procedure should be started, but preferably be preceded by a test frame, to assess the quality of the link.

- 25 The simplified procedure reduces a peer list, but at the cost of dismissing information about the quality of the Direct Link.

Proof

This section proves that a single intra-BSS Data transmission via the AP triggers a Direct Link setup procedure based on the above described method. First of all, it is helpful to realize that a 3 point constellation {S, AP, D} in a 3 dimensional space can be analyzed in a 2 dimensional plane that extends through the antennas of the three nodes. The radio signal is assumed to spread spherically, so that the range limits are circles in the plane.

It is assumed that stations have an arbitrarily fine grained PHY rate selection, tuned such that the signal reaches the destination but not necessarily beyond that. (The range of a PHY rate is influenced by the coding gain and the transmit power. Higher PHY rates will have a shorter range, because there is less coding gain.) We will assume that each station (including the AP) selects the optimal PHY rate to reach the receiver, so the distance between the receiver and the sender determines the radius of the range limiting circle. In practice, there will not be an infinite granularity, which implies that frames may be decoded in a wider range around the sender than strictly necessary to reach the receiver, but this will only make it easier to overhear other transmissions and store the address information.

With respect to the location of the Source (S), the Destination (D) and the Access Point (AP), there are 6 possible constellations (see Figure 2). Each constellation has different properties with respect to which node overhears which transmissions.

The following can be said:

- Constellation I
D does not hear S transmit to the AP, and S does not hear the AP's transmissions to D. The only frame which will be overheard by D is the Ack frame transmitted by the AP to S (F2).
- Constellation II
D does not hear S transmit to the AP, and D does also not hear the AP's response with an Ack. But S does hear the AP's transmission to D (F3).
- Constellation III
D hears S transmit to the AP, and S hears the AP's transmission to D (F1, F3).
- Constellation IV
D hears both the S transmit to the AP, and the AP's response to S. S does not hear the transmission from the AP to D (F1, F2).
- Constellation V
D does not hear S transmit to the AP, but D does hear the AP transmit to S and S hears the AP transmit to D (F2, F3).
- Constellation VI
All frames are overheard: (F1, F2, F3).

The entire plane is covered by these constellations. Hence any 'inverted' constellation, where D and S are swapped, will be part of one of the above constellations as well.

- 5 To understand why there are six distinct constellations, consider the following. F1 is only
overheard by D when S is on the right side of line L. Every point on line L has an equal distance
to the AP and to D (see Figure 2), so on the right side of L, the distance to D is always smaller
than the distance to the AP, which implies that a transmission from S to the AP will be overheard
by D, while on the left side of L, the distance to D is larger than the distance to the AP, so
10 transmissions from S to AP will not be heard by D (see Figure 3).

For F2 and F3, which are both transmitted by the AP, there are 3 possibilities. Either F2 is
overheard by D (S outside C), or F3 is overheard by S (S inside C), or both (S on C). This is
shown in Figure 3.

- 15 S on C appears to be a hypothetical case because the circle C has a zero surface area and thus no
probability of occurrence. In practical situations, however, with finite decoding granularity, C
will be ring shaped, and will therefore have a non-zero surface area.

- 20 The transmissions and the corresponding Peer List populations are summarized in Table 4. It can
be seen that in all cases, either the Source or the Destination has the same address in PL3 and
either PL1 or PL2, after F3 is transmitted. This concludes the 'proof'.

- 25 The Direct Link setup procedure will be started after F3, either by the Source or the Destination
or both (see Table 5). The presence of unicast transmissions to or from S or D may pre-populate
the peer lists, which will expedite the Direct Link setup procedure.

A summary of the transmissions for constellations I through IV is shown in Figure 4 through
Figure 9.

30

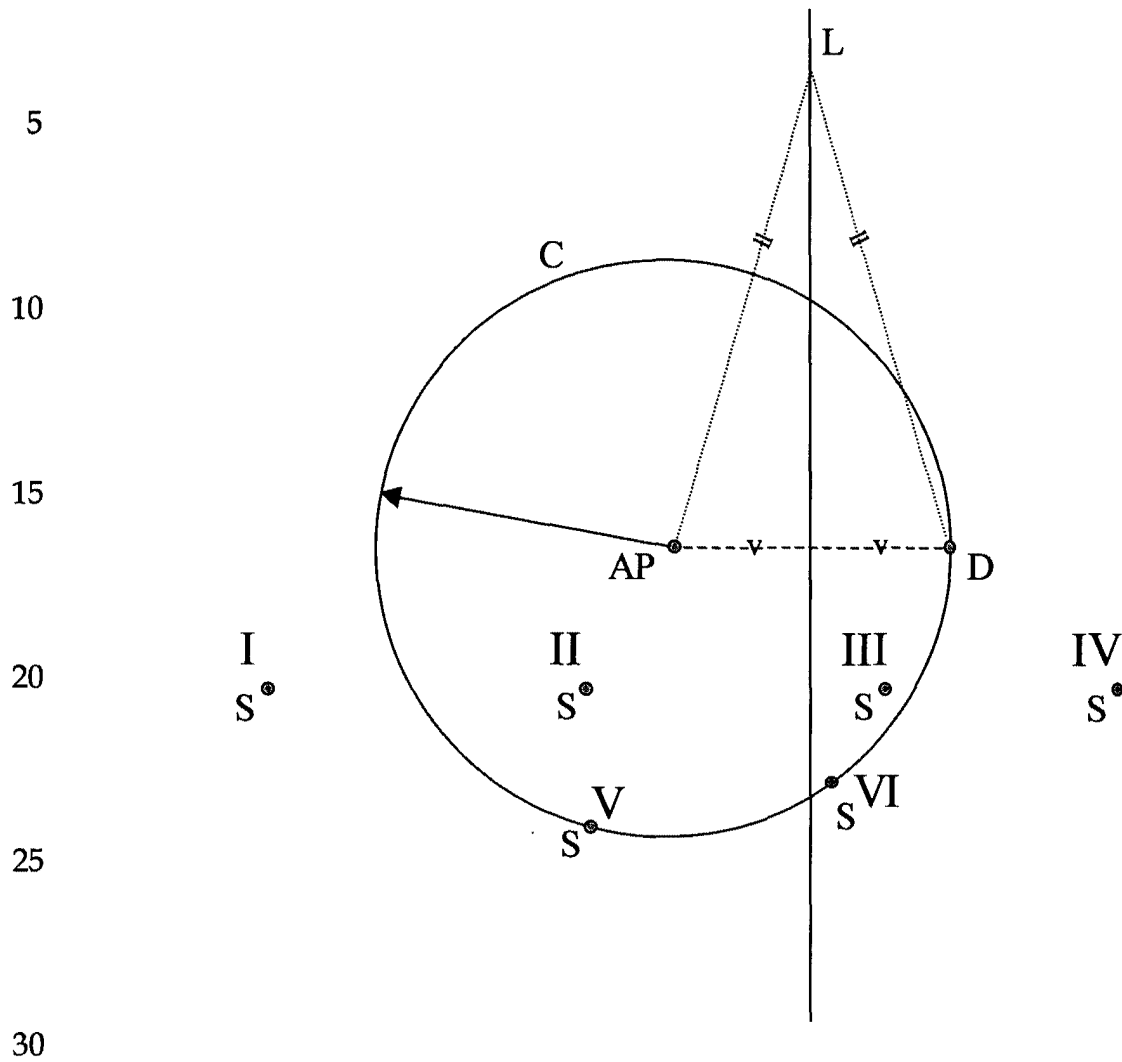


Figure 2. The plane through the antennas of S, AP and D can be divided into six possible constellation, I-VI. Each constellation has its own characteristics with respect to which frames are overheard by which node.

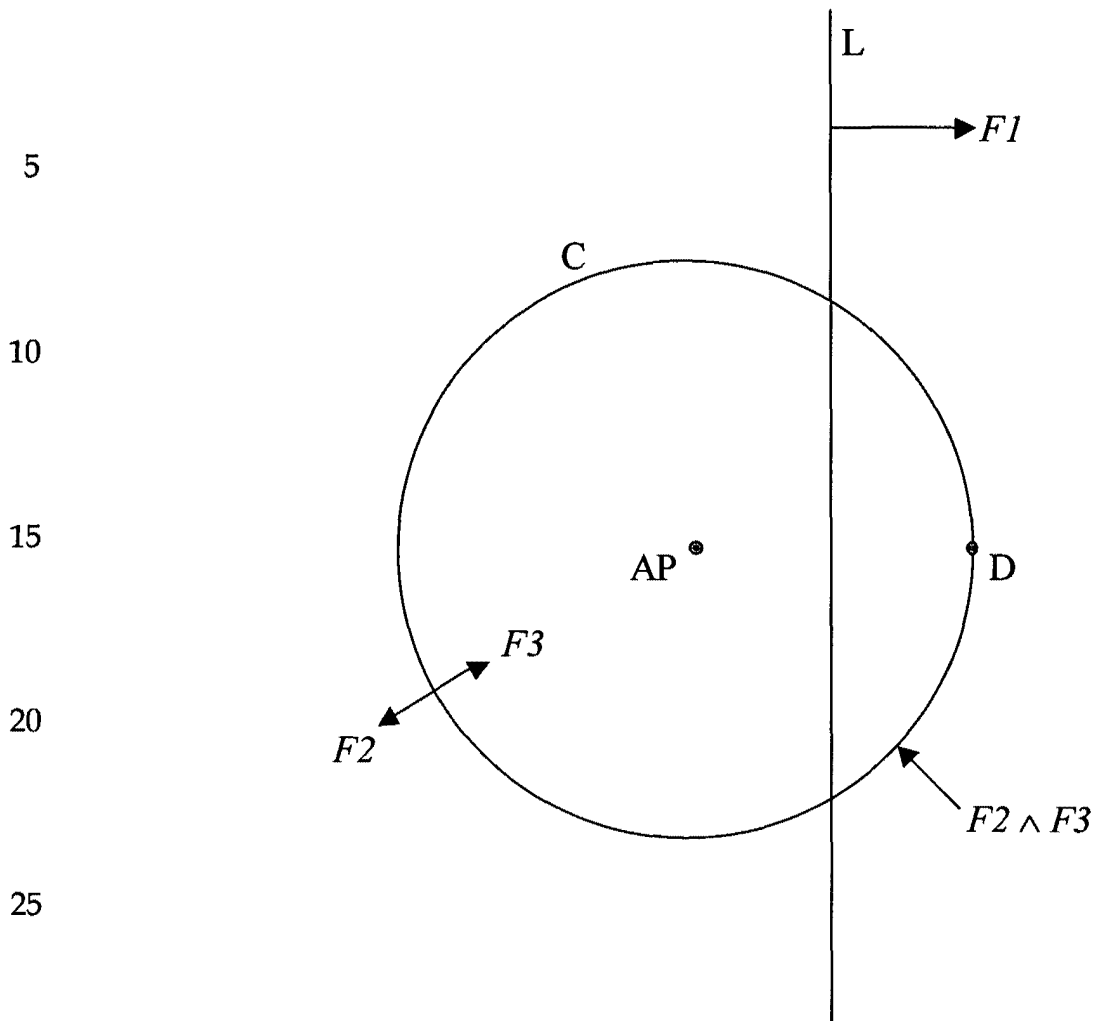


Figure 3. The location with respect to C and L determine which frames can be overheard. F1 is the Data frame sent from S to the AP, F2 is the ACK to that frame sent by the AP, F3 is the Data frame which is forwarded by the AP, F4 is the ACK to that frame sent by D. F4 does not convey any information about S or D, so it is omitted from this figure.

Const. I	S	D	direction	type
F1	PL3	PL1	up	Data
F2			down	Ack
F3	PL3	PL3	down	Data
F4			up	Ack

Const. II	S	D	direction	type
F1	PL3		up	Data
F2			down	Ack
F3	PL1	PL3	down	Data
F4			up	Ack

Const. III	S	D	direction	type
F1	PL3	PL2	up	Data
F2			down	Ack
F3	PL1	PL3	down	Data
F4			up	Ack

Const. IV	S	D	direction	type
F1	PL3	PL2	up	Data
F2			down	Ack
F3		PL3	down	Data
F4			up	Ack

Const. V	S	D	direction	type
F1	PL3	PL1	up	Data
F2			down	Ack
F3	PL1	PL3	down	Data
F4			up	Ack

Const. VI	S	D	direction	type
F1	PL3	PL2	up	Data
F2			down	Ack
F3	PL1	PL3	down	Data
F4			up	Ack

Table 4. Overview of when an address are stored in what Peer List, for each constellation.

Constellation	Initiator of Direct Link
I	D
II	S
III	S & D
IV	D
V	S & D
VI	S & D

Table 5. Initiator of the Direct Link setup procedure, for each constellation.

PATENT
Attorney Docket No. 56162.000497
GV 297

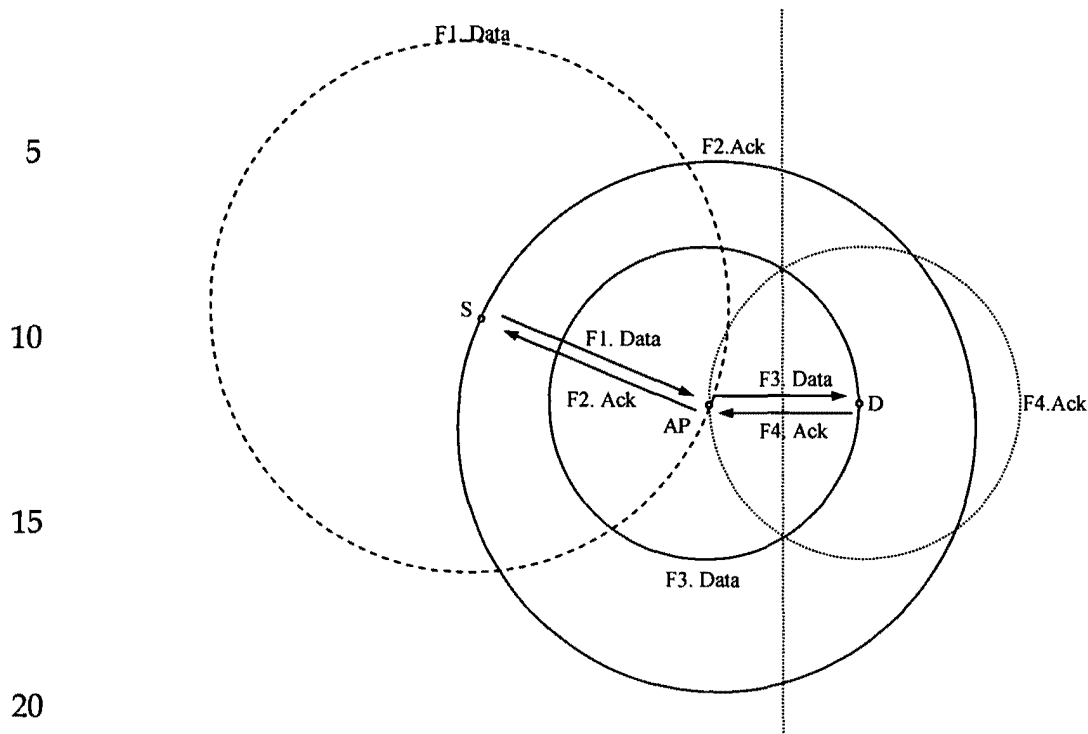


Figure 4. Overview of transmissions for constellation I.

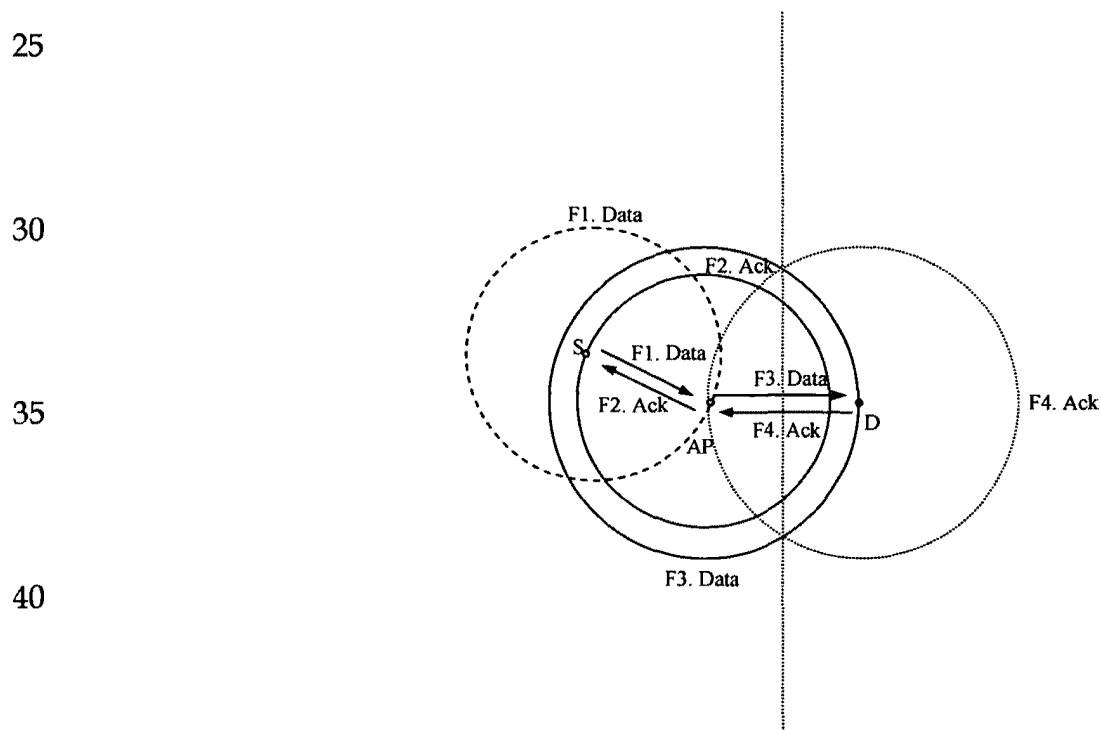


Figure 5. Overview of transmissions for constellation II.

5

10

15

20

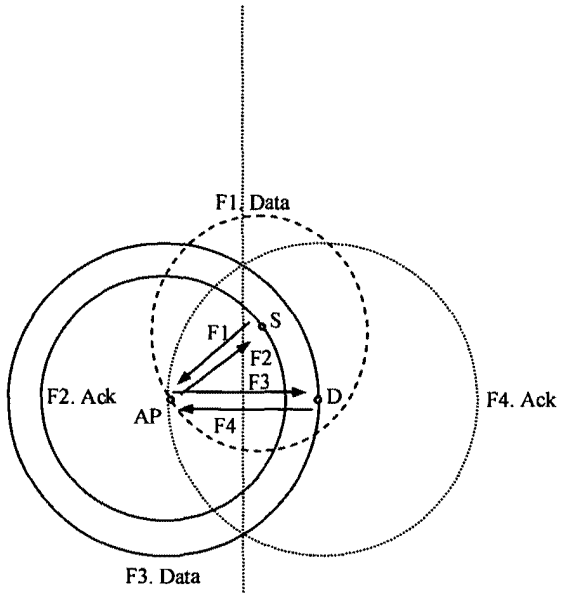


Figure 6. Overview of transmissions for constellation III.

25

30

35

40

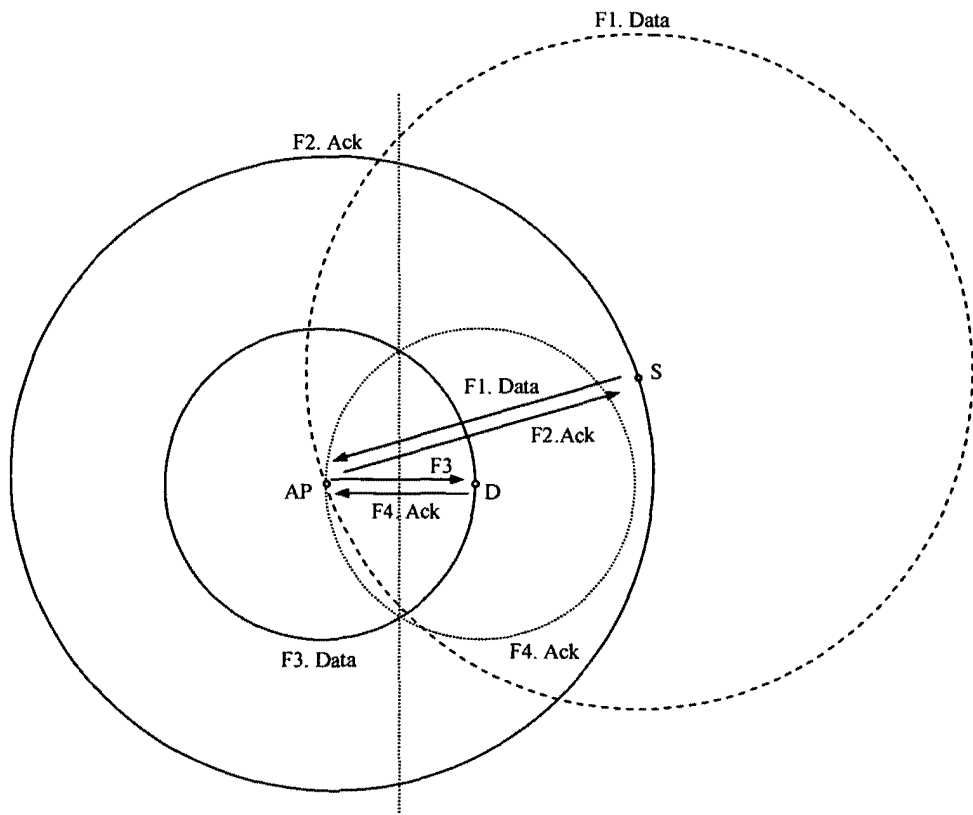


Figure 7. Overview of transmissions for constellation IV.

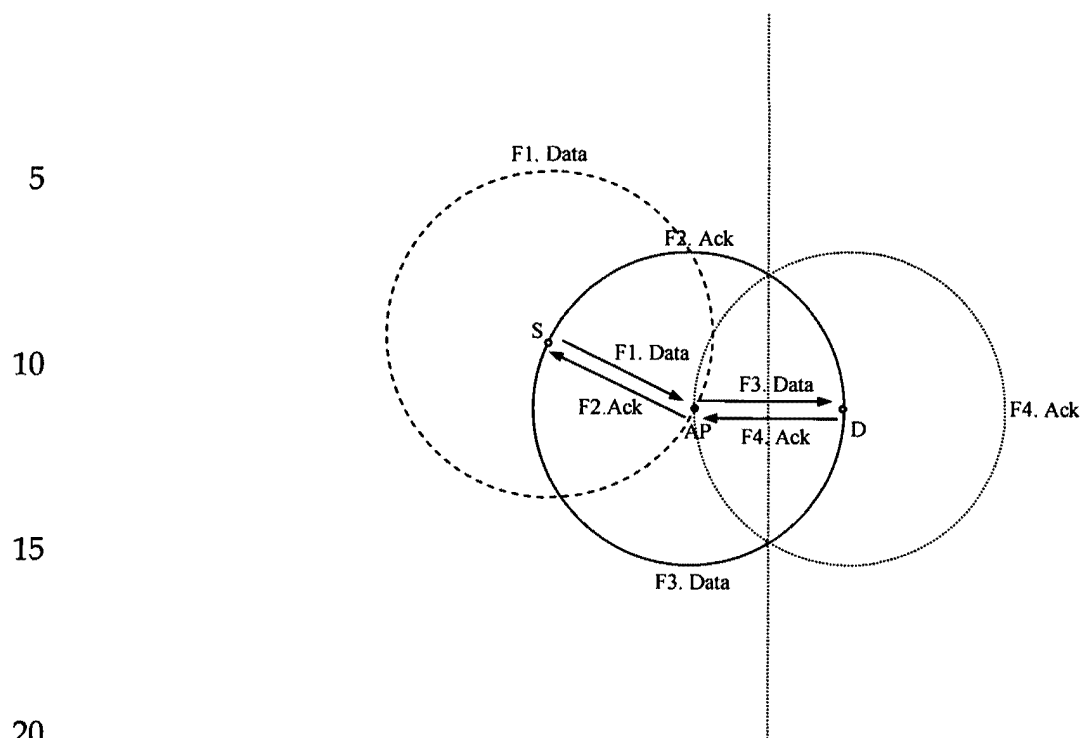


Figure 8. Overview of transmissions for constellation V.

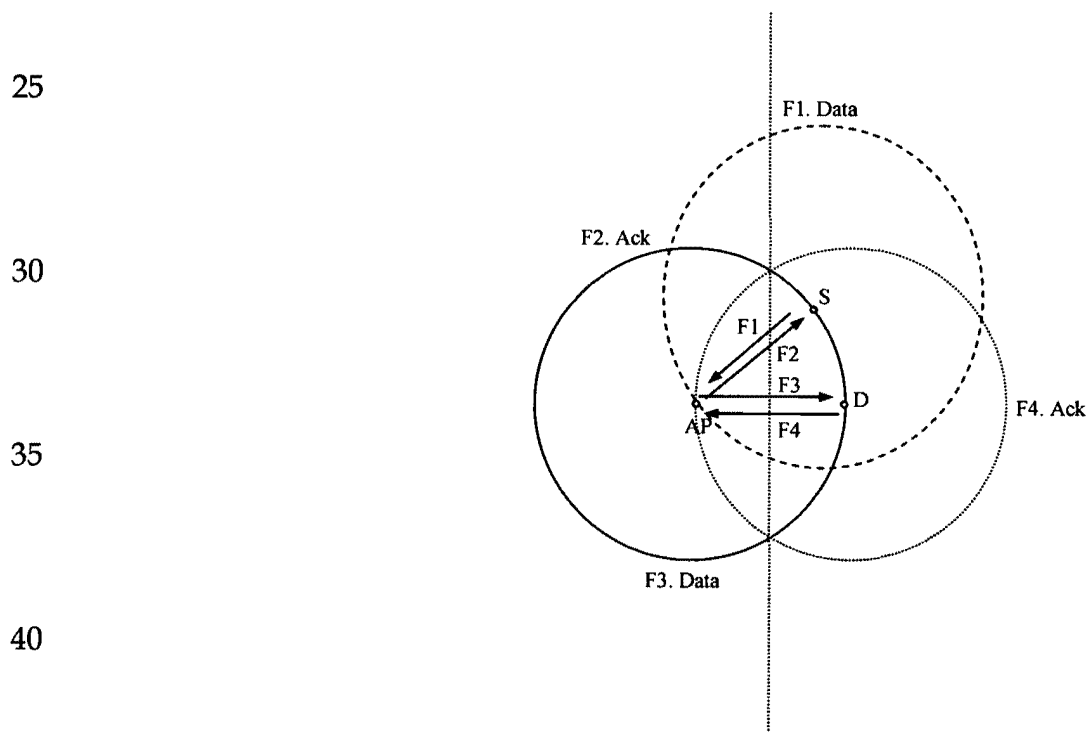


Figure 9. Overview of transmissions for constellation VI.

APPENDIX C

LOCATION AWARENESS SUMMARY:

Abbreviations

5	A1.....Address 1
	A2.....Address 2
	A3.....Address 3
	Ack.....Acknowledgement frame
	AP Access Point
	BSS Basic Service Set
10	BSSID Basic Service Set Identifier (MAC Address of AP)
	D.....Destination
	DA.....Destination Address
	Data.....Data Frame
	DL Direct Link
15	DLP Direct Link Protocol
	F1 Frame 1
	F2 Frame 2
	F3 Frame 3
	F4 Frame 4
20	IDLP.....Independent Direct Link Protocol
	DS Distribution System
	IEEE.....Institute of Electrics and Electronics Engineers
	LLC Logical Link Control
	PDLP.....Proprietary Direct Link Protocol
25	MAC Media Access Control
	NNL Nearby Node List
	PL.....Peer List
	PL1 Peer List 1
	PL2 Peer List 2
30	PL3 Peer List 3
	PHY.....Physical Layer
	S Source
	SA Source Address
35	WDS.....Wireless Distribution System

The invention consists of mechanisms to determine when two devices are connected to the same Wireless LAN Access Point or wireless network, in conjunction with the peer-to-peer exchange of data that may be enabled by the user notification of the other device in proximity on the network. The two devices are members of a set of users that is determined in advance, such as a list of friends and colleagues as is typically established for Instant Messenger systems. For example, mobile workers could discover that a colleague is in the same airport. Notifications of friends that are nearby at a wireless hot spot could pop up on users' screens. These functions could be offered as a value-added service by service providers and hot-spot operators, or could operate on an Internet-scope subscription service. Once users are aware of friends or colleagues that are nearby, they can establish direct (point to point) wireless connections to share data.

The use of the proximity notification can be as simple as enabling a face to face meeting and conversation, or as a first step in establishing a wireless direct link connection between the two users to exchange data. This direct link between users can be established using IEEE standards based methods, such as the Direct Link Protocol described in IEEE 802.11e Draft 5.0. A direct link can also be established in a proprietary manner (without the cooperation of the Access Point) using techniques similar to those described in the invention "TECHNIQUE FOR ACHIEVING CONNECTIVITY BETWEEN TELECOMMUNICATION STATIONS" (Intersil patent docket 680-061US), based on establishing a simultaneous IBSS, or Ad-Hoc network, while a station is also connected to an Infrastructure wireless network (Access Point).

This invention has application in products implementing 802.11, Bluetooth, and other wireless LAN standards. The typical application would be in a wireless LAN client station, where the functions would be implemented in software running in the MAC controller, driver, or as an application in the host operating system. The wireless LAN client implementing this invention could be located in a computer, PDA, mobile phone, game, toy, or consumer electronic device.

Note that some references to "network location awareness" (particularly with respect to Windows XP) actually refer to a computer determining what kind of network a system is connected to (EG dialup, wireless, enterprise wired LAN, hotspot) and have nothing to do with physical, geographic location of the network device. Wireless LAN based location awareness systems are generally intended to provide user location information to a central administrator or network operator.

This invention describes a personal use of location information to notify the user when they are in proximity of a friend or associate. The objective is not to provide a precise, absolute location – only an indication of relative proximity. This invention can take advantage of other location awareness technologies (if available) to help in making that determination. This invention has unique and novel claims with respect to the user to user notification features, and the enabling of user to user direct data transfers. In addition, this invention provides novel claims in the techniques used to determine relative proximity of users in the absence of absolute location information.

The invention can work with or without support from the wireless network infrastructure. It can be supported from the wireless client only, or in some implementations, with support from a central server located anywhere on the Internet.

Features:

1) A system to provide notification to a user of other "nearby" users of a wireless LAN system, where nearby is defined as a wireless client associated to the same Access Point, the same ESS network of multiple Access Points, or within wireless signal range (even if not associated to the same AP or network). The other users would be pre-determined and represented as "list" of friends or colleagues.

2) A set of methods for determining the proximity of other users on a wireless LAN system. These methods include

- a) directly reading the MAC address of data packets from other users within signal range.
- b) Direct probing / polling. Wireless devices embodying this invention would periodically send out broadcast frames that would be identified by other users with the same software. Receiving a broadcast would result in a directed response back to the station sending the broadcast. This methods works for the similar case as in a) where the stations are in signal range. It allows faster discover in the case where one or both stations are not in active operation sending frames to the AP that could be identified by the other station. (methods a) and b) are well known techniques and not novel in themselves, but are listed for completeness)
- c) Server assisted locality identification: Assuming the users are associated with a wireless network providing Internet access, a centralized server on the Internet can assist in providing local network identification and proximity detection of other users. Wireless devices embodying this invention would connect to a central server, and upload information about their local network connection. This information would include the MAC address of the AP the client is currently associated with, and the SSID (service set identifier) of the network it is currently connected to. The central server would compare the connection information to the corresponding information from members of the user's list of "friends and colleagues". If there are any matches, the server would send a notification back to the user that a friend or colleague is in the vicinity on the current network. MAC addresses are globally unique numbers, so a match guarantees two users are really associated to the same Access Point. SSIDs are not globally unique, so the value of a matching SSID only is lower, but can still indicate two users on different access points of the same network.
- d) Network path resolution: A wireless device embodying this invention could perform a IP (Internet Protocol) traceroute to provide additional information to the server described in c). This traceroute information provides information about the networks between the wireless client and the central server (or other Internet host). The traceroute path provides value in two ways. First, it can provide a indication of relative degree of "closeness". If two users are connected to the same service provider, but not on the same local subnet, they might share a common router on the path back to the central server. An example might be two users in different terminals at an airport equipped with a wireless LAN infrastructure. A common network router in a traceroute path does not guarantee physical proximity, but there is frequently a correlation, due to the way networks are deployed and the way blocks of IP addresses are often assigned. The central server could report the possible proximity back to both users. The second value of the traceroute function is to prevent "false positive" proximity indications due to the common use of NAT (Network Address Translation) in wireless access and hotspots. Where low-cost wireless routers are use, there is a very high probability that a wireless user will be issued an IP address of the form 192.168.0.X. This private address space

provides no location information. However, the traceroute can identify the next router in the path, and identify a public IP address that the router is connecting to the internet with, then additional location information can be derived. Services are available that will provide location information (not necessarily very precise) for any IP address on the Internet.

3) A method for establishing peer-to-peer (or direct link) connection between users of wireless devices that are in wireless signal range.

a) The use of 802.11e Direct Link Protocol (DLP) is not novel in itself, but may be claimable as part of this overall invention. The use of 802.11e DLP requires that both the client and the Access Points support 802.11e and the DLP option.

b) The creation of a local peer-to-peer connection when one station is already connected to an infrastructure BSS is described in the invention "TECHNIQUE FOR ACHIEVING CONNECTIVITY BETWEEN TELECOMMUNICATION STATIONS" (Intersil patent docket 680-061US. That invention is oriented towards establishing connectivity between an 802.11-enabled PDA and a notebook, while the notebook is part of another infrastructure wireless network. This invention is slightly different, in that both stations desiring to set up an peer-to-peer connection are already connected to an infrastructure wireless network. Some aspects of 680-061US (such as the private IP services, DHCP, and address translation) would not be needed in for this invention, in the case where both of the peer-to-peer connecting wireless clients were already associated to the same wireless network. In the case where they were associated to a different wireless networks, techniques such as address translation or multiple IP stacks would be required. A discovery, setup, and negotiation protocol would need to be defined to manage the establishment of peer-to-peer connections under the various combinations of network connection scenarios for the two participating wireless devices.

c) The direct link connections would incorporate security mechanisms to authenticate the other user, and to provide privacy for the wireless data. In the server-assisted case, each party would obtain unique session keys from the server which could authenticate the other user, and provide keys for the peer-to-peer wireless connection. Even without server availability, pre-arranged (as part of the "friends" list creation) public and private keys could be used to authenticate the other user and encrypt the wireless traffic.

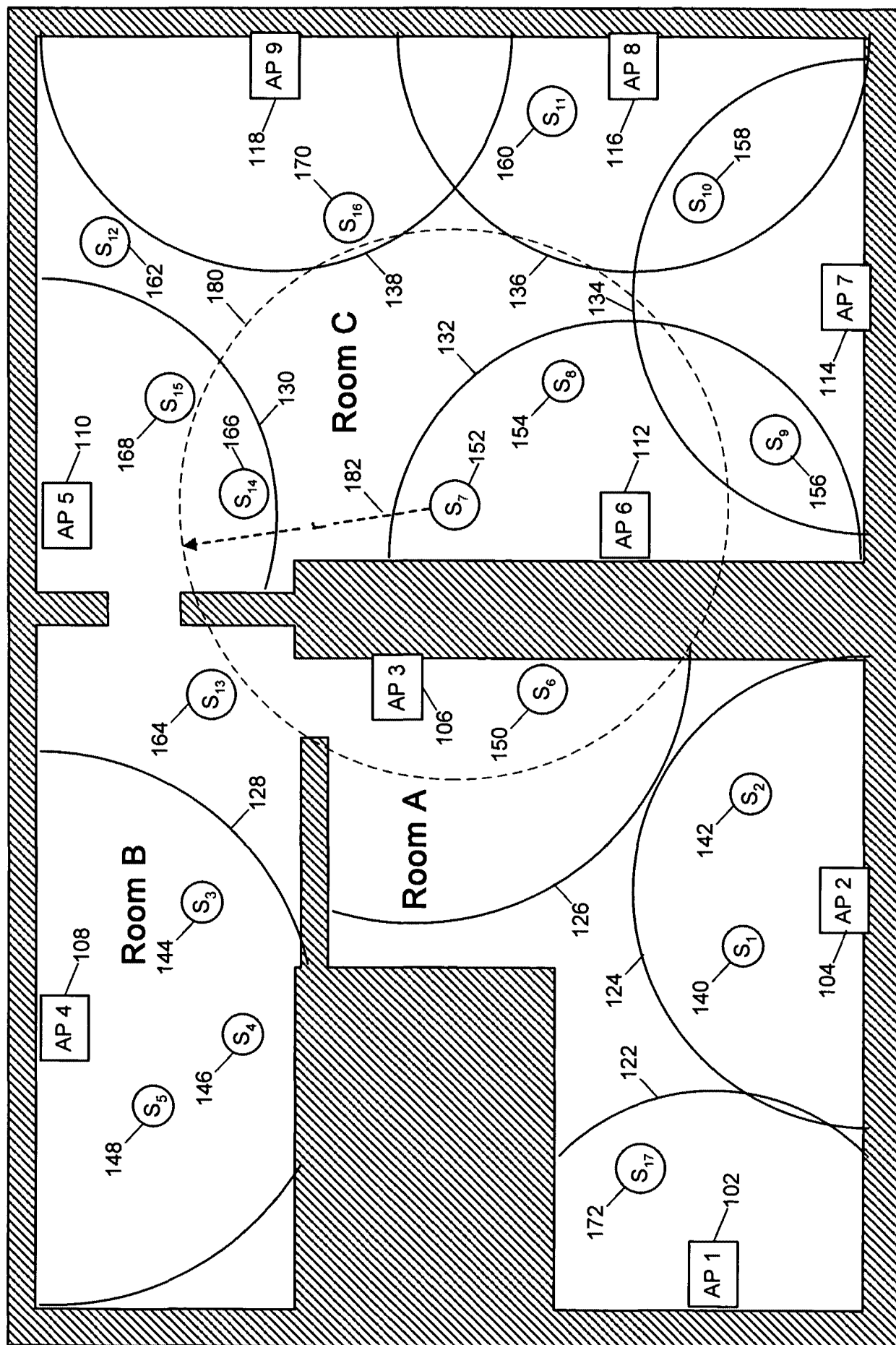


Fig. 1

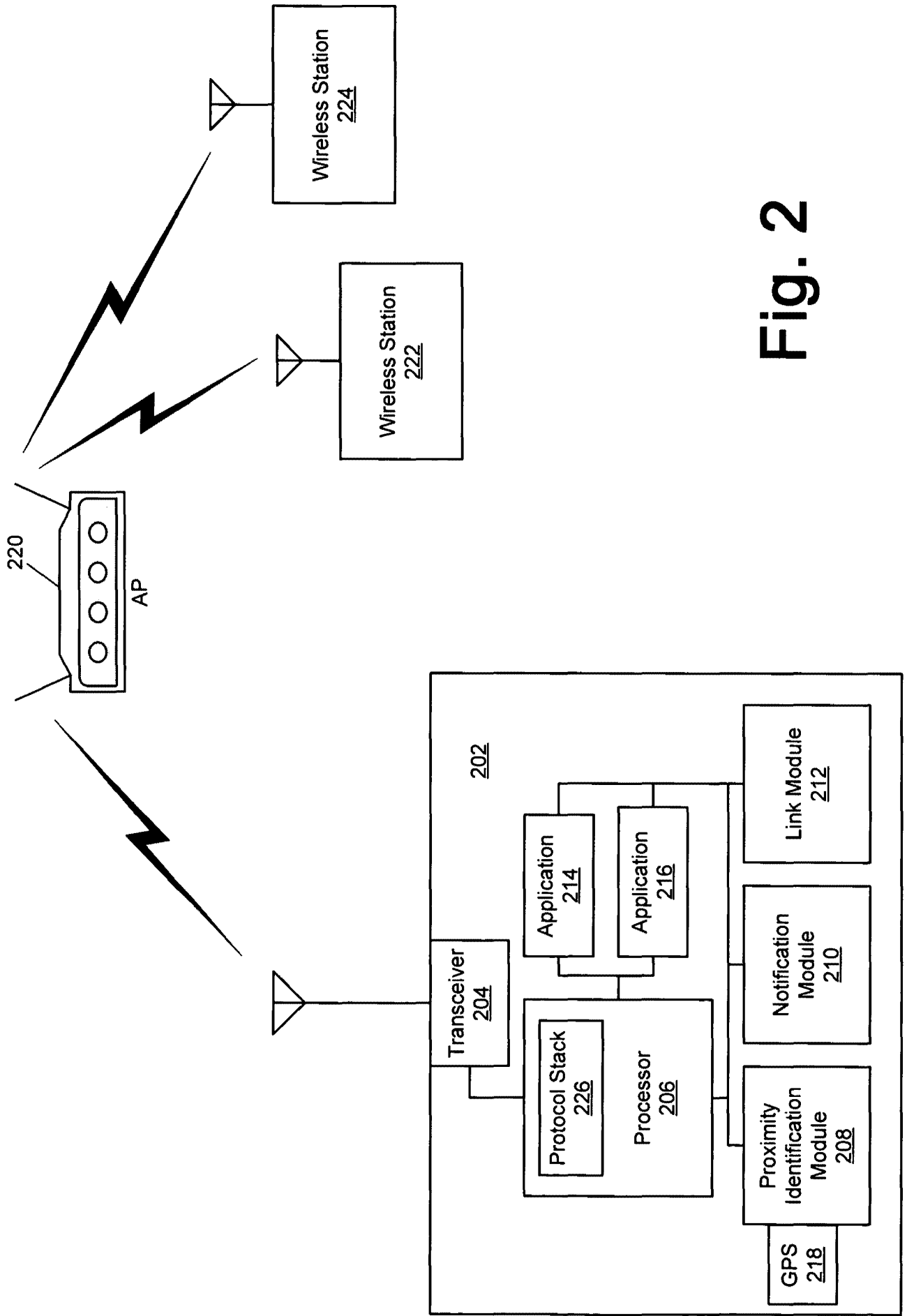


Fig. 2

FIG. 3

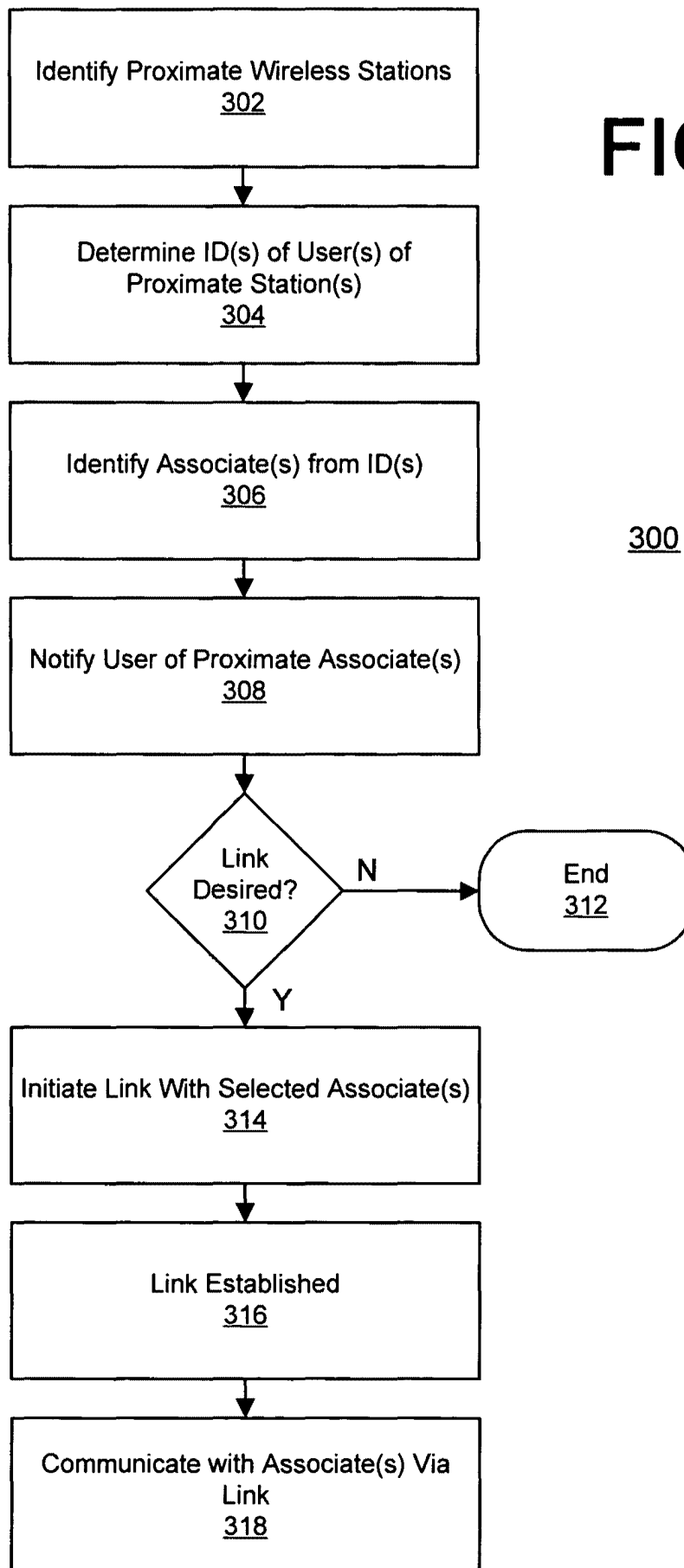
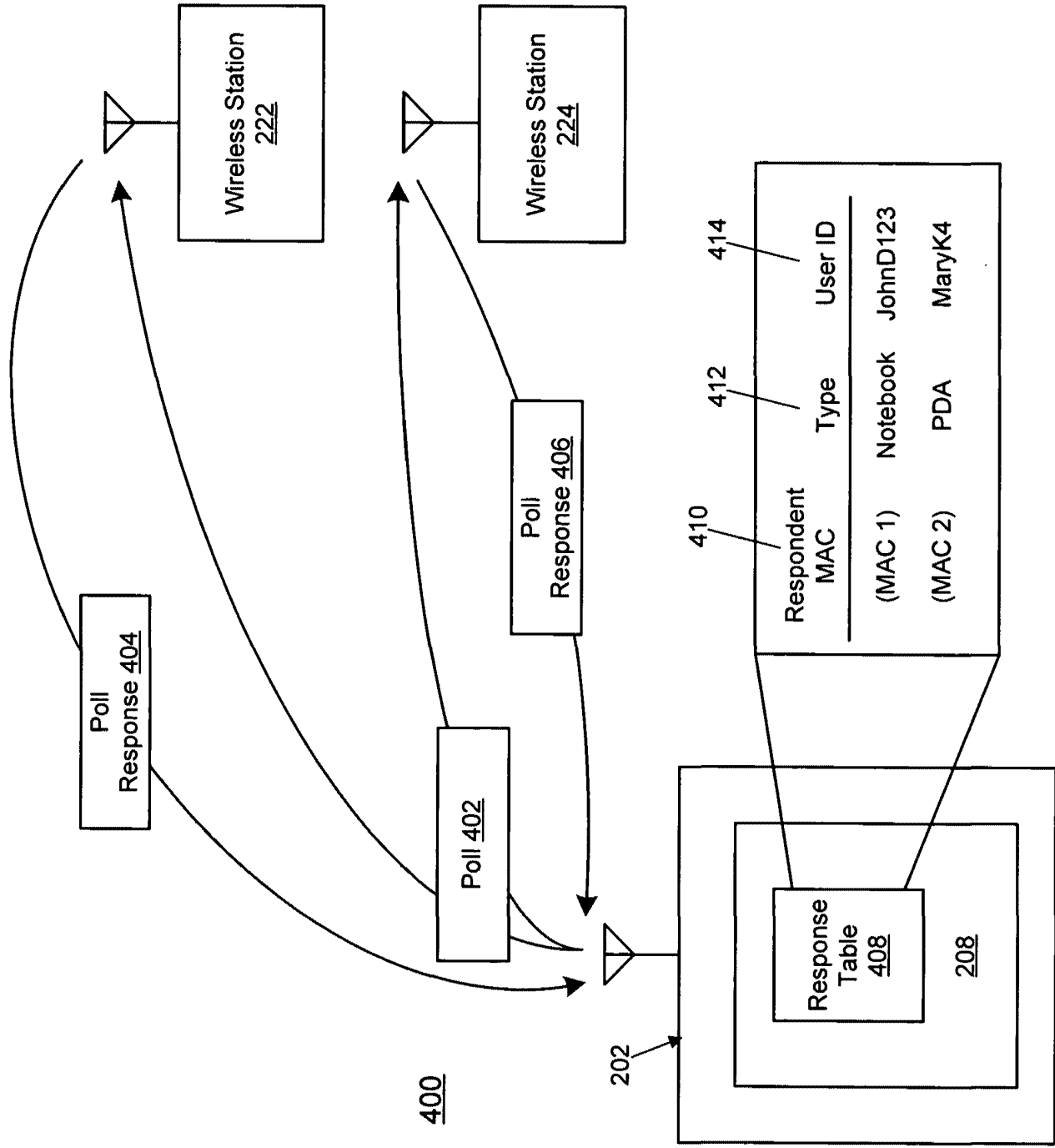


Fig. 4



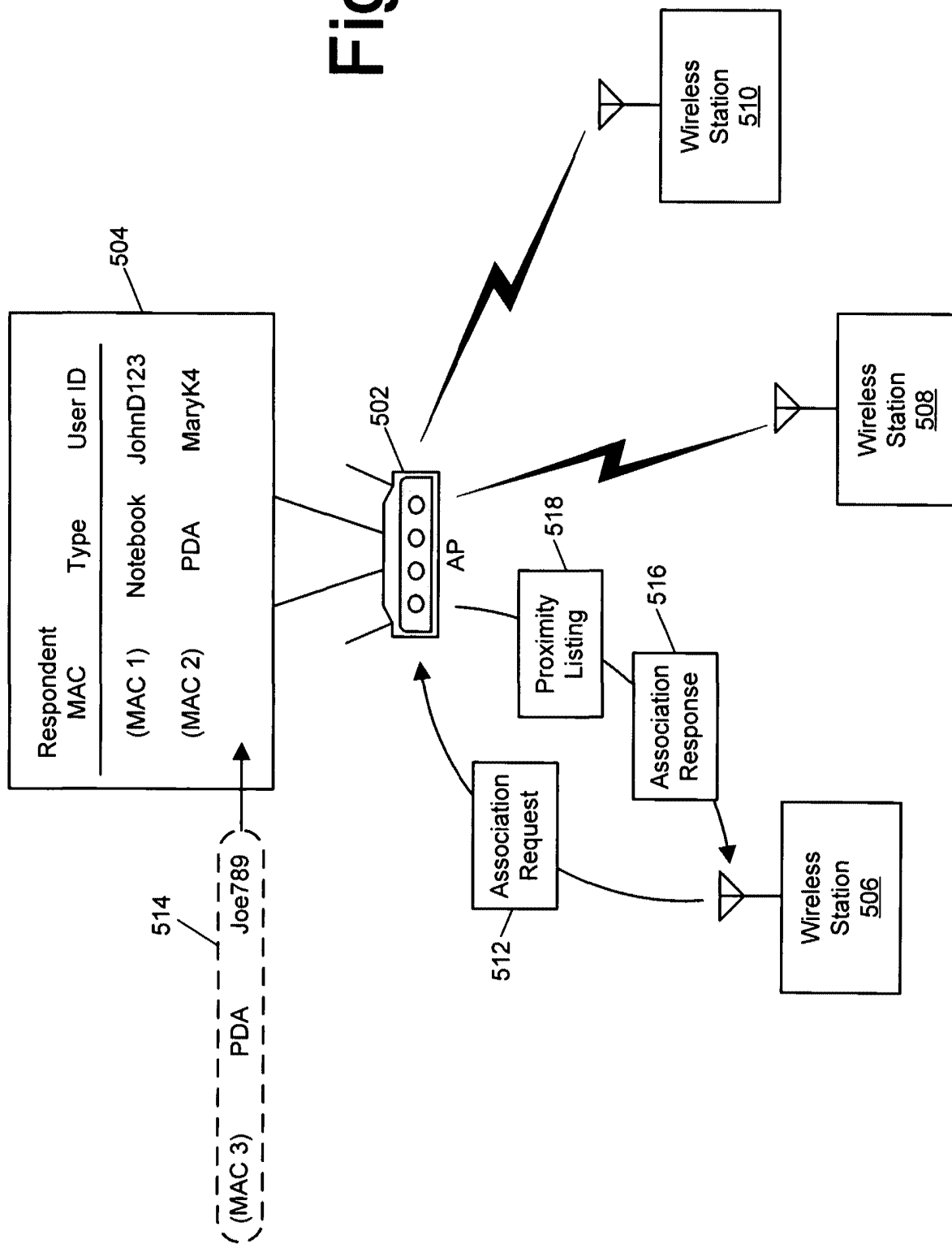


Fig. 5

Fig. 6

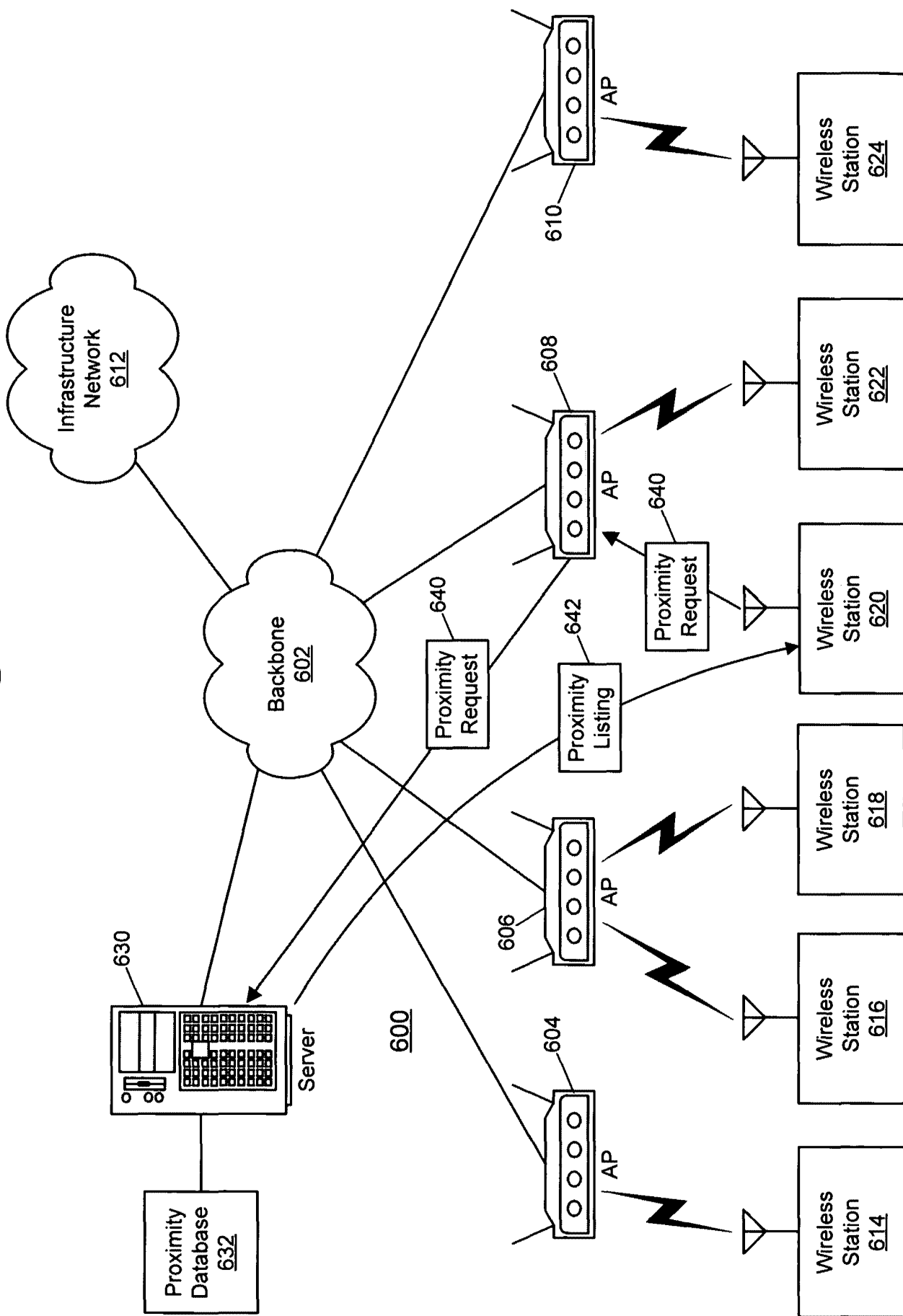
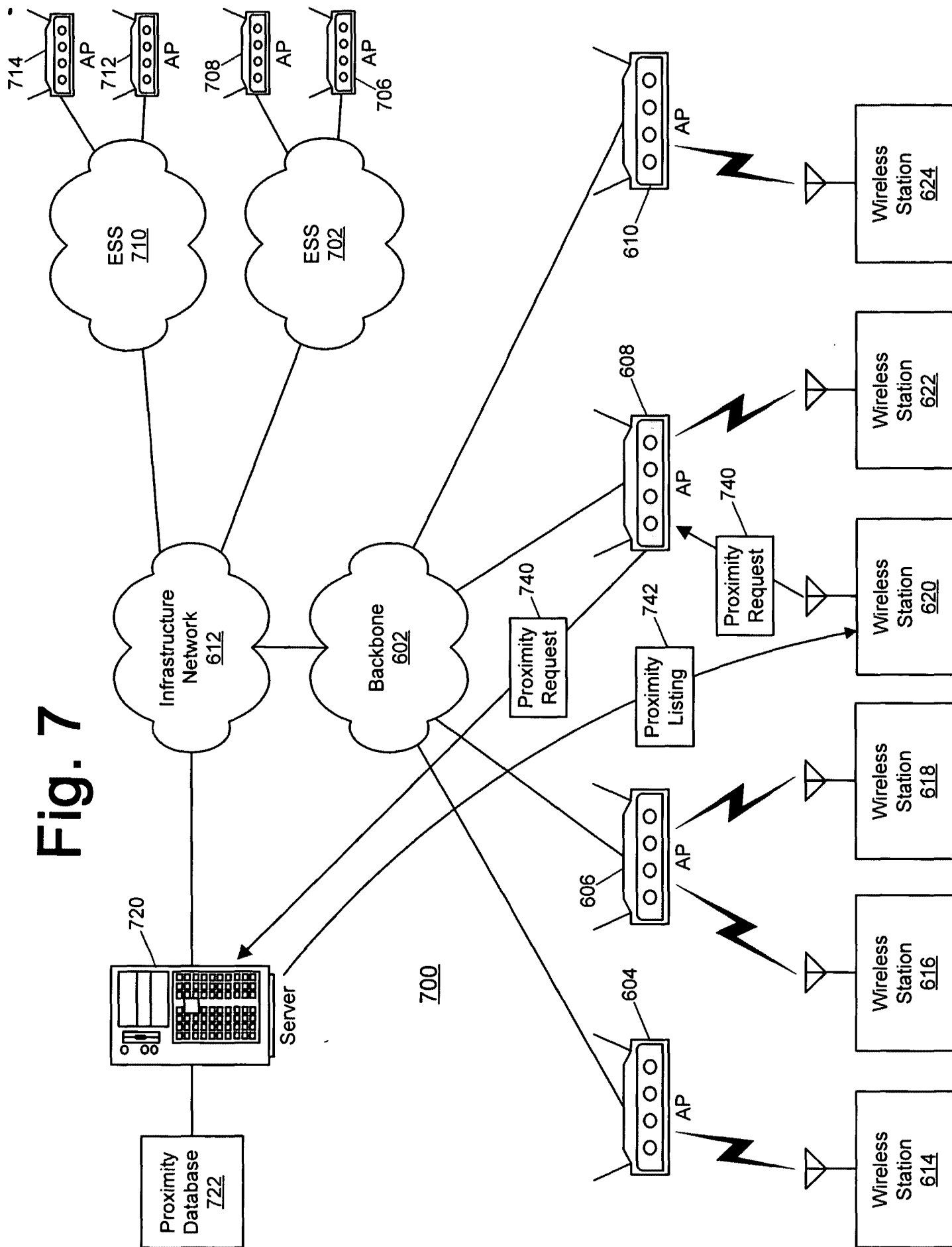


Fig. 7



MAC	AP	Type	User ID
(MAC 1)	1	PDA	(user 1)
(MAC 2)	2	Notebook	(user 2)
(MAC 3)	2	Workstation	(user 3)
(MAC 4)	3	PDA	(user 4)
(MAC 5)	3	Cell Phone	(user 5)
(MAC 6)	4	Notebook	(user 6)

Fig. 8

SSID	AP	Client
(SSID 1)	(AP MAC 1)	(MAC 1)
	(AP MAC 2)	(MAC 2)
		(MAC 3)
	(AP MAC 3)	(MAC 4)
	(AP MAC 4)	(MAC 5)
		(MAC 6)
(SSID 2)	(AP MAC 5)	...
	(AP MAC 6)	...
(SSID 3)	(AP MAC 7)	...
	(AP MAC 8)	...

Fig. 9

AP	MAC	Room
1	(MAC 1)	A
2	(MAC 2)	A
3	(MAC 3)	A
4	(MAC 4)	B
5	(MAC 5)	C
6	(MAC 6)	C
7	(MAC 7)	C
8	(MAC 8)	C
9	(MAC 9)	C

Fig. 10A

Room 1	Room 2	Proximity
A	B	1
B	C	1
A	C	2

Fig. 10B

MAC	Location
(MAC 1)	X1, Y1
(MAC 2)	X2, Y2
(MAC 3)	X3, Y3
(MAC 4)	X4, Y4
(MAC 5)	X5, Y5
(MAC 6)	X6, Y6
(MAC 7)	X7, Y7
(MAC 8)	X8, Y8
(MAC 9)	X9, Y9
(MAC 10)	X10, Y10
(MAC 11)	X11, Y11
(MAC 12)	X12, Y12
(MAC 13)	X13, Y13
(MAC 14)	X14, Y14
(MAC 15)	X15, Y15

Fig. 10C

Room	Boundary Description
A	xxxxxx
B	xxxxxx
C	xxxxxx

Fig. 10D

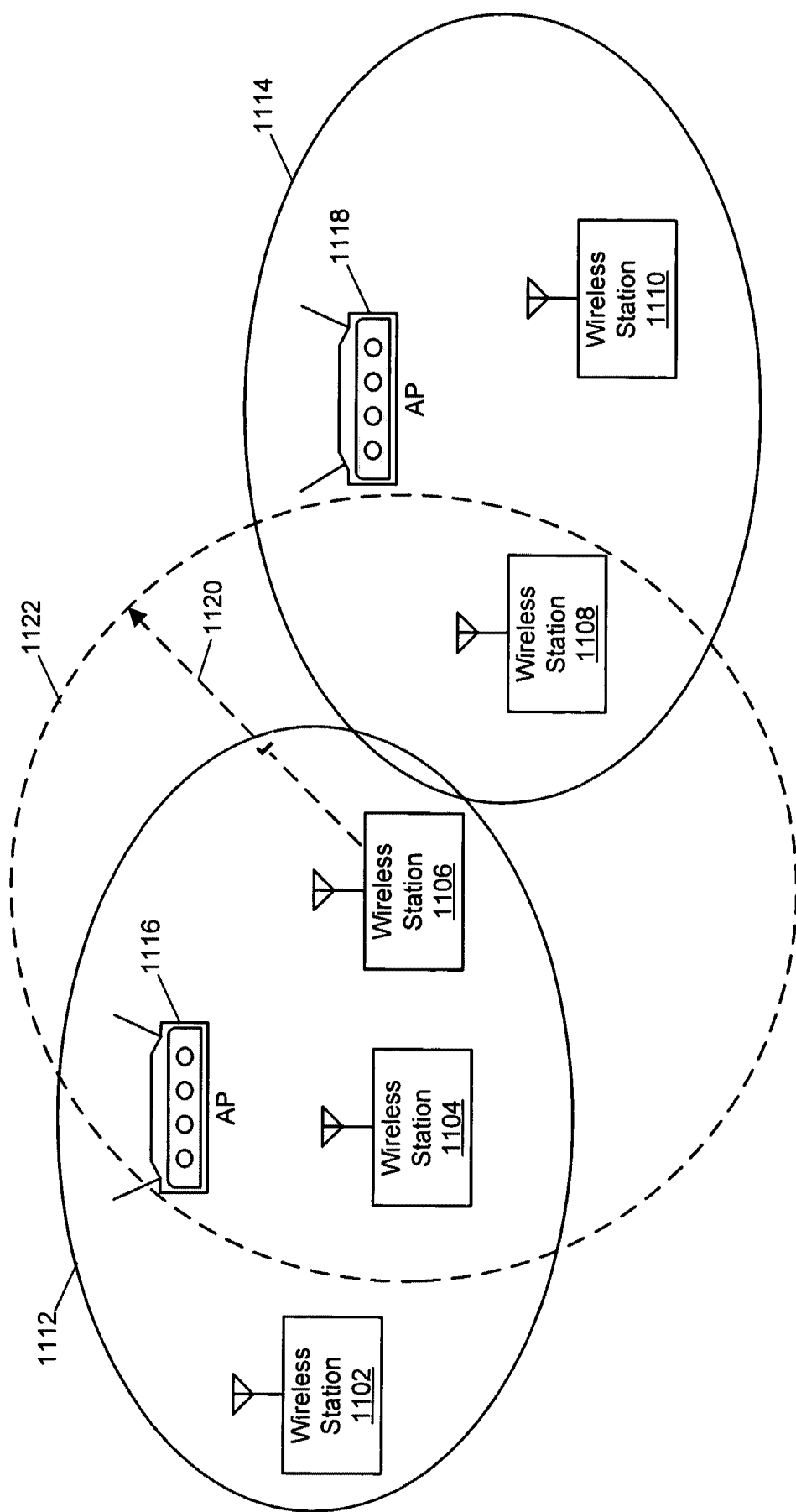


Fig. 11

Fig. 12A

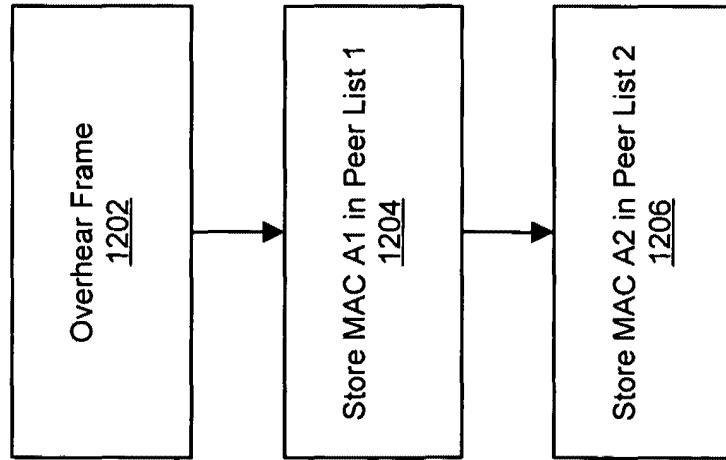


Fig. 12B

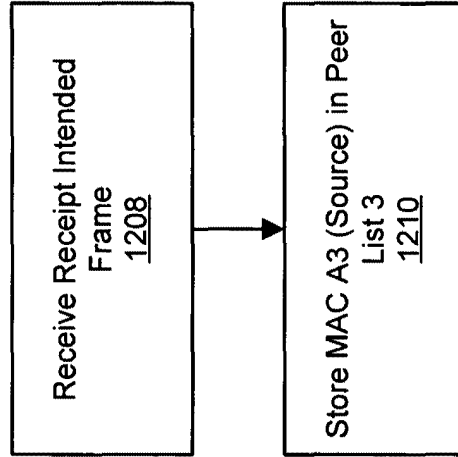


Fig. 12C

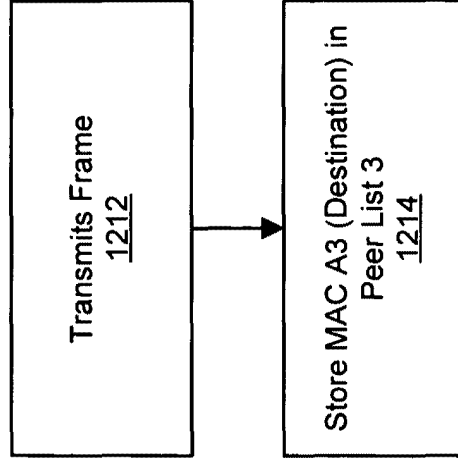


Fig. 13A

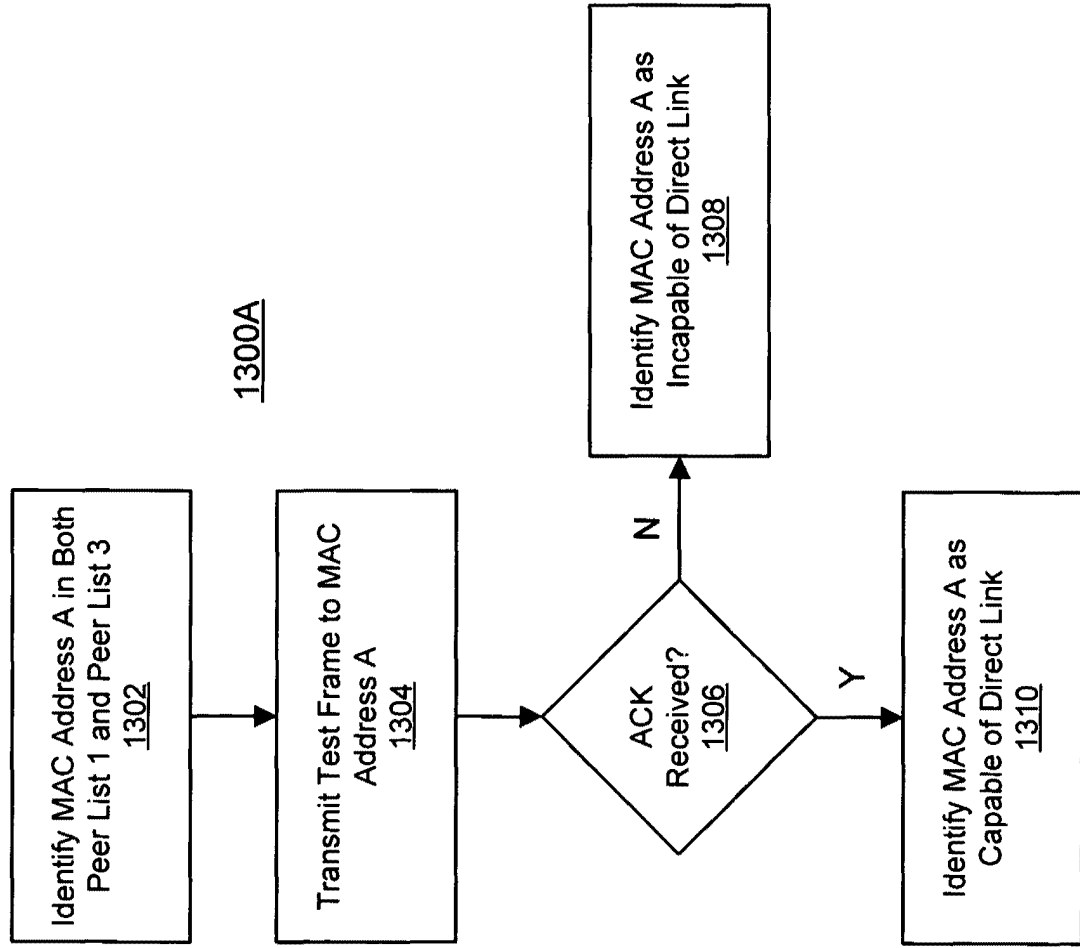


Fig. 13B

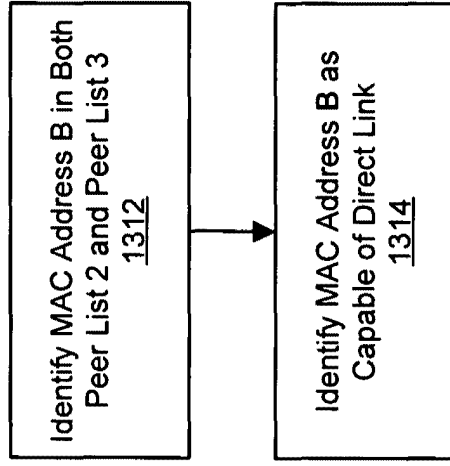
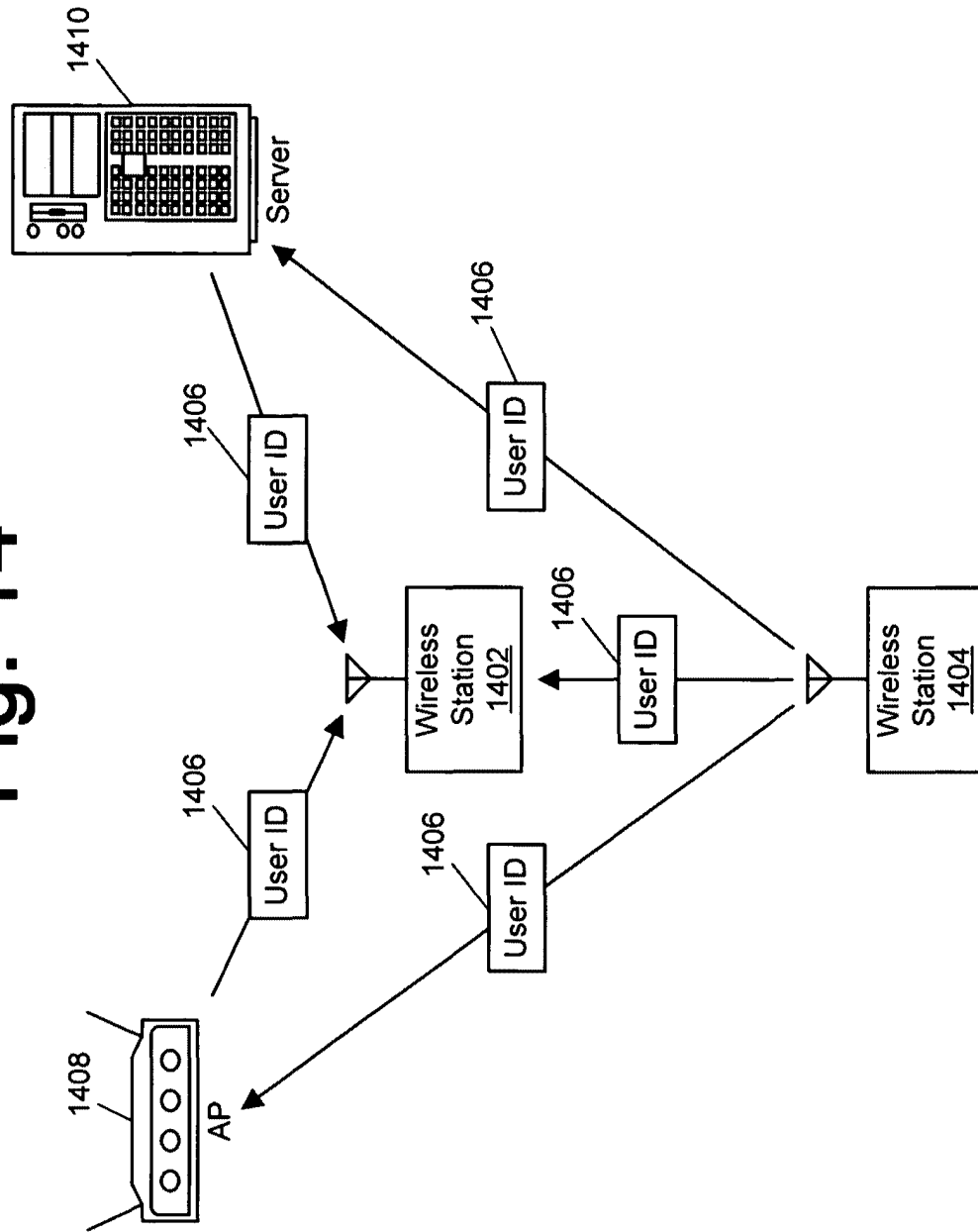


Fig. 14



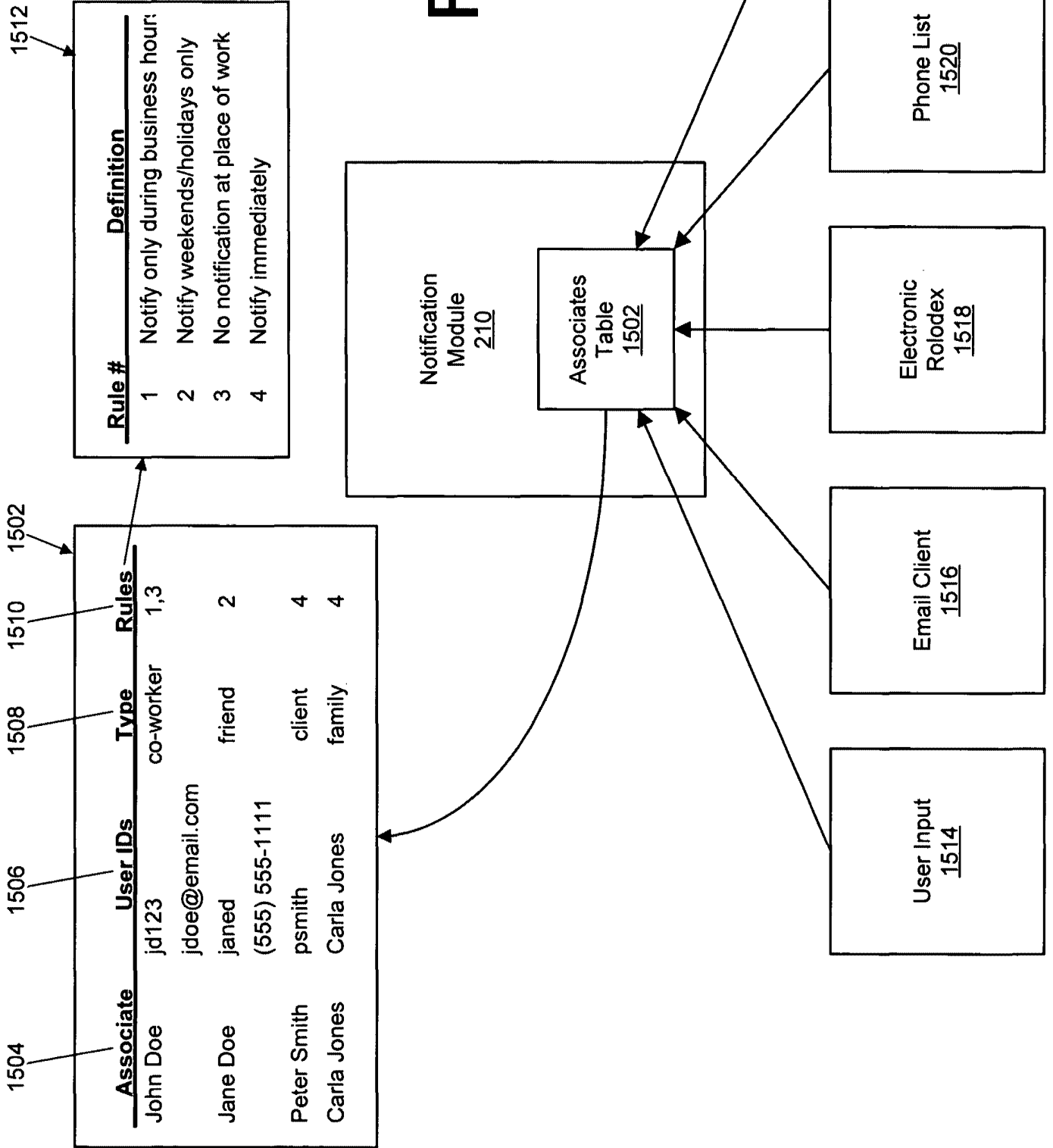


Fig. 15

Fig. 16

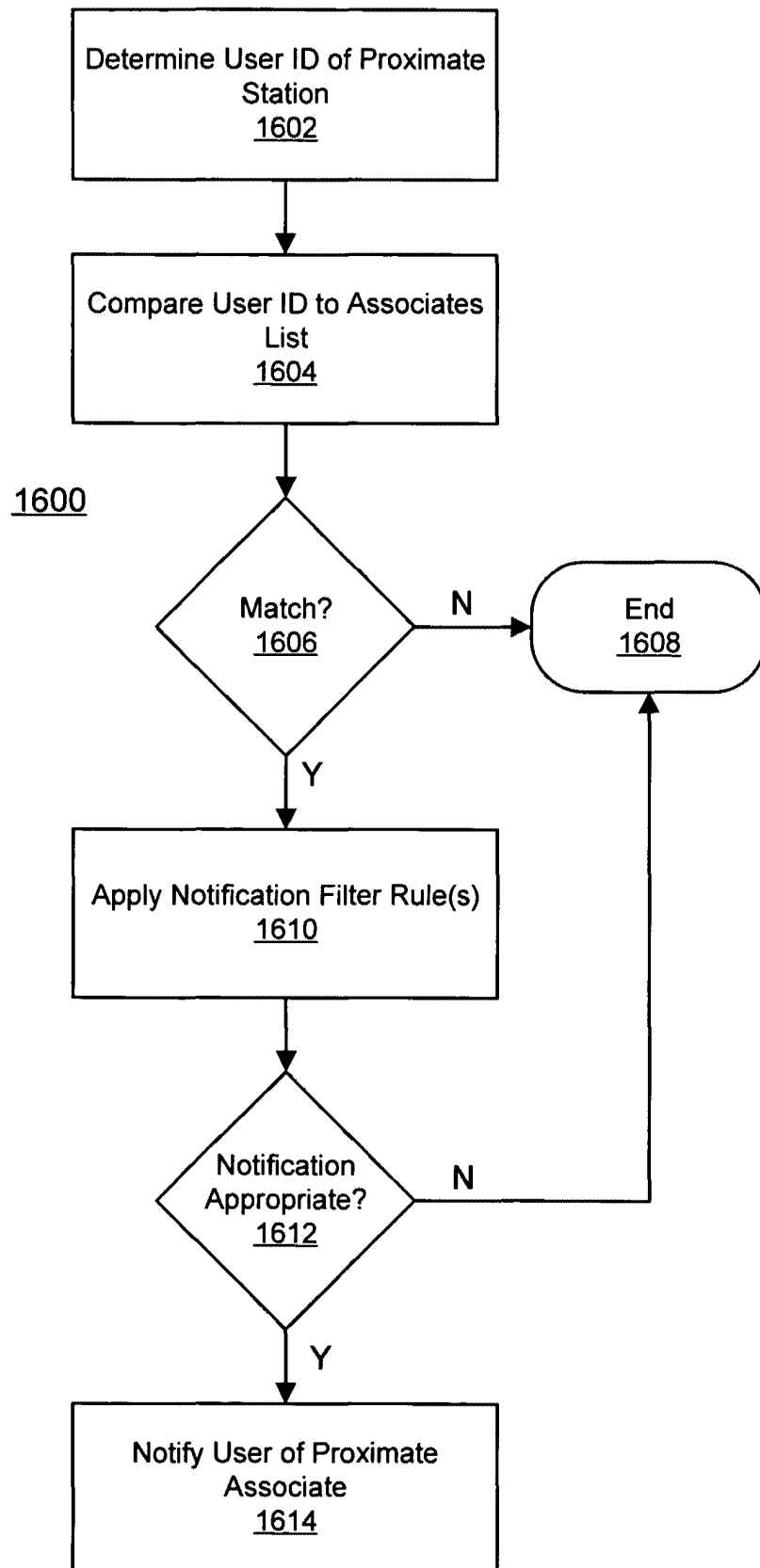
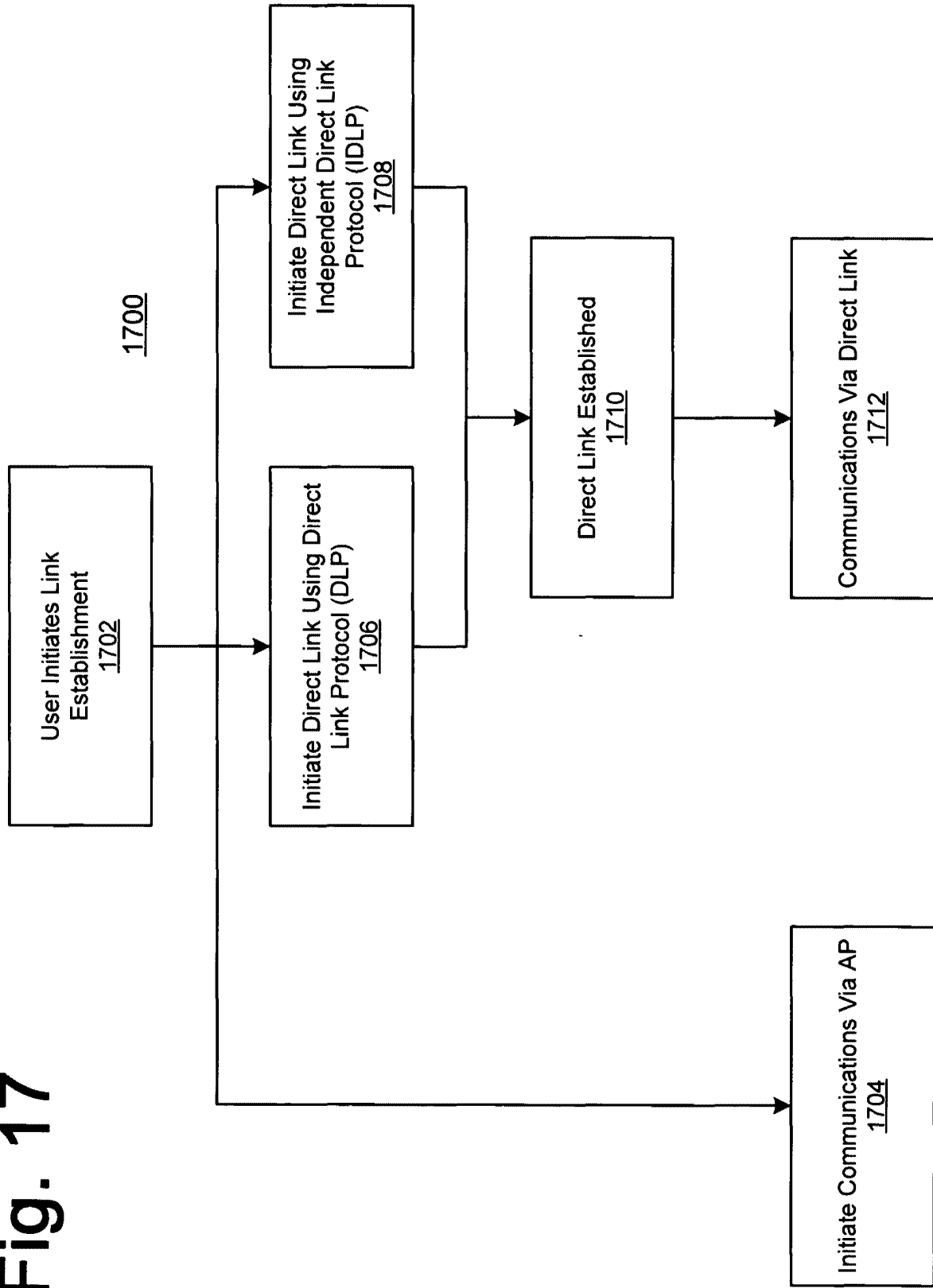


Fig. 17



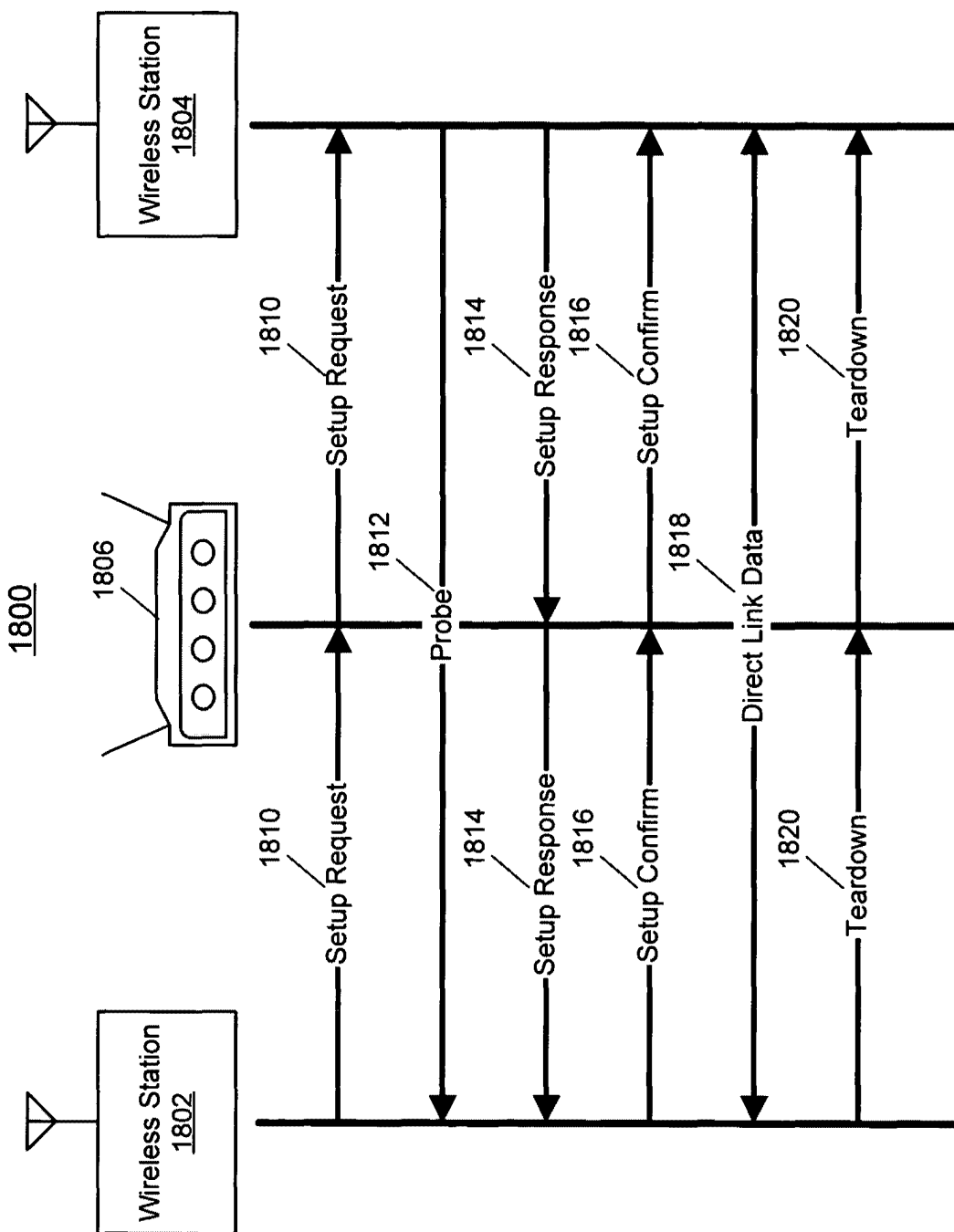


Fig. 18

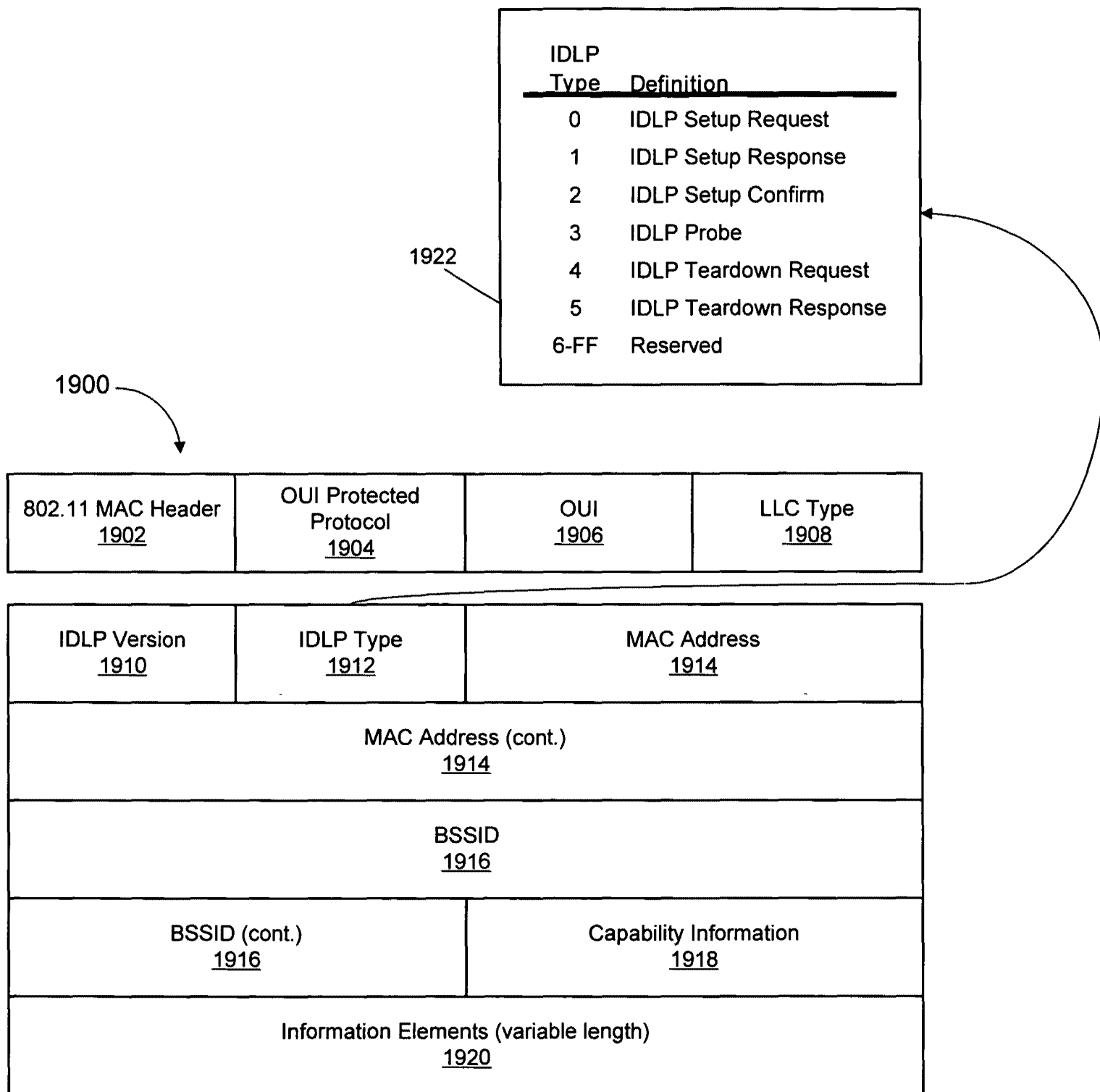


Fig. 19