

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
11 November 2004 (11.11.2004)

PCT

(10) International Publication Number
WO 2004/098214 A1

(51) International Patent Classification⁷: **H04Q 7/20**,
H04B 7/00

Dr. #2190, Sunnyvale, CA 94085 (US). **KAWAHARA, Toshio** [JP/US]; 20100 Pampas Ct., Saratoga, CA 95070 (US).

(21) International Application Number:
PCT/US2004/010390

(74) Agents: **BERNSTEIN, Frank** et al.; SUGHRUE MION, PLLC, 401 Castro Street, Suite 220, Mountain View, CA 94041-2007 (US).

(22) International Filing Date: 2 April 2004 (02.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/466,259 29 April 2003 (29.04.2003) US
60/470,228 13 May 2003 (13.05.2003) US

(71) Applicant (for all designated States except US): **DO-COMO COMMUNICATIONS LABORATORIES USA, INC.** [US/US]; 181 Metro Drive, Suite 300, San Jose, CA 95110 (US).

(72) Inventors; and

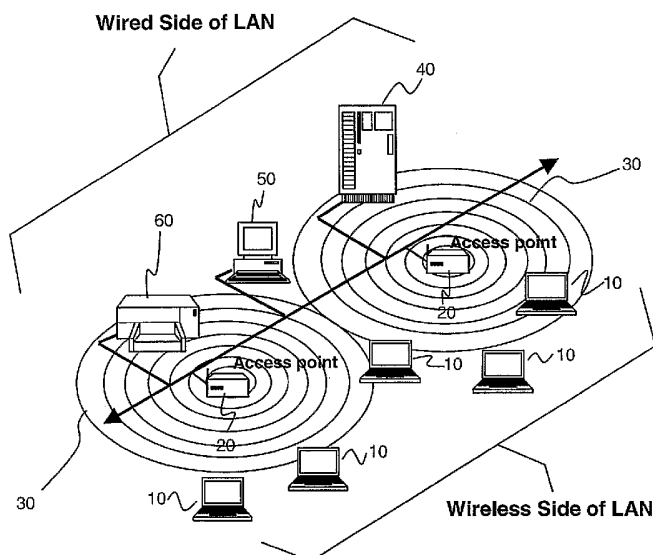
(75) Inventors/Applicants (for US only): **JEONG, Moo Ryong** [KR/US]; 305 Elan Village Lane, #206, San Jose, CA 95134 (US). **WATANABE, Fujio** [JP/US]; 1263 Lakeside

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: FAST ACTIVE SCANNING WIRELESS NETWORK APPARATUS AND METHOD



(57) Abstract: In a fast active scanning wireless network apparatus and method for quick determination of available access points (20), information about a candidate set of available access points (20) is obtained, and a candidate access point is identified from the candidate set. A mobile station (10) then queries the candidate access point with a probe request that designates the candidate access point as a sole responder. The probe request prevents other access points from contending for the medium of communication between the mobile station and the designated sole responder access point by excluding the attempt by other access points (20) to transmit probe responses. The apparatus and method thus increases the probability of a fast and successful probe request from the mobile station and subsequent response from the designated access point (20). The designated access point may also respond with a probe response of high priority, preventing intervention of communication.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

Published:

— *with international search report*

FAST ACTIVE SCANNING WIRELESS NETWORK APPARATUS AND METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of Provisional Application Nos. 60/466,259, filed April 29, 2003, and 60/470,228, filed May 13, 2003. The present application incorporates the disclosure of these provisional applications by reference.

FIELD OF THE INVENTION

[0002] This invention relates to a method, apparatus and system for fast active scanning of a wireless network, for instance, fast active scanning of those networks certified under one or more of the IEEE 802.11 wireless local area network (LAN) standards of interoperability, WPAN (Wireless Personal Area Networks), networks certified under one or more of the IEEE 802.16 and 802.16a standards, Bluetooth TM networks (including but not limited to IEEE 802.15.1 standard), HomeRF TM networks, HIPERLAN TM networks, IrDA TM networks and/or other wireless networks.

BACKGROUND OF THE INVENTION

[0003] Wireless networks generally include multiple access points for wireless connectivity to multiple mobile stations. Such connectivity allows a mobile station to communicate with any number of types of devices within a network, for instance, a mainframe, a server, a networked printer, another mobile station, and the like. Mobile

stations determine which network to join by scanning for available channels. Scanning may be either an active or passive on one or more radio channels.

[0004] Passive scanning is carried out by a mobile station simply listening for signals broadcast from access points attached to the network. Active scanning is performed when a mobile station actively broadcasts a probe request signal or the like. A probe request signal is meant to solicit a probe response signal from available access points, based on which the mobile station is then able to gain access to the network. The interchange of the probe request and probe response signals is generally referred to as a "handshake."

[0005] When a mobile station is moving out of range of one access point and potentially into range of another access point, a handoff between those access points occurs. Conventionally, such handoffs have been time consuming. Different problems can result from either of handshake or handoff latency, ranging from interruption of communication all the way to lack of communication between a mobile station and a network's access points.

[0006] For instance, communications interruptions can result from Transfer Control Protocol ("TCP") congestion-avoidance algorithms kicking-in because of TCP-imposed time limits, causing decreased throughput between mobile stations and the network. Such latency can cause serious deterioration in voice transmission quality, for example, when handshake latency causes voice service interruption time to exceed 35 msec. As explained in greater detail below, handshake latency can easily exceed permissible limits, potentially causing a total loss of communication.

[0007] Figure 1 is a diagrammatic example of a wireless local area network (“WLAN”), in which multiple mobile stations 10 wirelessly communicate with access points 20 via wireless signals 30. Access points 20 act as mediators between the mobile stations 10 and devices already connected to the network in either wired or wireless fashion (*e.g.*, a server 40, a computer 50, a networked printer 60, or other mobile stations).

[0008] In order to communicate with the network, the mobile station 10 first senses the wireless medium 30 to determine if another mobile station is transmitting over a particular channel. If the channel is determined not to be busy, the mobile station proceeds with an attempt to communicate with the network on that channel.

[0009] The mobile station’s attempt to communicate is orchestrated by, for example, a Distributed Coordination Function (“DCF”) which may determine using techniques, such as Carrier Sense Multiple Access with Collision Avoidance (“CSMA/CA”), when any number of mobile stations are operating within the network, as well as when those mobile stations should be permitted to transmit and receive frames over the wireless medium.

[0010] Using one or more algorithms in accordance with the DCF, the CSMA/CA requires that a gap of a specified duration (otherwise called an Interframe Space, or “IFS”) exists between all contiguous sequences of transmitted data. A transmitting device (whether an access point on the network or a mobile station) is required to ensure that the wireless medium is idle for a specific duration (the duration being specified by the type of IFS, as explained herein) prior to attempting to transmit. An IFS differs in length according to the priority of the frames being transmitted.

[0011] For example, a Short Interframe Space (“SIFS”), which is the shortest interframe gap, is employed when a transmitting device has seized a channel on the wireless medium and needs to keep the channel for the duration of the frame exchange to be performed. One such SIFS example is the acknowledgement frame (otherwise known as the “ACK signal” or “ACK frame”). Using the smallest gap between transmissions within the frame exchange sequence prevents other transmitting devices (whether access points or mobile stations) from attempting to use the seized channel because the other transmitting devices have to wait for the channel to be idle for a period of time that is longer than the SIFS period. Accordingly, the DCF and CSMA/CA provide priority to the current frame/data exchange sequence over attempts by other transmitting devices to transmit new data exchange sequences over the same channel on the wireless medium.

[0012] Another example of an interframe space is the Point Interframe Space (or “PIFS”). A PIFS is only used by transmitting devices operating under a Point Coordination Function (“PCF”) to gain priority access to a channel on the wireless medium at the start of a contended free period. A PIFS gap is longer than a SIFS gap.

[0013] A Distributed Interframe Space (“DIFS”), which is longer than a PIFS gap, is used by transmitting devices operating under the Distributed Coordination Function (“DCF”) and CSMA/CA to transmit data exchange frames and management frames. Management frames include such frames as probe requests and probe responses, which are used for communications handshakes between a mobile station and an access point.

[0014] When transmitting under the DCF, if a mobile station determines that a channel on the wireless medium is busy, the mobile station delays transmitting any new frames

until the end of the current transmission. After this delay, or before attempting to transmit immediately following a successful transmission, the station selects a random backoff interval and decrements a backoff interval counter while the channel on the wireless medium is idle. The station reattempts transmission when the backoff interval counter reaches zero.

[0015] Further general parameters of the various IEEE 802.11 WLAN standards concern frame receptions/acknowledgments, physical and virtual carrier sense functions, and frame types. These parameters provide transport functions that ensure an intended receiver receives the total amount of bits and bytes in a data message correctly. These further parameters are generally discussed below with respect to Figures 2 - 7.

[0016] In Figure 2, the basic field of a probe request signal may include the following: frame control, duration, destination address ("DA"), source address ("SA"), basic service set identification ("BSSID"), sequence control, service set identification ("SSID"), supported rates, and frame check sequence ("FCS"). Of these fields, the first six (frame control, duration, DA, SA, BSSID, and Sequence Control) are part of what is known as the Media Access Control (or "MAC") header for controlling transmission over the wireless medium. The next two fields (SSID and supported rates) constitute the probe request body. The final field (FCS) is used for error-detection.

[0017] The MAC header derives from the data link layer (otherwise known as the Media Access Control layer, or "MAC" layer) of the network. This layer provides a virtual carrier-sense mechanism (also known as a network allocation vector, or "NAV"), for

maintaining a prediction of future traffic on the medium based on duration information that is available in the MAC headers of all transmitted information, with few exceptions.

[0018] The network may include a physical layer for providing a physical carrier-sense mechanism, which is based on energy detection in the wireless medium. In combination, the physical and virtual carrier-sense mechanisms help to determine the state of the wireless medium.

[0019] When attempting to communicate, mobile stations send probe request signals (including the MAC header) to scan the area for an existing network channel, and to solicit a probe response from a network access point ("AP"). Receiving APs use the probe request body (including the SSID and supported rates fields) to determine whether the mobile station can join the network. The mobile station desirably supports the data rates required by the AP, and indicates a desire to join any network or the network identified by the SSID.

[0020] Further, as noted above, general receiving rules under the 802.11 standards include a mobile station using a DA (destination address) field to perform address matching for receiving decisions. In the case of the DA field containing a group address (*e.g.*, a broadcast address) when the field is other than a beacon field, the BSSID must be validated. That is, the BSSID field must have the same BSSID as the recipient. The BSSID field can be the broadcast BSSID if the field is a probe request. All transmitting devices (including APs and mobile stations) receiving data or management fields with a DA field other than a group address, respond to the received data or management fields with an acknowledgement signal (or "ACK" signal) transmitted with a SIFS deferral.

However, if received fields have a group address in the DA field, ACK fields are not transmitted.

[0021] Figure 3 is a diagram showing commonly incorporated bits that make up the control field of a probe request. Type bits (B2, B3) and subtype bits (B4 - B7) of the control field are used for identification of the field type. Table 1 provides examples of valid type and subtype combinations as used in the field control field of the probe request signal.

Table 1 Examples of Valid Type and Subtype Combinations

Type Value B3 B2	Type description	Subtype value B7 B6 B5 B4	Subtype description
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1101	Action
00	Management	1110-1111	Reserved
01	Control	1101	Acknowledgement (ACK)

[0022] Figure 4 shows the basic fields of a probe response signal, including a MAC header (for instance those MAC header fields described above in relation to the probe request signal) and a frame body. The frame body includes a timestamp, a beacon interval, capability information, the SSID, supported rates, data set parameters ("DS" parameters), control frame parameters ("CF" parameters) and frame check sequence (FCS).

[0023] The probe response comprises fields for informing the mobile station transmitting the probe request of the network's characteristics, enabling the mobile station to match parameters so as to be able to join the network. Similarly to the fields of a probe request,

type bits (B2, B3) and subtype bits (B4 - B7) of the probe response's frame control field identify the frame type. Table 1 provides examples of valid type and subtype combinations as used in the frame control field of the probe response signal.

[0024] Figure 5 shows the fields of the acknowledgement (or "ACK") signal. ACK signals are used to send positive acknowledgments in response to received frames. Similarly to the fields of a probe request and probe response, type bits (B2, B3) and subtype bits (B4 - B7) of the ACK's frame control field identify the frame type. Table 1 provides examples of valid type and subtype combinations as used in the frame control field of the ACK signal.

[0025] Figure 6 is a flowchart depicting the probe request portion of a handshake when scanning a network for available channels. The mobile station begins by discerning whether there are any unscanned channels in the network. If all channels have been scanned under the Distributed Coordination Function, the process is complete.

[0026] When there are unscanned channels, the mobile station transmits a probe request to a selected channel while simultaneously clearing and starting a probe timer clock (also known as "ProbeTimer"). The mobile station then senses the wireless medium to determine if the medium is busy until a minimum channel time is reached (the minimum channel time is also known as "MinChannelTime").

[0027] If the wireless medium is not busy during MinChannelTime, the channel is marked as scanned and the mobile station returns to querying whether there are any unscanned channels in the network. If all channels have been scanned under the Distributed Coordination Function, the process is complete. If any unscanned channels

remain, the mobile station transmits another probe request to a selected channel while simultaneously clearing and starting the ProbeTimer clock. The mobile station then senses the wireless medium to determine if the medium is busy until MinChannelTime is reached.

[0028] If the wireless medium is busy during MinChannelTime, then the station waits until the ProbeTimer clock signal reaches a maximum channel time (also known as the "MaxChannelTime" signal). Additionally, if any unicast frame is received at the mobile station, the unicast frame is responded to with an acknowledgement signal (also known as an "ACK" signal) from the mobile station.

[0029] When the MaxChannelTime is reached, any received probe responses are processed, and the probed channel is marked as scanned. The process of Figure 6 continues until all unscanned channels have been scanned.

[0030] Figure 7 is a flowchart showing the procedure used by access points (APs) for sending out a probe response in answer to a received probe request signal. Proper probe request signals include a broadcast destination designated by the destination address ("DA") field, a broadcast BSSID, and probe request fields that satisfy the particular reception rules for the particular access points ("APs") receiving the probe request. On receiving probe request fields, the APs respond with a probe response only if the SSID in the probe request is the broadcast SSID, or if the SSID in the probe request matches the specific SSID of a particular AP. Probe response frames (for example, those response frames with the characteristics as described above in relation to Figure 4) are sent as

directed frames to the address of the mobile station that generated the probe request. On receipt, the mobile station acknowledges them with an ACK signal.

[0031] If a probe response is not acknowledged with an ACK signal, the probe response is retransmitted for a predetermined number of attempts (the limit on number of retransmission attempts is also known as the RetransmissionLimit). The probe response follows the normal rules of the DCF (as previously described). APs transmitting a probe response are continuously maintained in an awake state, and respond to all probe requests meeting the above-noted criteria.

[0032] In Figure 7, a counter (for counting the number of attempts before an ACK signal is received in response to a transmitted probe response) is cleared at the beginning of the process. Then, received probe requests are checked to see whether the request's SSID is the broadcast SSID, or whether the SSID of the probe request matches the AP's SSID. If neither of these criteria is met, a probe response is not sent, and the process ends. If either of these criteria is met, the counter is checked to see whether the retransmission limit is less than the predetermined retransmission limit. If the retransmission limit has been reached, an additional probe response is not sent, and the process ends.

[0033] If the retransmission limit has not been reached, then a probe response is sent under the normal rules of DCF. The AP then waits for reception of an acknowledgement ("ACK") signal. If the ACK signal is received before an acknowledgement timeout ("AckTimeOut"), then the process is complete. If an ACK signal is not received prior to the AckTimeOut timing out, the counter is incremented and the process begins again with the comparison of the retransmission limit to the counter value, as described above, until

the process has completed with either the RetransmissionLimit being reached, or reception of an ACK signal before the AckTimeOut timing out.

[0034]

Figure 8 shows an example of an overall handshake between a mobile station and an AP, from initial probe request to subsequent probe response and acknowledgement signal transmission. In Figure 8, a first mobile station ("STA 1") is scanning for availability of a specific channel on a network, for example, channel 1. STA 1 contends for the medium of channel 1 under the basic access rules of DCF by transmitting a probe request signal with a broadcast destination address and broadcast BSSID. Since the probe request has been broadcast, any APs in the physical transmission area of the probe request that are using channel 1 will receive the probe request signal and will attempt to respond with their own probe response signals. For instance, AP 1 and AP 2 shown in Figure 8 will each attempt to respond with a probe response.

[0035]

When AP 1 and AP 2 transmit their own probe responses, AP 1 and AP 2 contend for the medium under the basic access rules of the DCF, as explained above. Further, AP 1 and AP 2 are also contending with other transmitting devices (*e.g.*, STA 2 as shown in Figure 8) attempting to send their own frames under the DCF. Frames thus colliding are known to potentially cancel one another out, or to cancel one or the other out.

[0036]

A mobile station that has sent a probe request frame determines the availability of the APs based on the medium status as reflected by the receipt of probe responses within the minimum channel time (also known as the MinChannelTime). A probe timer (also known as "ProbTimer") tracks the time for response to the probe request. If the wireless

medium is idle until the ProbTimer reaches MinChannelTime, the mobile station considers that no AP is available, as reflected by cases 5 and 7 in Table 2.

Table 2 Determination of AP Availability Through Probing

	Availability of AP	Receipt of Probe Request	Medium busy during MinChannelTime	Transmission of Probe Response during MaxChannelTime	Receipt of Probe Response	Determined Availability of AP	Judgment Correctness
Case 1	O	O	O	O	O	O	O
Case 2	O	O	O	O	X	X	X
Case 3	O	O	O	X	X	X	X
Case 4	O	X	O	X	X	X	X
Case 5	O	O/X	X	O/X	X	X	X
Case 6	X	X	O	X	X	X	O
Case 7	X	X	X	X	X	X	O

[0037] Conversely, if the wireless medium is not idle as determined by receipt of a probe response within the MinChannelTime period, the AP having sent the probe response is considered as available to serve the mobile station (for instance, case 1 of Table 2). Otherwise (as shown by cases 2, 3, 4, and 6 of Table 2), the mobile station considers that no APs are available. However, the judgment that no AP is available is not always correct, as explained below.

[0038] In Table 2, correct judgment is reflected by cases 1, 6 and 7. In case 1, the AP is available and successful receipt of a probe response signal verifies this. In case 6, no AP is available. That is, either the AP or mobile station are out of the physical transmission area and either the probe request or probe response cannot be delivered to the recipient. This fact is derived from a failure to receive a probe response within the time limit of MaxChannelTime.

[0039] In case 7, no AP is available. That is, either the AP or mobile station are out of the physical transmission area and there fails to be another active station transmitting in the vicinity. MinChannelTime thus expires without the mobile station detecting the wireless medium as busy.

[0040] Further in Table 2, incorrect judgment is reflected in cases 2, 3, 4 and 5. In case 2, the probe request was received correctly, and the probe response was sent before expiration of MaxChannelTime. However, the mobile station could not receive the probe request correctly. Reasons why this may occur include the probe response signal colliding with frame transmissions of other stations or other APs. In case 3, the probe request has also been received correctly, but the probe response signal cannot be sent prior to MaxChannelTime expiring. This may be due to the AP not being able to get a timely transmission opportunity for a probe response, or because of medium contention with other stations or APs, or as a result of other data frames that precede the probe response in the transmission queue. In case 4, the AP could not receive the probe request correctly. The probe request could have collided with the frame transmissions of other mobile stations or APs. In case 5, MinChannelTime has been set to an improper value that is smaller than is actually required.

[0041] In cases 2 through 5 of Table 2, the decision that no APs are available is incorrect. A scanning mobile station in conventional scanning mode is thus provided three options for handling these problems: (1) use of a larger MinChannelTime, (2) use of a larger MaxChannelTime, or (3) retransmission of the probe request signal.

[0042] In any of the above-three options, an increase in scanning time is traded for the associated increase in accuracy. The problem of handshake latency resulting from any of the above-three options is only multiplied by the plurality of channels to be scanned, as there typically is more than one channel to be scanned in a wireless network. Conventional methods are accordingly extremely inefficient in terms of scanning time, the result being high handshake latency. As explained above, problems resulting from high handshake latency vary from mere interruption of communication all the way to utter non-communication between a mobile station and a network's access points.

SUMMARY OF THE INVENTION

[0043] Therefore, one feature of the present invention provides a method, network and system for fast active scanning of a wireless network, including collecting candidate access point information that differentiates between candidate access points which are most likely to provide communication with wireless stations in the network and candidate access points which are not; and transmitting the candidate access point information. It is also a feature of the present invention to select, from the candidate access point information, the candidate access points that have been differentiated as most likely to provide communication; and transmitting the differentiated candidate access point information.

[0044] It is a further feature of the present invention to scan, with a wireless station, the candidate access points that have been differentiated as most likely to provide communication. It is yet a further feature of the present invention that the scanning of

candidate access points includes the wireless station transmitting a probe request for a specified candidate access point chosen from among the candidate access points differentiated as most likely to provide communication with the network.

[0045] Additional features of the present invention are evident from the associated drawings and in the Detailed Description of Embodiments section, below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] The invention, both as to its organization and manner of operation, may be further understood by reference to the drawings that include Figures 1 - 27, taken in connection with the following detailed description.

[0047] Fig. 1 is an illustration of a wireless local area network;

[0048] Fig. 2 is an example of the basic fields included in a probe request signal;

[0049] Fig. 3 is a diagram showing commonly incorporated bits that make up the control field of a probe request;

[0050] Fig. 4 is an example of the basic fields included a probe response signal;

[0051] Fig. 5 is an example of the basic fields included in an acknowledgement signal;

[0052] Fig. 6 is a flowchart which shows the basic procedure of sending probe request signals;

[0053] Fig. 7 is a flowchart which shows the basic procedure of sending probe response signals;

- [0054] Fig. 8 is a temporal illustration showing a handshake between a mobile station and an access point on a wireless network, including sending a probe request, a probe response and acknowledgement signals;
- [0055] Fig. 9 depicts fields of candidate access point ("CAP") information;
- [0056] Fig. 10 depicts bit-frame information for the scanning capability of a typical AP;
- [0057] Fig. 11 depicts an AP with a bit assignment for B8 that indicates that the AP is provided with the fast active scanning of the instant invention;
- [0058] Fig. 12 depicts a neighborhood graph showing the relationship of each AP to the other;
- [0059] Fig. 13 is a flowchart that depicts a first embodiment of the instant invention;
- [0060] Fig. 14 depicts an exchange of frames in a handshake according to the first embodiment;
- [0061] Fig. 15 is a flowchart that depicts a second embodiment of the instant invention;
- [0062] Fig. 16 depicts an exchange of frames in a handshake according to the second embodiment;
- [0063] Fig. 17 is a flowchart showing the procedure that a CAP follows in the second embodiment after reception of a probe request;
- [0064] Fig. 18 is a flowchart illustrating a third embodiment of the instant invention;
- [0065] Fig. 19 is another flowchart illustrating the third embodiment;
- [0066] Fig. 20 depicts an exchange of frames in a handshake according to the third embodiment;

[0067] Fig. 21 is a flowchart which depicts fast active scanning according to a fourth embodiment of the instant invention;

[0068] Fig. 22 is a flowchart that illustrates the procedure of a CAP (for the fourth embodiment) after receiving a probe request;

[0069] Fig. 23 depicts an exchange of frames in a handshake according to the fourth embodiment;

[0070] Fig. 24 is a flowchart illustrating a fifth embodiment of the instant invention;

[0071] Fig. 25 depicts an exchange of frames in a handshake according to the fifth embodiment (incorporating elements of the third and fourth embodiments);

[0072] Fig. 26 depicts an exchange of frames in a handshake according to the fifth embodiment (incorporating elements of the second embodiment);

[0073] Fig. 27 is an example of frames including the format of action frames; and

[0074] Fig. 28 illustrates an example of a processor or processors that may be used in the candidate access points and the mobile stations of the instant invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0075] The following description of illustrative non-limiting embodiments of the invention discloses specific configurations and components. However, the embodiments are merely examples of the present invention, and thus, the specific features described below are merely used to describe such embodiments and to provide an overall understanding of the present invention.

[0076] Accordingly, skilled artisans readily recognize that the present invention is not limited to the specific embodiments described below. Furthermore, the descriptions of

various configurations and components of the present invention that are known to one skilled in the art are omitted for the sake of clarity and brevity.

[0077] Further, while the following embodiments employ the IEEE 802.11 standards by way of example, the present invention may be applied to different wireless networks, including but not limited to those enumerated above.

[0078] The present invention reduces scanning time and handshake latency by making handshakes less susceptible to misjudgment without increasing the number of times a probe request is retransmitted and also without increasing either of MinChannelTime or MaxChannelTime. Indeed the present invention is capable of reducing handshake time when there is no designated AP by allowing the use of a small MinChannelTime.

[0079] In brief, the instant invention incorporates information on neighboring APs to focus a probe request to a specific AP, chosen from a list of candidate access points ("CAPs"). CAPs are determined by providing the mobile station with prior knowledge of the likely state of existing APs. Figure 9 is an example of the information provided to mobile stations concerning candidate access points.

[0080] CAP information includes respective addresses and operational channel numbers for each CAP provided in the list. Further, if CAPs of multiple extended service sets (ESSs) are listed, then the SSID of the respective CAP may be included to facilitate appropriate CAP selection by the mobile station. Additionally, if a plurality of methods are deployed for active scanning, information on the CAPs' scanning capability may also be included to facilitate the selection of a scanning method by the mobile station to match the CAPs' capabilities.

[0081] Figure 10 depicts bit-frame information of the scanning capability of a typical AP. The depicted bit-frame information shows assignment of the capability information field. These frames may be transmitted in beacon or probe response signals, or in other signals.

[0082] Figure 11 depicts an AP with a bit assignment for B8 that indicates the AP is provided with the fast active scanning of the instant invention. Any reserved bit space could be used to denote fast active scanning. The depicted use of B8 in Figure 11 is purely an example. Furthermore, more than one reserved bit could be used to indicate the specific scanning capability.

[0083] Information on CAPs can be collected and delivered to the mobile station(s) in any of various fashions. One such method is offline collection by an operator, in which network providers or operators can collect information by examining coverage of each AP offline. This method of collection of information may be extracted/implemented during the original planning for all APs.

[0084] Another method is real time collection by all APs, using reassociation messaging, in which mobile stations that make a handshake between two APs are recommended to send a reassociation frame containing information of prior APs to subsequent APs. Subsequent APs are then required to send a move-notify message containing information about themselves to prior APs. Through such message exchanges, APs can themselves collect information on CAPs.

[0085] Another real time collection method for information on CAPs would be scan reporting, in which mobile stations that have finished scanning can be requested by the current AP to send a scanning results report of the previous scan to the current AP.

[0086] Because information collected by the two above-noted methods (reassociation messaging and scan reporting) may be constrained within the boundaries of direct-neighbor APs, a corresponding real time method for collecting CAP information is information exchange among existing APs. This method could be incorporated with either or both of reassociation messaging and scan reporting to exchange information among all APs in a network. Figure 12 depicts how exchanging information among all APs results in a neighborhood graph of the APs that shows their relationship to each other.

[0087] A further real time collection method could be the collection of CAP information by a mobile station. That is, results of prior scans can be utilized for subsequent scans. For instance, when beginning an initial scan, mobile stations could use the above-noted information on CAPs as provided by an offline operation or as provided by real time collection by APs. Another option would be to simply use conventional scanning as an initial scanning method, and then to switch to a scanning method of the instant invention as provided herein.

[0088] If CAP information is collected by entities other than a mobile station, the information needs to be delivered to the station. Information may be delivered in any of several ways, as follows, by way of example.

[0089] Delivery of CAP information may be performed via beacon or probe response for an existing AP to a receiving mobile station. Sending the CAP information in a beacon signal may result in a relatively long lag time as a beacon signal is typically sent periodically. Additionally, a mobile station receiving a probe response is generally more

interested in the availability of the AP itself (rather than neighboring APs), so containing the CAP information in a probe response may result in unnecessary overhead.

[0090] Delivery of CAP information may also be done by request and response. That is, only when a mobile station requests the CAP information will it be delivered. The CAP information may be sent to the specific requesting mobile station, or to the entire network.

[0091] Delivery of CAP information may also be performed by simply uploading the information to each station during initial setup.

[0092] Collection and delivery of CAP information may be performed in any of the above-described methods, or in combinations of the above-described methods, or via other methods. Further, the following embodiments may be combined in various ways.

[0093] In the following embodiments, the instant invention employs the CAP information that has been collected and delivered (as described above) to the mobile station attempting to communicate with the network. Accordingly, mobile stations attempting to communicate with the network are therefore enabled to tune to the operational channel of a specific CAP in practicing the various embodiments.

[0094] Embodiments of the invention are enumerated below. The numbering does not imply any order of importance. All of these embodiments depict various aspects of the invention.

I. FIRST EMBODIMENT

[0095] In a first embodiment, the mobile station uses the CAP information that has been collected and delivered to the mobile station to differentiate between those access points

that are most likely to provide communication (CAPs) and those access points which are not likely to provide communication (*e.g.*, busy or otherwise non-communicative APs).

This allows the MaxChannelTime to be set to less than in conventional scanning methods.

[0096] In comparison to conventional scanning techniques (*e.g.*, the scanning technique disclosed in Figure 6), the process of the first embodiment involves the directed scanning of specific APs (candidate access points) vis-à-vis the scanning of network channels (as disclosed by Figure 6, for instance).

[0097] The first embodiment accomplishes directed scanning of available CAPs through utilization of the provided CAP information, using the received CAP information to enter specific access point identification information in the fields of probe requests for individual CAPs. This may be done by entering the address of a specific CAP in the BSSID field along with the SSID of the CAP in the SSID field of the probe request signal. Alternatively, this may also be done by inserting the address of the CAP in the BSSID field along with the broadcast SSID in the SSID field of the probe request signal. Table 3, below, reflects possibilities in specifying permissible field values for the probe request signal of the first embodiment.

Table 3 Permissible Field Values for the Probe Request in the First Embodiment

	DA	BSSID	SSID
Type 1	Broadcast address	Address of the AP	SSID of the AP
Type 2	Broadcast address	Address of the AP	Broadcast SSID

[0098] In this embodiment, the CAP that has received a probe request signal will respond with a probe response only if the SSID in the probe request is the broadcast SSID or if the SSID field matches the specific SSID of the CAP. Probe response frames will be sent as directed frames to the address of the mobile station that generated the probe request and will be subsequently acknowledged by the mobile station. This exchange of frames is illustrated in Figure 14. Notably, only the CAP that has the address of the BSSID field will be able to respond to the probe request frame. Other APs, although operating on the same channel or having the same SSID, will not respond to the probe request because the probe request does not designate them as a responder.

[0099] Figure 13 is a flowchart that depicts the first embodiment. In Figure 13, the mobile station begins by receiving CAPs information (wherein the CAPs information differentiates between those access points most likely to enable communication and those access points that are not) and then specifying a list of CAPS that are to be examined based on those most likely to enable communication.

[00100] Next, the mobile station discerns, from the list of CAPs to be examined, if any unscanned CAPs are present. If all CAPs have been scanned under the Distributed Coordination Function, the process is complete.

[00101] When there are unscanned CAPs, the mobile station transmits a probe request to a selected CAP while simultaneously clearing and starting a probe timer clock (also known as "ProbeTimer"). The mobile station then senses the wireless medium to determine if the medium is busy until a minimum channel time is reached (the minimum channel time is also known as "MinChannelTime").

[00102] If the wireless medium is not busy during MinChannelTime, the CAP is marked as scanned and the mobile station returns to querying whether there are any unscanned CAPs in the network. If all CAPs have been scanned under the Distributed Coordination Function, the process is then complete.

[00103] If any unscanned CAPs remain, the mobile station transmits another probe request to a selected CAP while simultaneously clearing and starting the ProbeTimer clock. The mobile station then senses the wireless medium to determine if the medium is busy until MinChannelTime is reached. If the wireless medium is busy during MinChannelTime, then the station waits until the ProbeTimer reaches a maximum channel time (also known as the "MaxChannelTime" signal). Additionally, if any unicast frame is received, it is responded to with an acknowledgement signal (also known as an "ACK" signal) from the mobile station.

[00104] When the MaxChannelTime is reached, any received probe responses are processed, and the probed CAP is marked as scanned. The process of Figure 13 continues until all unscanned CAPs have been scanned.

[00105] Figure 14 depicts a temporal exchange of frames in the first embodiment between a mobile station and a CAP. A scanning mobile station sends a probe request signal to a CAP. After the DIFS period and a random backoff interval, the CAP responds with a probe response signal. After a subsequent SIFS period, the mobile station confirms receipt of the probe response with an acknowledgement ("ACK") signal.

II. SECOND EMBODIMENT

[00106] In a second embodiment, MinChannelTime and MaxChannelTime can both be set to less than required for conventional scanning systems, for the reasons explained herein. The mobile station of the second embodiment can learn of the actual availability of a CAP not only through the receipt of a probe response signal from the CAP, but also, if the mobile station is only interested in knowing if the CAP is available, through receipt of an ACK signal. Accordingly, a probe response is not necessary.

[00107] That is, instead of (or in addition to) a probe response, the mobile station may be alerted to the availability of a CAP through receipt of an ACK signal sent from the CAP. Conversely, if the mobile station is interested in more information than just the availability of the CAP, it may wait for a probe response signal to be transmitted subsequent to the transmission of an ACK signal from the CAP. Otherwise, the mobile station may proceed to the scanning of other CAPs without waiting for a probe response.

[00108] The procedure of the second embodiment of the invention is shown by the flowchart of Figure 15. As Figure 15 is similar in nature to Figure 13, similar features will not be reiterated.

[00109] Figure 15 shows that for an ACK signal received in response to a transmitted probe request, the CAP in question is marked as scanned and available, and then either the remaining CAPs to be scanned are scanned or the process is at an end because all CAPs have been scanned.

[00110] Conversely, if an ACK signal is not received in response to a probe request, the CAP is simply marked as scanned and then either the remaining CAPs to be scanned are scanned or the process is at an end because all CAPs have been scanned.

[00111] The second embodiment accomplishes directed scanning of available CAPs using the provided CAP information to enter specific access point identification information in the frames of probe requests for individual CAPs. This may be done by entering the address of a specific CAP in the DA field in the probe request signal. Either of the address of a specific CAP or the broadcast BSSID is entered in the BSSID field, along with either of the SSID of the CAP or the broadcast SSID in the SSID field of the probe request signal. Table 4, below, reflects possibilities in specifying permissible field values for the probe request signal of the second embodiment.

Table 4 Permissible Field Values for the Probe Request in Embodiment 2

	DA	BSSID	SSID
Type 1	Address of the AP	Address of the AP	SSID of the AP
Type 2	Address of the AP	Broadcast BSSID	SSID of the AP
Type 3	Address of the AP	Address of the AP	Broadcast BSSID
Type 4	Address of the AP	Broadcast BSSID	Broadcast BSSID

[00112] Frame exchange in the second embodiment is altered so that transmitted probe request signals are responded to with an ACK signal. While different from conventional scanning methods, the second embodiment still complies with the general rules for IEEE 802.11 acknowledgements, since the probe request maintains non-group destination address assignment, as shown in Table 4, above. Notably, in the second embodiment

(and additionally in the first embodiment) only the CAP that has the address of the DA field will be able to respond to the probe request frame. Other APs, although operating on the same channel or having the same SSID, will not respond to the probe request because the probe request does not designate them as a responder.

[00113] An entire frame exchange of the second embodiment is illustrated by Figure 16. As shown in the figure, a probe request is sent to a specific CAP, and the designated CAP responds with an ACK signal. It should be understood that the subsequent probe response and ACK depicted in dotted line as shown in the figure is purely an optional feature of the second embodiment.

[00114] Figure 17 is a flowchart showing the procedure that a CAP follows in the second embodiment after reception of a frame request. In the figure, CAPs that receive probe requests that are in compliance with Table 4 respond with an ACK signal. As an optional feature, if the SSID in the probe request is the broadcast SSID or if the SSID matches the specific SSID of the CAP, then the CAP initiates transmission of a probe response as directed frames to the address of the mobile station that generated the probe request. The probe response is sent using the normal frame transmission rules of the DCF.

[00115] In the second embodiment, MinChannelTime can be set to a value not much greater than the SIFS value, since an ACK signal is sent in response to the probe request immediately after the SIFS interval.

III. THIRD EMBODIMENT

[00116] Figure 18 is a flowchart illustrating a third embodiment of the instant invention. In the figure, a mobile station in fast active scanning mode is first provided with CAP

information, as previously described. The station then specifies a list of CAPs that are to be examined based on the provided CAP information. Next, the station waits either until a ProbeDelay time has expired or until an indication that an incoming frame has been received.

[00117] The mobile station then sends a probe request signal similar to that shown in Figure 2, but with the DA, BSSID and SSID fields filled with information as provided in Table 3. That is, the broadcast address will be entered in the DA field, the address of the CAP will be entered in the BSSID field, and either of the SSID of the CAP or the broadcast SSID will be entered in the SSID field of the probe request. The ProbeTimer is then cleared and begun. If the medium has not been detected as busy before the ProbeTimer reaches MinChannelTime, then the next CAP is scanned. Otherwise, any received probe responses are acknowledged and processed. Then, the next CAP is scanned. When all CAPs in the CAP list have been examined, the scanning process ends.

[00118] Notably, MinChannelTime in the third embodiment may be reduced to that not much greater than a SIFS value or even to the same value as the ACKTimeout.

[00119] Figure 19 is a flowchart depicting the third embodiment of the instant invention. In Figure 19, the CAP receiving the probe request signal responds with a probe response only if the SSID in the probe request is the broadcast SSID or if the SSID in the probe request matches the specific SSID of the CAP. What differentiates the third embodiment from other embodiments (such as the first and second embodiments), however, is that the transmission of the probe response is commenced immediately after an IFS period that is smaller than the DIFS period.

[00120] Although either of a SIFS or PIFS period may be employed in the third embodiment, the following description incorporates the use a SIFS period. (If a PIFS period is used, MinChannelTime should be set to a value not much greater than the PIFS period.) Accordingly, the designated CAP in the third embodiment has higher priority access to the wireless medium due to a shortened IFS period.

[00121] The probe response frame is acknowledged with an ACK signal sent by the scanning station. An entire frame exchange of the third embodiment is depicted in Figure 20. In the Figure, a probe request is sent to a specific CAP. The minimum channel time has been reduced to the SIFS period, after which the CAP sends a probe response. After a further SIFS period, the probe response is acknowledged by the mobile station with an ACK signal.

[00122] Determination of availability of the CAP in the third embodiment is performed as follows. If the wireless medium is idle until ProbeTimer reaches MinChannelTime, the mobile station thus discerns that the designated CAP is not available in the area. If the wireless medium becomes busy before ProbeTimer reaches MinChannelTime, and the received probe response is from the designated CAP, the CAP is regarded as available to serve the mobile station. If the wireless medium becomes busy before ProbeTimer reaches MinChannelTime, and the received signal is other than the probe response signal from the designated CAP, the CAP is regarded as unavailable.

IV. FOURTH EMBODIMENT

[00123] While the third embodiment obeys the general receiving rule of the IEEE 802.11 WLAN standards that directed frames should be acknowledged with an ACK signal and that frames with group destination addresses are not acknowledged, the fourth embodiment loosens some of the general receiving rules of the IEEE 802.11 standards, allowing for more time-efficient scanning.

[00124] Figure 21 is a flowchart that depicts the fast active scanning of the fourth embodiment. In the figure, the mobile station is provided with CAP information from which a specific list of CAPs to be examined is created. If there are any CAPs in the list that have not been scanned, a CAP is selected for scanning and the mobile station transmits a probe request to the selected CAP (simultaneous to clearing and starting a ProbeTimer). In the transmitted probe request, the DA, BSSID and SSID fields are filled in with information corresponding to that shown in Tables 3 or 4.

[00125] If the wireless medium is not detected as busy prior to the ProbeTimer reaching MinChannelTime, then the next CAP is scanned. Otherwise, any received probe responses are processed. Subsequent CAPs are scanned until all CAPs in the list have been scanned.

[00126] In the fourth embodiment, MinChannelTime is a value only large enough to ensure the successful detection of frames transmitted using SIFS or PIFS periods, and preferably is set to a period not much greater than a SIFS period (if the probe response is sent with a SIFS period), or set to not much greater than a PIFS period (if the probe

response is sent with a PIFS period). In a non-limiting version of the fourth embodiment, the probe response signal is sent with a SIFS period, and MinChannelTime is set to the same value as ACKTimeout.

[00127]

In compliance with the general receiving rules of the IEEE 802.11 WLAN standards, only the access point designated by the scanning station receives the probe request signal that is sent with the DA, BSSID and SSID fields filled in according to the information provided in Tables 3 and 4. With further reference to Figure 21, the CAP receiving the probe request signal responds with a probe response only if the SSID in the probe request is the broadcast SSID or if the SSID in the probe request matches the specific SSID of the CAP.

[00128]

Probe response signals are sent, immediately after an IFS period that is smaller than a DIFS period, as directed frames to the address of the station that generated the probe request. Although either a SIFS or PIFS could be used, the fourth embodiment is described herein as using a SIFS period.

[00129]

The probe response signal sent by the recipient of the probe request signal may be regarded as successful acknowledgement of the probe request signal. The probe response signal, however, is neither acknowledged nor expected to be acknowledged. The mobile station thus proceeds with scanning the next CAP in the list of CAPs without transmitting an ACK signal to the CAP that has transmitted a probe response.

[00130]

Figure 22 illustrates the procedure of a CAP (for the fourth embodiment) after receiving a probe request. In the figure, if a probe request's SSID is the broadcast SSID

or if the probe request's SSID matches the CAP's SSID, then a probe response is sent after either a SIFS or PIFS period.

[00131]

Figure 23 depicts an entire frame exchange of the fourth embodiment. In the figure, the CAP responds to a response request with a probe response signal after a SIFS (or PIFS) period. Determination of availability of the CAP in the fourth embodiment is performed as follows. If the wireless medium is idle until ProbeTimer reaches MinChannelTime, the mobile station thus discerns that the designated CAP is not available in the area. If the wireless medium becomes busy before ProbeTimer reaches MinChannelTime, and the received probe response signal is from the designated CAP, the CAP is regarded as available to serve the mobile station. If the wireless medium becomes busy before ProbeTimer reaches MinChannelTime, and the received signal is other than the ACK signal from the designated CAP, the CAP is regarded as unavailable.

V. FIFTH EMBODIMENT

[00132]

When transmitting a probe request in conventional methods, a scanning station must contend for the wireless medium under the access procedure provided by the DCF. Although this ensures fairness of opportunity among any transmitting stations, it is also time-consuming. Therefore, in the fifth embodiment of the instant invention, after transmitting a first probe request signal under the basic rules of the DCF, a scanning station is then allowed a higher priority transmission opportunity (the number of which may be restricted in fairness to other mobile stations which may be attempting to transmit their own probe request signals).

[00133] The fifth embodiment is a modification of embodiments 2, 3 and 4 and is shown by the flowchart depicted in Figure 24. In the fifth embodiment, a SIFS period is used for the IFS period between a probe request signal and probe response signal. If the SIFS period lapses without the receipt of the expected probe response signal, the mobile station is then allowed to resend the probe request signal as soon as one PIFS period after transmission of the probe request. This permits the scanning station to retain control of the wireless medium until an allowed retransmission limit (RetryLimit) has been reached.

[00134] An entire frame exchange of the fifth embodiment with a RetryLimit of 1 is illustrated in Figure 25 (incorporating elements of previously described embodiments 3 and 4) and Figure 26 (incorporating elements of previously described embodiment 2). In Figure 25 and Figure 26, an initial probe request signal has not been responded to within the PIFS period by an appropriate probe response and ACK, respectively. Accordingly, the mobile station retransmits another probe request at the end of the PIFS period. As further shown in the figures, an appropriate probe response and ACK is received after the second transmission of the probe request. An acknowledgment signal may or may not be transmitted in response to the probe response signal in Figure 25.

VI. SIXTH EMBODIMENT

[00135] In a sixth embodiment of the invention, employment of the fast active scanning as provided in any of the previous embodiments is made optional in conjunction with conventional scanning. By way of explanation, conventional scanning and fast active scanning (per disclosed embodiments of the invention) use different values in the DA and BSSID fields of a probe request. That is, conventional scanning uses broadcast

destination and broadcast BSSID in the probe request signal, while the invention uses the address of the CAP in the DA or BSSID fields.

[00136] Therefore, the sixth embodiment deploys conventional scanning techniques if either the broadcast destination or the broadcast BSSID is used in the DA and BSSID fields of a probe request, respectively. Conversely, if the address of the CAP is used in either the DA or BSSID fields of the probe request, the CAP uses fast active scanning (as provided herein by deployment of an embodiment of the invention). In deploying either of the scanning methods, the probe request uses type bits of 00 and subtype bits of 0100 in the frame control field.

VII. SEVENTH EMBODIMENT

[00137] In the seventh embodiment of the invention, scanning methods are distinguished by explicit indication in the header of the probe request signal. In this embodiment, the explicit notification desirably uses reserved type bits and subtype bits of the frame control field as depicted in Table 1. More desirably, the explicit notification uses reserved subtype bits for the management field.

[00138] For example, type bits of 00 and subtype bits of 1110 in the frame control field are assigned to indicate the active scanning according to the second embodiment of the invention, while type bits of 00 and subtype bits of 1111 are assigned to indicate the fast active scanning of the fourth embodiment of the invention. As in Table 1, type bits of 00 and subtype bits of 0100 in the frame control field are used to indicate conventional active scanning. Therefore, in the seventh embodiment, the active scanning method to be deployed by the CAP is determined as follows.

[00139]

If the probe request, in the frame control field, has the pair of type bits and subtype bits that are assigned to indicate a specific fast active scanning method, the CAP uses the indicated fast active scanning method. The CAP will allow probe request signals of assigned type and subtype bits even before authentication or association, without filtering.

VIII. EIGHTH EMBODIMENT

[00140]

In an eighth embodiment of the invention, scanning methods are distinguished by explicit indication in the header and frame body of probe request signals. Preferably, the explicit notification uses predetermined fields in the frame body of the action frame (*i.e.*, type bits 00 and subtype bits 1101 in the frame control field).

[00141]

The action frame provides a mechanism for specifying extended management actions. The format of the action field is shown by example in Figure 27. The category field will be set to one of the non-reserved values shown below in Table 5.

Table 5 Category Values

<u>Name</u>	<u>Value</u>
Reserved	0-2
Radio measurement	3
Reserved	4-127
Error	128-255

[00142]

The action details field contains the details of the action. The details of the actions allowed in each category include a radio measurement category with action field values, for instance, those values depicted in Table 6, below.

Table 6 Radio measurement action field values

<u>Action field value</u>	<u>Description</u>
0	Measurement Request
1	Measurement Report
2-255	Reserved

[00143] In any reserved category, values may be used to explicitly indicate the specific fast active scanning to be used. For example, a category value of 4 may be assigned to indicate the fast active scanning according to the second embodiment, while a category value of 5 may be assigned to indicate the active scanning of the fourth embodiment. Therefore, determination of the fast active scanning method to be deployed is determined as follows. In the predetermined header or frame body of a probe request, if the specific value that is assigned to indicate a specific fast active scanning method is found, the CAP uses the indicated fast active scanning method. The CAP will not filter out probe request signals of assigned type and subtype bits even before authentication or association.

ADDITIONAL EMBODIMENTS

[00144] Figure 28, which is similar in nature to Figure 1, depicts an embodiment of the invention including at least one processor 21 that, as part of a candidate access point 20, is capable of processing candidate access point information that differentiates between candidate access points which are most likely to provide communication and candidate access points which are not, according to one or more of the embodiments of the invention described herein.

[00145] Figure 28 also depicts a further embodiment of the invention including at least one processor 11 that, as part of a wireless station 10, is capable of processing candidate

access point information that differentiates between candidate access points which are most likely to provide communication and candidate access points which are not, also according to one or more of the embodiments of the invention described herein.

[00146]

Although probe responses are described herein as directed frames sent to the scanning station, the probe responses could also be a broadcast frame or a multicast frame to a set of stations. Additionally, the fields in the probe response described herein for informing the scanning station of the characteristics of the AP are not always required in their listed entirety. Some or all of the fields can be removed. Furthermore, although specific frame formats are depicted herein for both the probe request and probe response, the invention is not constrained by any specific frame format. Further, the terms "field" and "frame" may be used analogously herein.

[00147]

Also, the IEEE standards described herein use a network allocation vector ("NAV") for directed frame transmission to secure the channel for the subsequent atomic frame transmissions. This can be used for any of the embodiments described herein without change. In embodiments 3, 4 and 5, NAV can even be used for the probe request signal with a broadcast destination address, since these embodiments expect effectively only one recipient (even though they are broadcast). The NAV value for the probe request in embodiments 3, 4 and 5 could thus be set to the sum of SIFS and the transmission time of the probe request and probe response with a minimum size.

[00148]

Moreover, as previously noted, the invention is herein explained through use of the IEEE 802.11 WLAN standards. The invention may readily be applied to other

wireless communication systems, including but not limited to those mentioned throughout the specification.

[00149] Advantageous characteristics in the embodiments of the present invention include reduced scanning time and handshake latency while simultaneously reducing handshake susceptibility to misjudgment without increasing the number of times a probe request is retransmitted and also without increasing either of MinChannelTime or MaxChannelTime.

[00150] The previous description of embodiments is provided to enable a person skilled in the art to make and use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles and specific examples defined herein may be applied to other embodiments without the use of inventive faculty. For example, some or all of the features of the different embodiments discussed above may be deleted from the embodiment. Therefore, the present invention is not intended to be limited to the embodiments described herein but is to be accorded the widest scope defined only by the claims below and equivalents thereof.

WHAT IS CLAIMED IS:

1. A method of enabling channel scanning in a wireless network, said method comprising:

collecting candidate access point information that differentiates between candidate access points which are most likely to provide communication with wireless stations in the network and candidate access points which are not; and

transmitting said candidate access point information.
2. The method of claim 1, comprising selecting, from said candidate access point information, said candidate access points that have been differentiated as most likely to provide communication.
3. The method of claim 2, comprising scanning, with a wireless station, said candidate access points that have been differentiated as most likely to provide communication.
4. The method of claim 3, wherein said scanning comprises said wireless station transmitting a probe request for a specified candidate access point chosen from among said candidate access points differentiated as most likely to provide communication with the network.
5. The method of claim 4, wherein said probe request comprises fields of information wherein a broadcast address is entered in a destination address field, an individual address of said specified candidate access point is entered in a basic service set

identification field, and either of a service set identification for said specified candidate access point or a broadcast service set identification for said specified candidate access point is entered in a service set identification field.

6. The method of claim 4, wherein said specified candidate access point responds to said probe request with an acknowledgement frame prior to any other type of frame being transmitted from said specified candidate access point and immediately following an interframe space that immediately follows said probe request.

7. The method of claim 4, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said wireless station responds to said probe response with an acknowledgement frame.

8. The method of claim 4, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said probe response is neither acknowledged nor expected to be acknowledged with an acknowledgement frame from said wireless station.

9. The method of claim 4, wherein, if said specified candidate access point does not respond to said probe request with a probe response within an interframe space period that immediately follows said probe request and that is shorter than a distributed interframe space period, said wireless station resends said probe request in the time period after said interframe space period that immediately follows said probe request has ended but prior to the time period that a distributed interframe space period would have begun if said distributed interframe space period had begun at the same time as said interframe space period that immediately follows said probe request.

10. The method of claim 4, wherein, if a probe request frame's destination address field includes a broadcast destination or if the basic service set identification field includes a broadcast basic service set identification, then said scanning comprises a scanning technique selected from the group consisting of the IEEE 802.11, 802.15 and 802.16 wireless standards of interoperability.

11. A wireless communications network comprising:
a collector which collects candidate access point information that differentiates between candidate access points which are most likely to provide communication with wireless stations in the network and candidate access points which are not; and
a transmitter for transmitting said candidate access point information.

12. The network of claim 11, further comprising a selector for selecting, from said candidate access point information, said candidate access points that have been differentiated as most likely to provide communication.

13. The network of claim 12, further comprising a wireless station for scanning said candidate access points that have been differentiated as most likely to provide communication.

14. The network of claim 13, wherein said scanning comprises said wireless station transmitting a probe request for a specified candidate access point chosen from among said candidate access points differentiated as most likely to provide communication with the network.

15. The network of claim 14, wherein said probe request comprises fields of information wherein a broadcast address is entered in a destination address field, an individual address of said specified candidate access point is entered in a basic service set identification field, and either of a service set identification for said specified candidate access point or a broadcast service set identification for said specified candidate access point is entered in a service set identification field.

16. The network of claim 14, wherein said specified candidate access point responds to said probe request with an acknowledgement frame prior to any other type of frame being transmitted from said specified candidate access point and immediately following an interframe space that immediately follows said probe request.

17. The network of claim 14, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space

period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said wireless station responds to said probe response with an acknowledgement frame.

18. The network of claim 14, wherein

said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said probe response is neither acknowledged nor expected to be acknowledged with an acknowledgement frame from said wireless station.

19. The network of claim 14, wherein, if said specified candidate access point does not respond to said probe request with a probe response within an interframe space period that immediately follows said probe request and that is shorter than a distributed interframe space period, said wireless station resends said probe request in the time period after said interframe space period that immediately follows said probe request has ended but prior to the time period that a distributed interframe space period would have begun if said distributed interframe space period had begun at the same time as said interframe space period that immediately follows said probe request.

20. The network of claim 14, wherein, if a probe request frame's destination address field includes a broadcast destination or if the basic service set identification field

includes a broadcast basic service set identification, then said scanning comprises a scanning technique selected from the group consisting of the IEEE 802.11, 802.15 and 802.16 wireless standards of interoperability.

21. A wireless telecommunications system comprising:

a plurality of access points, at least some of said access points containing candidate access point information that differentiates between candidate access points which are most likely to provide communication with wireless stations in the system and candidate access points which are not;

wherein said access points containing candidate access point information include a transmitter for transmitting said candidate access point information.

22. The system of claim 21, further comprising at least one selector for selecting, from said candidate access point information, said candidate access points that have been differentiated as most likely to provide communication.

23. The system of claim 22, wherein at least one wireless station scans said candidate access points that have been differentiated as most likely to provide communication.

24. The system of claim 23, wherein said scanning comprises said at least one wireless station transmitting a probe request for a specified candidate access point chosen from among said candidate access points differentiated as most likely to provide communication with the network.

25. The system of claim 24, wherein said probe request comprises fields of information wherein a broadcast address is entered in a destination address field, an individual address of said specified candidate access point is entered in a basic service set identification field, and either of a service set identification for said specified candidate access point or a broadcast service set identification for said specified candidate access point is entered in a service set identification field.

26. The system of claim 24, wherein said specified candidate access point responds to said probe request with an acknowledgement frame prior to any other type of frame being transmitted from said specified candidate access point and immediately following an interframe space that immediately follows said probe request.

27. The system of claim 24, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said wireless station responds to said probe response with an acknowledgement frame.

28. The system of claim 24, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space

period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said probe response is neither acknowledged nor expected to be acknowledged with an acknowledgement frame from said wireless station.

29. The system of claim 24, wherein, if said specified candidate access point does not respond to said probe request with a probe response within an interframe space period that immediately follows said probe request and that is shorter than a distributed interframe space period, said wireless station resends said probe request in the time period after said interframe space period that immediately follows said probe request has ended but prior to the time period that a distributed interframe space period would have begun if said distributed interframe space period had begun at the same time as said interframe space period that immediately follows said probe request.

30. The system of claim 24, wherein, if a probe request frame's destination address field includes a broadcast destination or if the basic service set identification field includes a broadcast basic service set identification, then said scanning comprises a scanning technique selected from the group consisting of the IEEE 802.11, 802.15 and 802.16 wireless standards of interoperability.

31. In a wireless telecommunications system comprising a plurality of access points, the improvement wherein at least one of the access points comprises a processor which processes candidate access point information that differentiates between candidate

access points which are most likely to provide communication with wireless stations in the system and candidate access points which are not.

32. The system of claim 31, further comprising a wireless station for scanning said candidate access points that have been differentiated as most likely to provide communication.

33. The system of claim 32, wherein said scanning comprises said wireless station transmitting a probe request for a specified candidate access point chosen from among said candidate access points differentiated as most likely to provide communication with the network.

34. The system of claim 33, wherein said probe request comprises fields of information wherein a broadcast address is entered in a destination address field, an individual address of said specified candidate access point is entered in a basic service set identification field, and either of a service set identification for said specified candidate access point or a broadcast service set identification for said specified candidate access point is entered in a service set identification field.

35. The system of claim 33, wherein said specified candidate access point responds to said probe request with an acknowledgement frame prior to any other type of frame being transmitted from said specified candidate access point and immediately following an interframe space that immediately follows said probe request.

36. The system of claim 33, wherein

said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said wireless station responds to said probe response with an acknowledgement frame.

37. The system of claim 33, wherein

said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein

said probe response is neither acknowledged nor expected to be acknowledged with an acknowledgement frame from said wireless station.

38. The system of claim 33, wherein, if said specified candidate access point does not respond to said probe request with a probe response within an interframe space period that immediately follows said probe request and that is shorter than a distributed interframe space period, said wireless station resends said probe request in the time period after said interframe space period that immediately follows said probe request has ended but prior to the time period that a distributed interframe space period would have begun if said distributed interframe space period had begun at the same time as said interframe space period that immediately follows said probe request.

39. The system of claim 33, wherein, if a probe request frame's destination address field includes a broadcast destination or if the basic service set identification field includes a broadcast basic service set identification, then said scanning comprises a scanning technique selected from the group consisting of the IEEE 802.11, 802.15 and 802.16 wireless standards of interoperability.

40. In a wireless telecommunications system comprising a plurality of wireless stations, the improvement wherein at least one of the wireless stations comprises a processor which processes candidate access point information that differentiates between candidate access points which are most likely to provide communication with said wireless station and candidate access points which are not.

40. The system of claim 40, wherein at least one wireless station scans said candidate access points that have been differentiated as most likely to provide communication.

41. The system of claim 40, wherein said scanning comprises said at least one wireless station transmitting a probe request for a specified candidate access point chosen from among said candidate access points differentiated as most likely to provide communication with the network.

42. The system of claim 41, wherein said probe request comprises fields of information wherein a broadcast address is entered in a destination address field, an individual address of said specified candidate access point is entered in a basic service set

identification field, and either of a service set identification for said specified candidate access point or a broadcast service set identification for said specified candidate access point is entered in a service set identification field.

43. The system of claim 41, wherein said specified candidate access point responds to said probe request with an acknowledgement frame prior to any other type of frame being transmitted from said specified candidate access point and immediately following an interframe space that immediately follows said probe request.

44. The system of claim 41, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein
said wireless station responds to said probe response with an acknowledgement frame.

45. The system of claim 41, wherein
said specified candidate access point responds to said probe request with a probe response frame immediately following an interframe space period, said interframe space period immediately following said probe request and being shorter in time than a distributed interframe space period; and wherein
said probe response is neither acknowledged nor expected to be acknowledged with an acknowledgement frame from said wireless station.

46. The system of claim 41, wherein, if said specified candidate access point does not respond to said probe request with a probe response within an interframe space period that immediately follows said probe request and that is shorter than a distributed interframe space period, said wireless station resends said probe request in the time period after said interframe space period that immediately follows said probe request has ended but prior to the time period that a distributed interframe space period would have begun if said distributed interframe space period had begun at the same time as said interframe space period that immediately follows said probe request.

47. The system of claim 41, wherein, if a probe request frame's destination address field includes a broadcast destination or if the basic service set identification field includes a broadcast basic service set identification, then said scanning comprises a scanning technique selected from the group consisting of the IEEE 802.11, 802.15 and 802.16 wireless standards of interoperability.

1/28

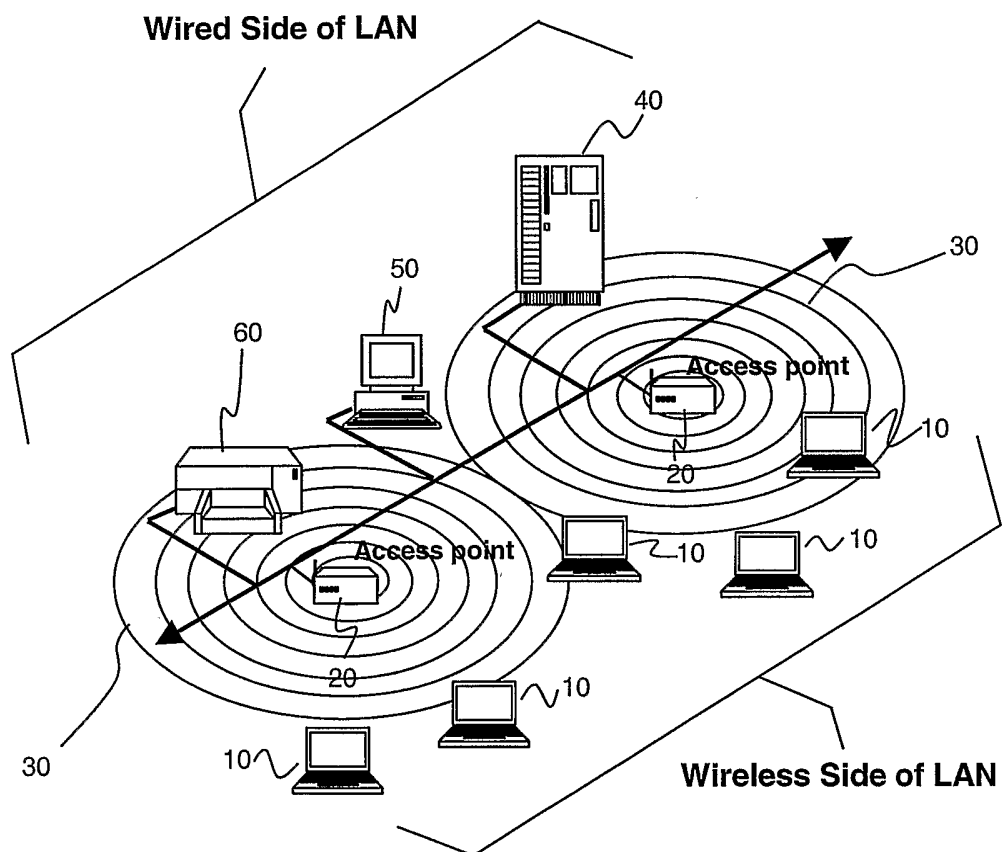


FIG. 1

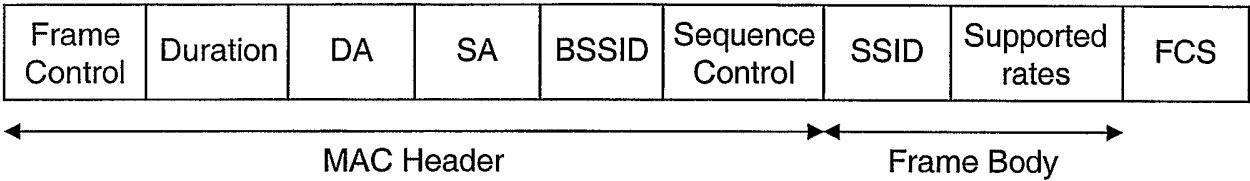


FIG. 2

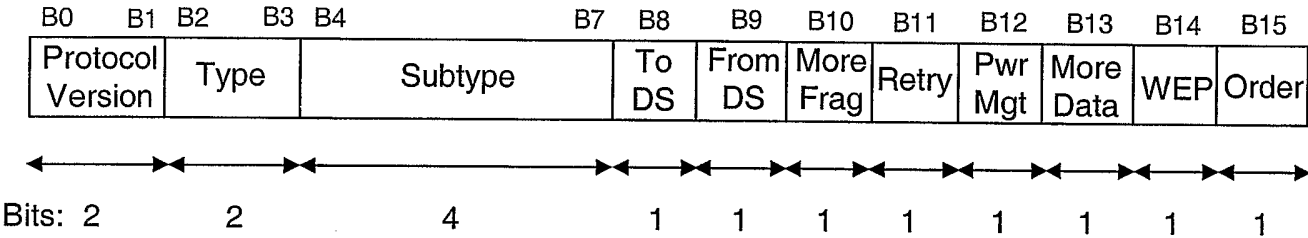


FIG. 3

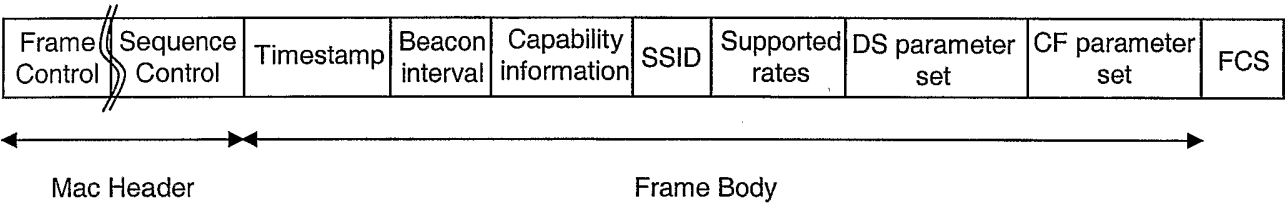


FIG. 4

5/28

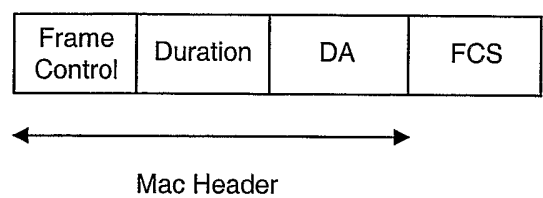


FIG. 5

6/28

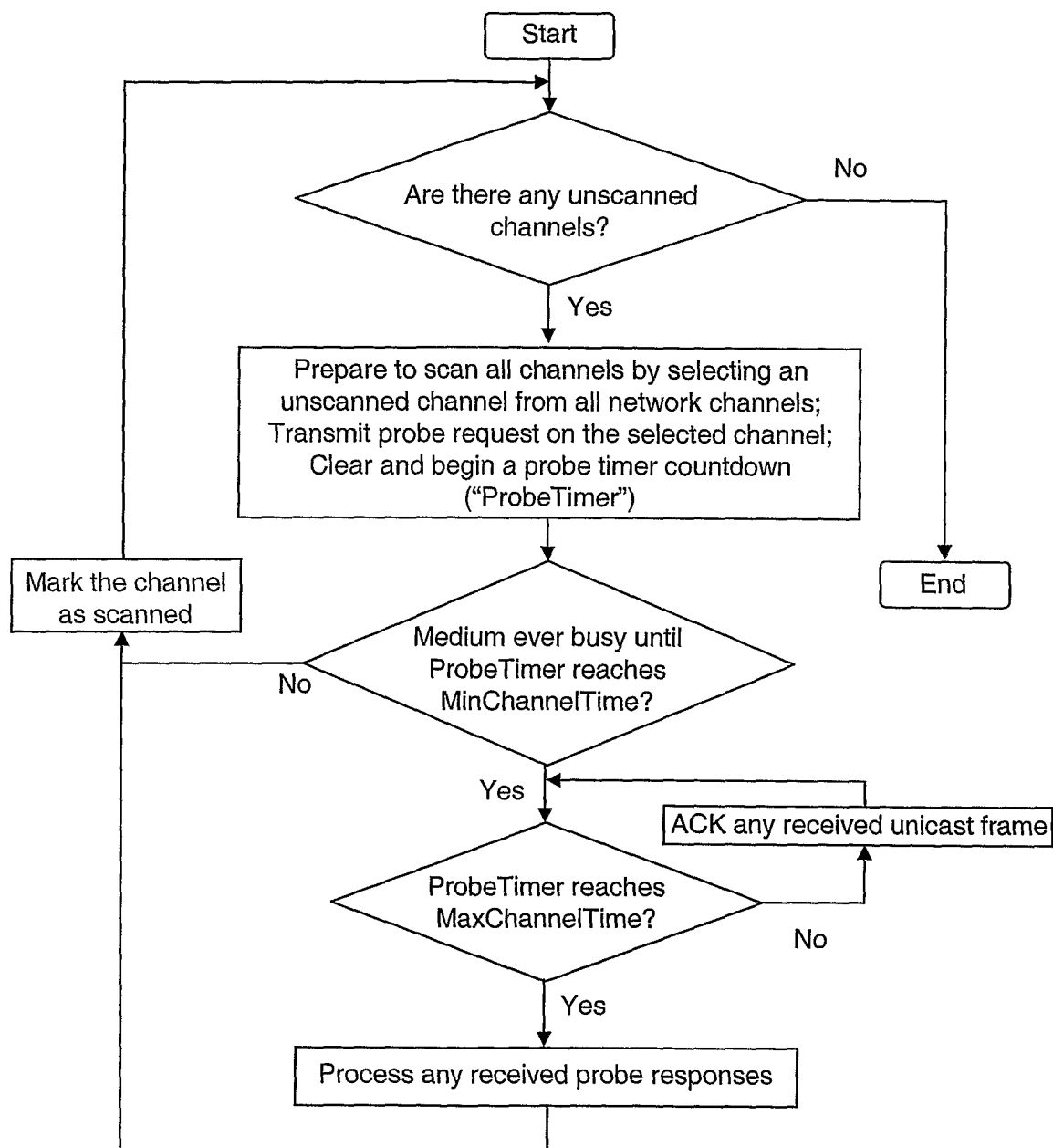


FIG. 6

7/28

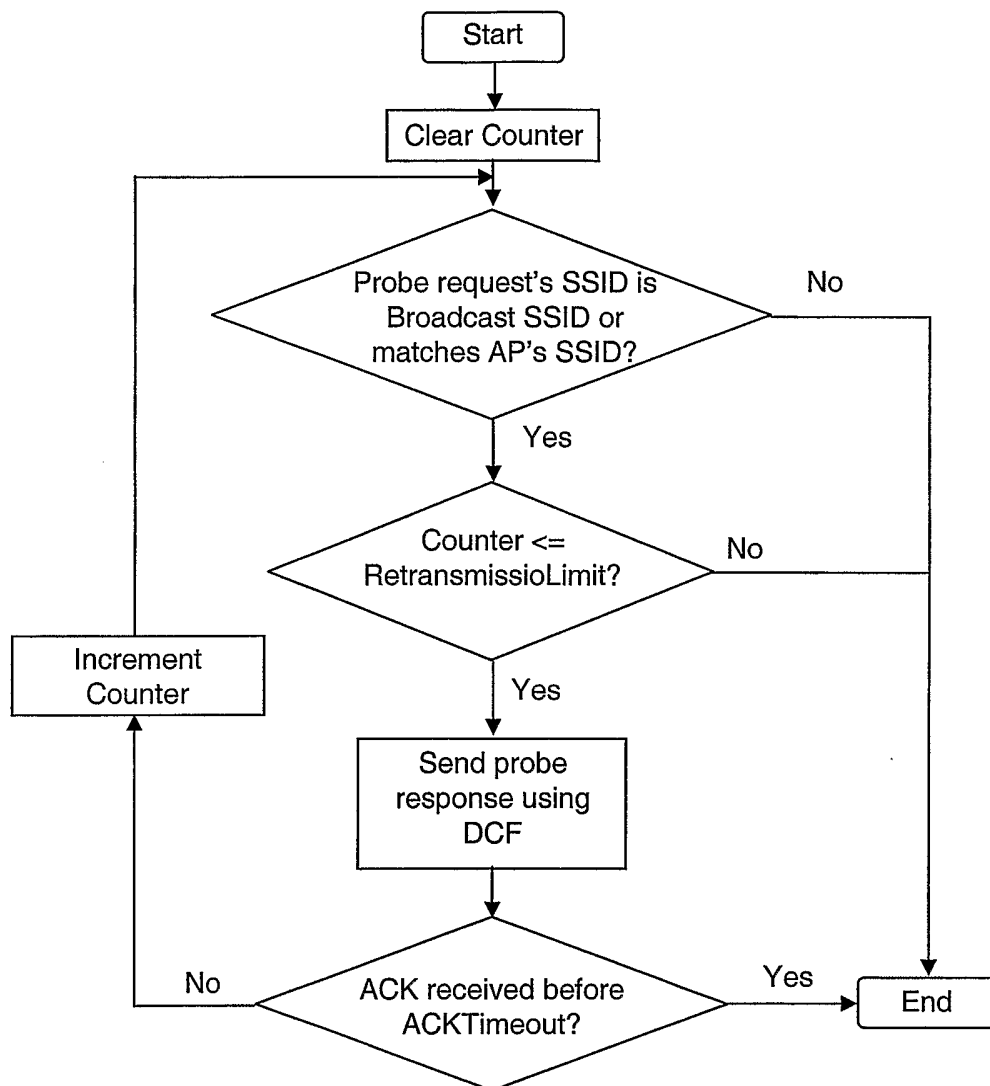


FIG. 7

8/28

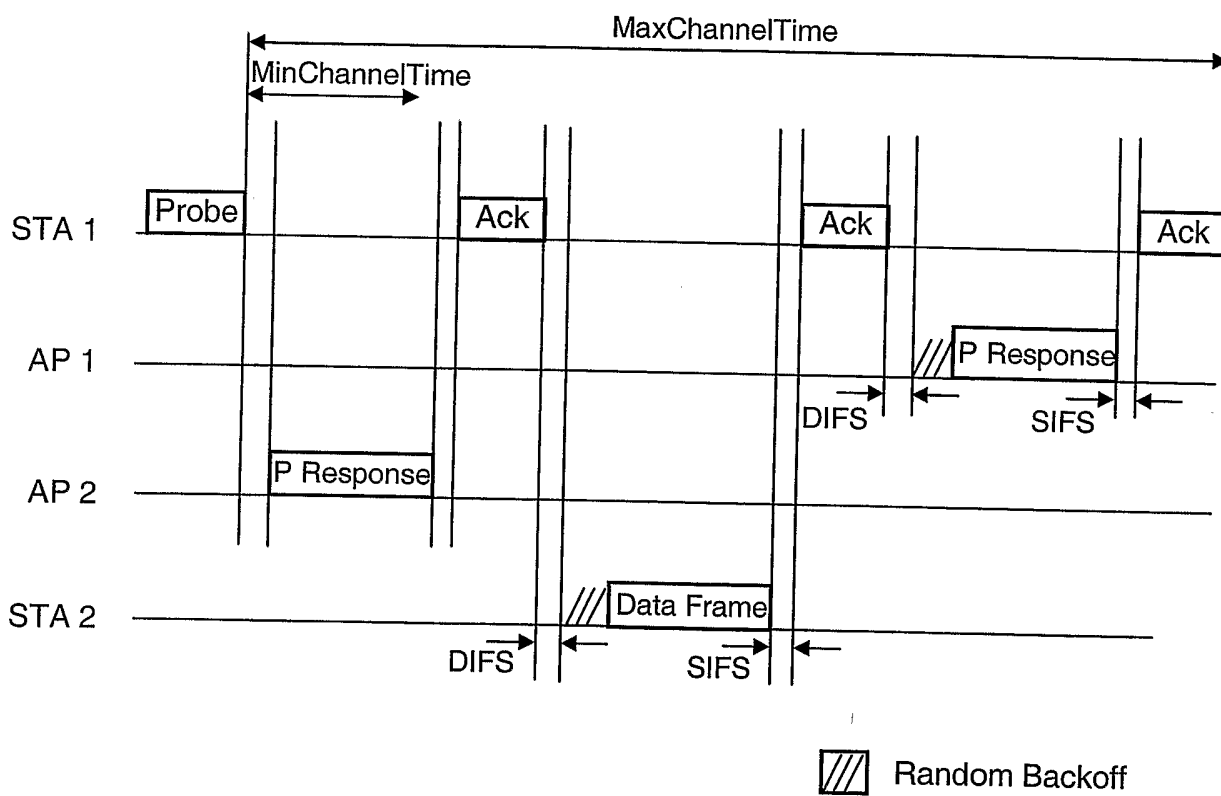


FIG. 8

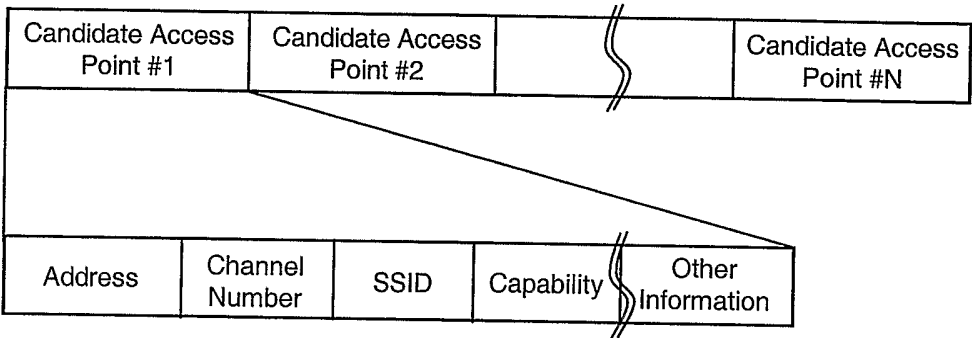


FIG. 9

10/28

B0	B1	B2	B3	B4	B5	B6	B7
ESS	IBSS	CF Pollable	CF Poll Request	Privacy	Short Preamble	PBCC	Channel Agility

B8	B9	B10	B11	B12	B13	B14	B15
Reserved (0)	Reserved (0)	Reserved (0)	Reserved (0)	Radio Measurement	Reserved (0)	Reserved (0)	Reserved (0)

FIG. 10

11/28

B0	B1	B2	B3	B4	B5	B6	B7
ESS	IBSS	CF Pollable	CF Poll Request	Privacy	Short Preamble	PBCC	Channel Agility

B8	B9	B10	B11	B12	B13	B14	B15
Fast Active Scan	Reserved (0)	Reserved (0)	Reserved (0)	Radio Measurement	Reserved (0)	Reserved (0)	Reserved (0)

FIG. 11

12/28

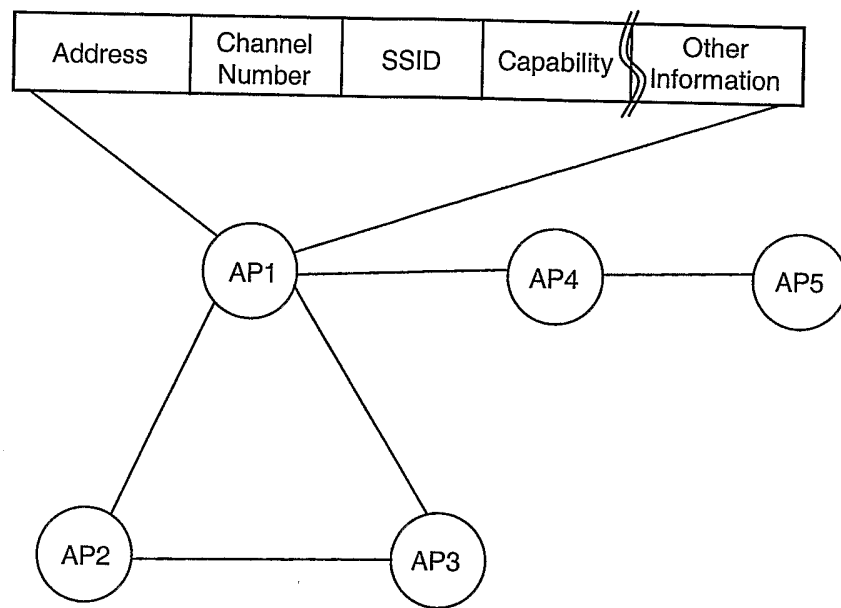


FIG. 12

13/28

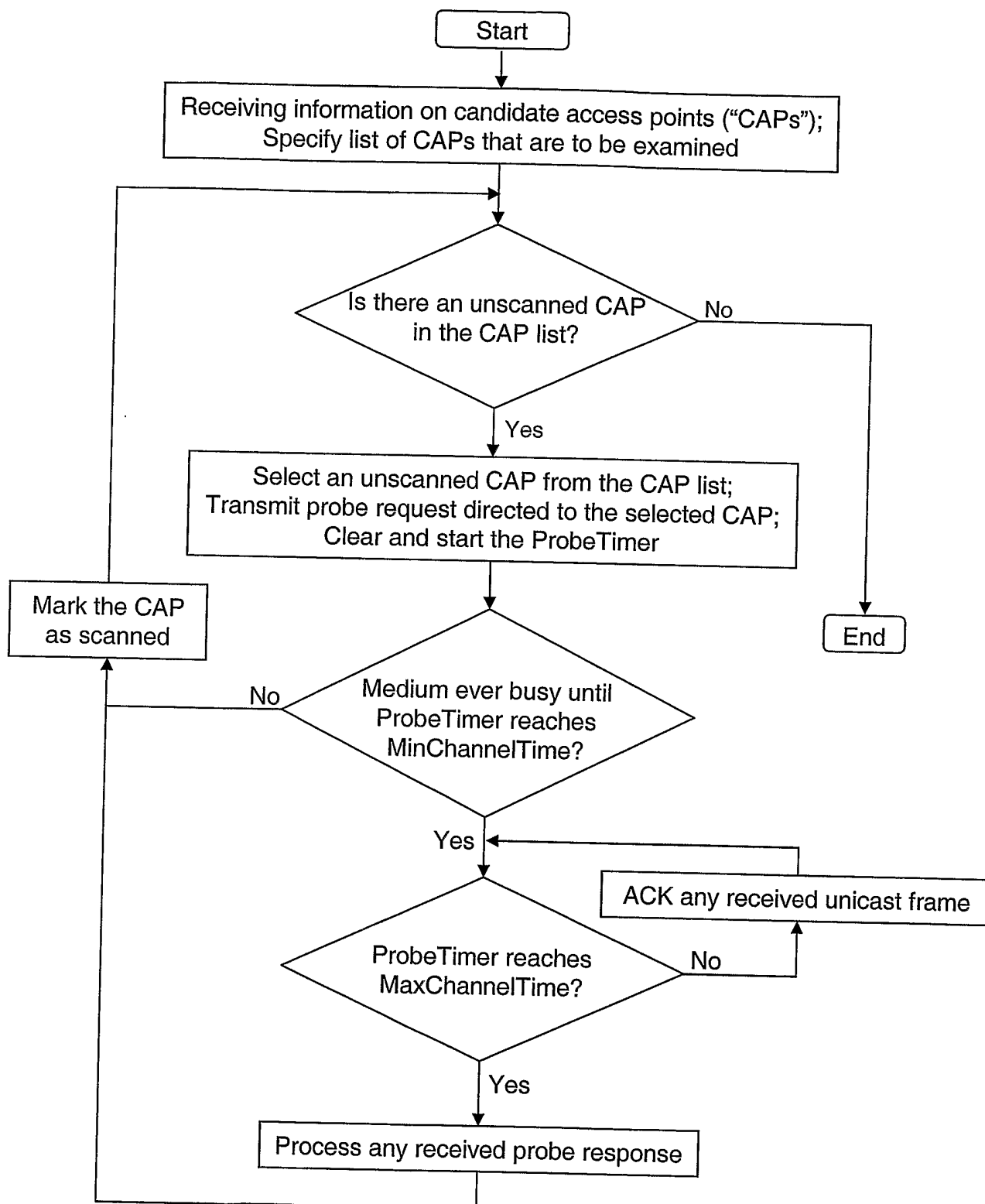


FIG. 13

14/28

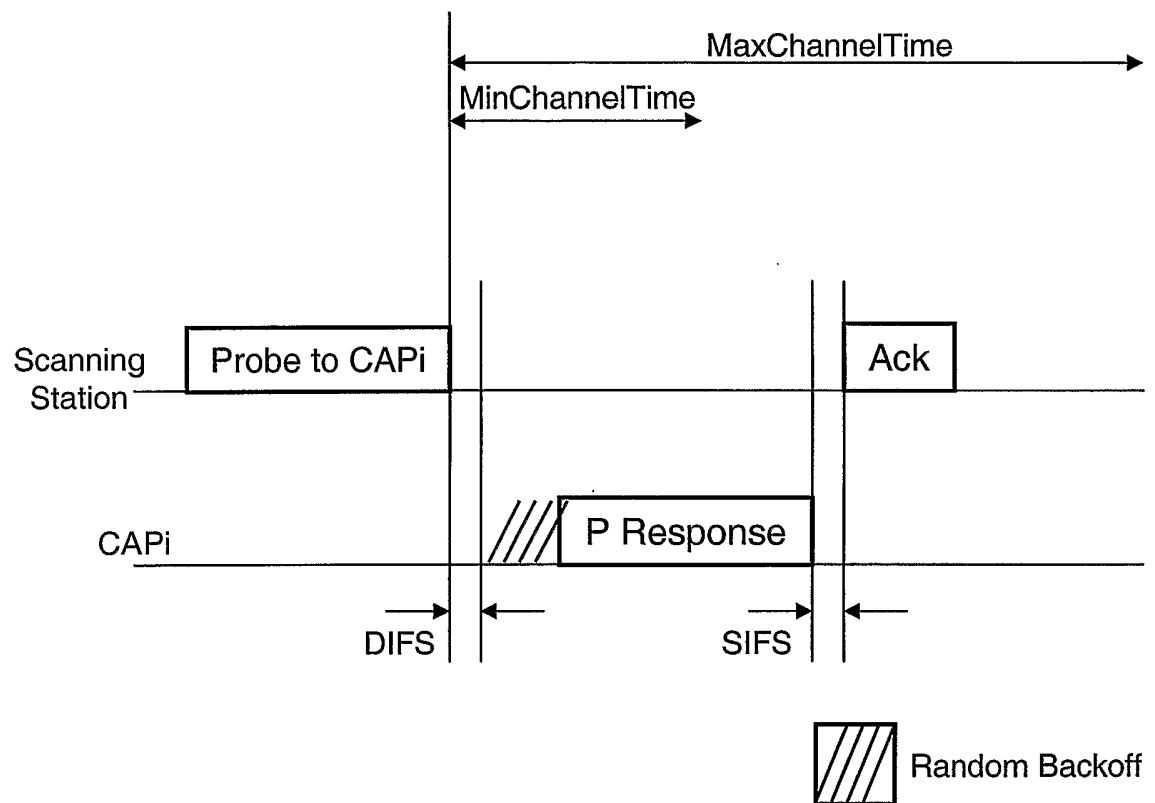


FIG. 14

15/28

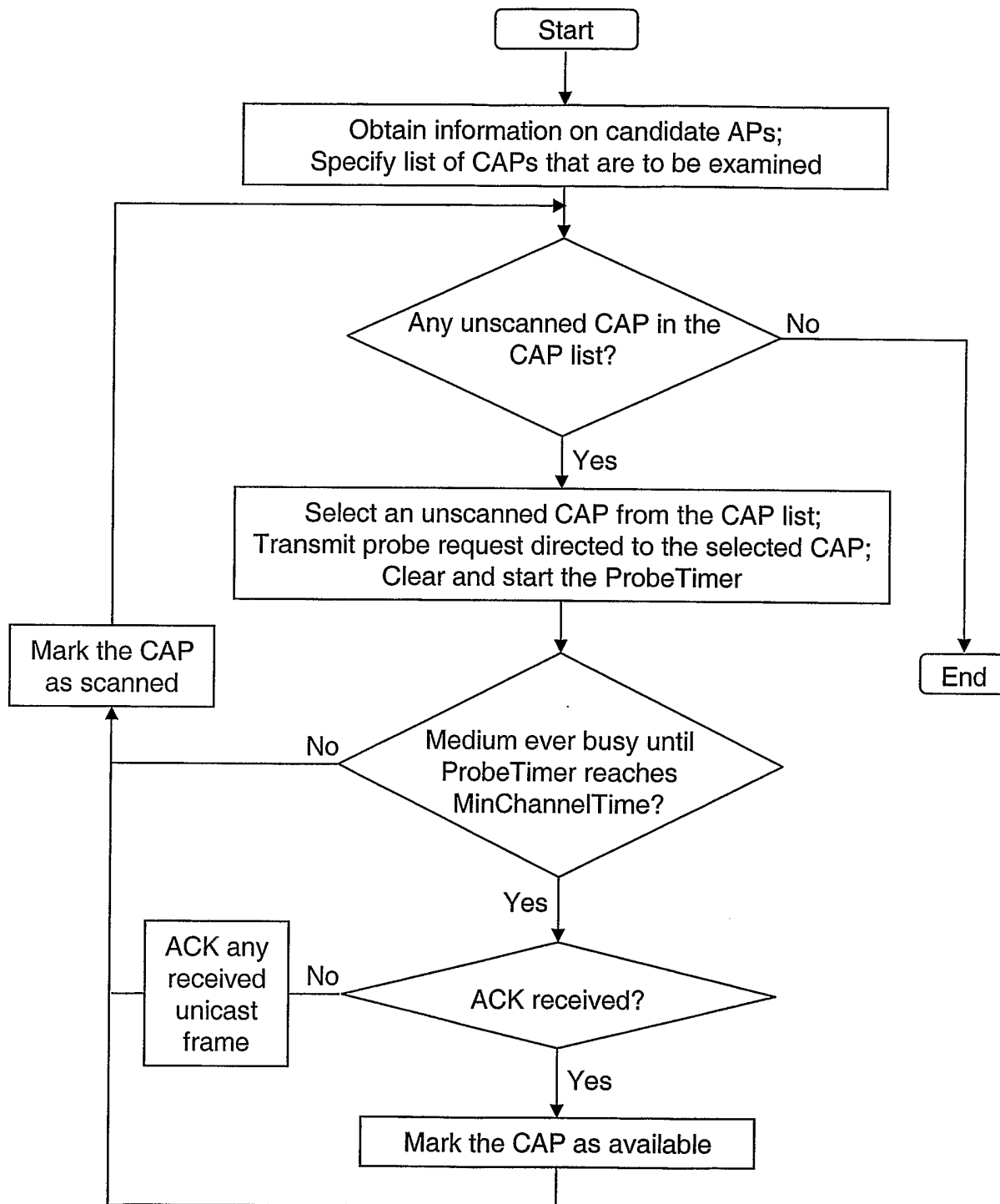


FIG. 15

16/28

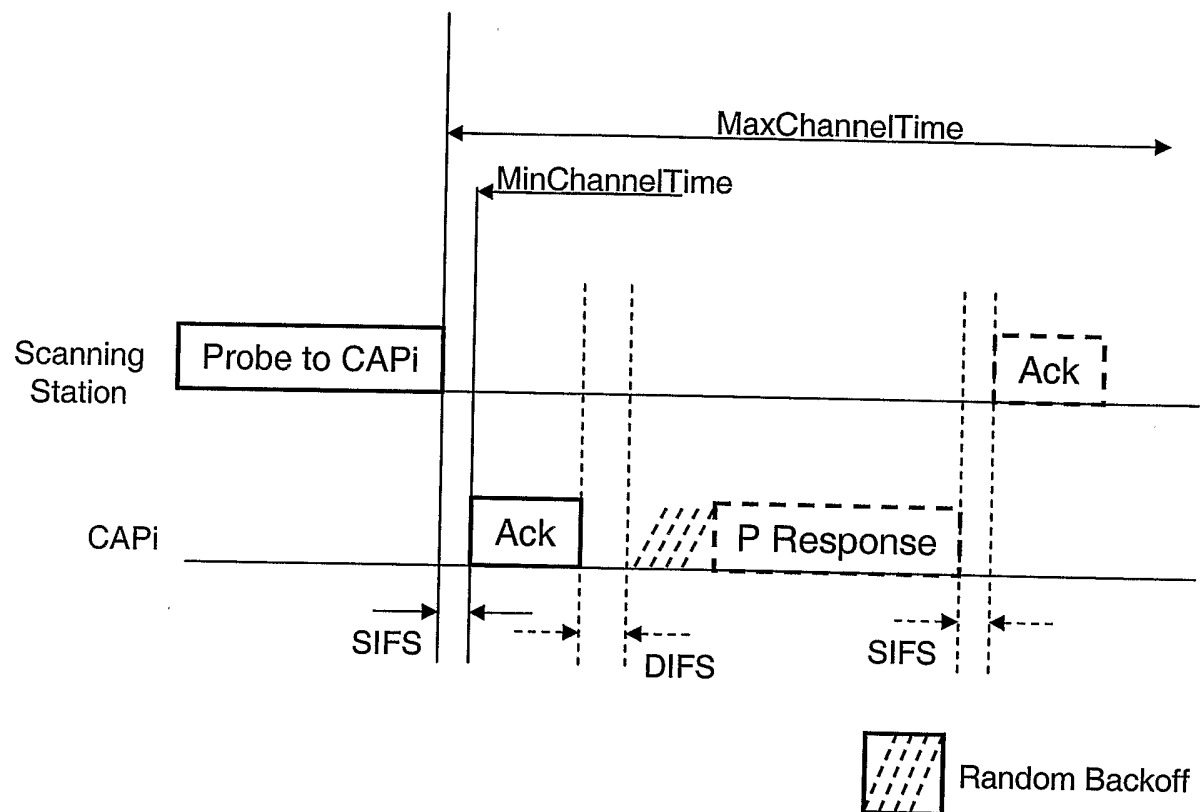


FIG. 16

17/28

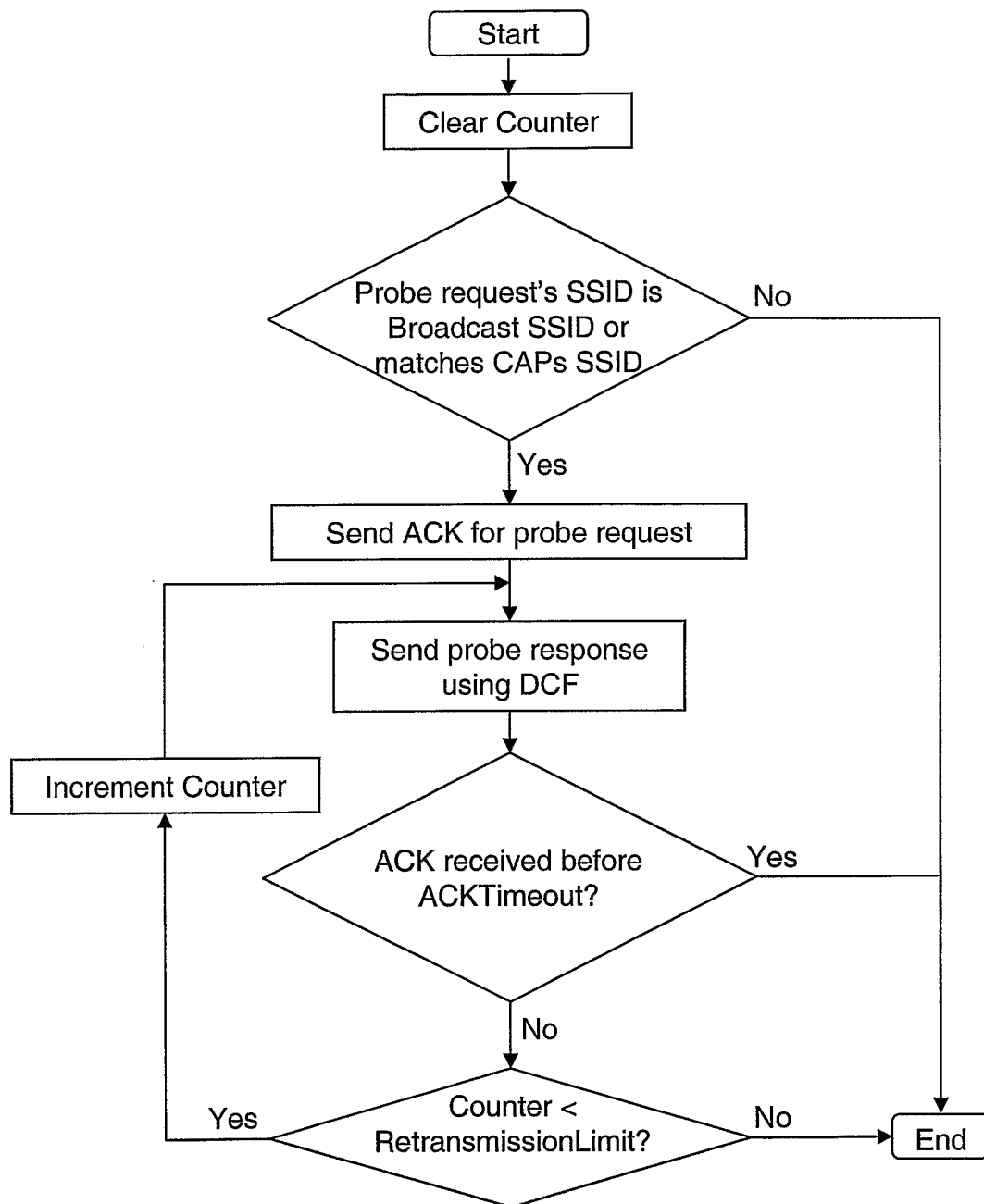


FIG. 17

18/28

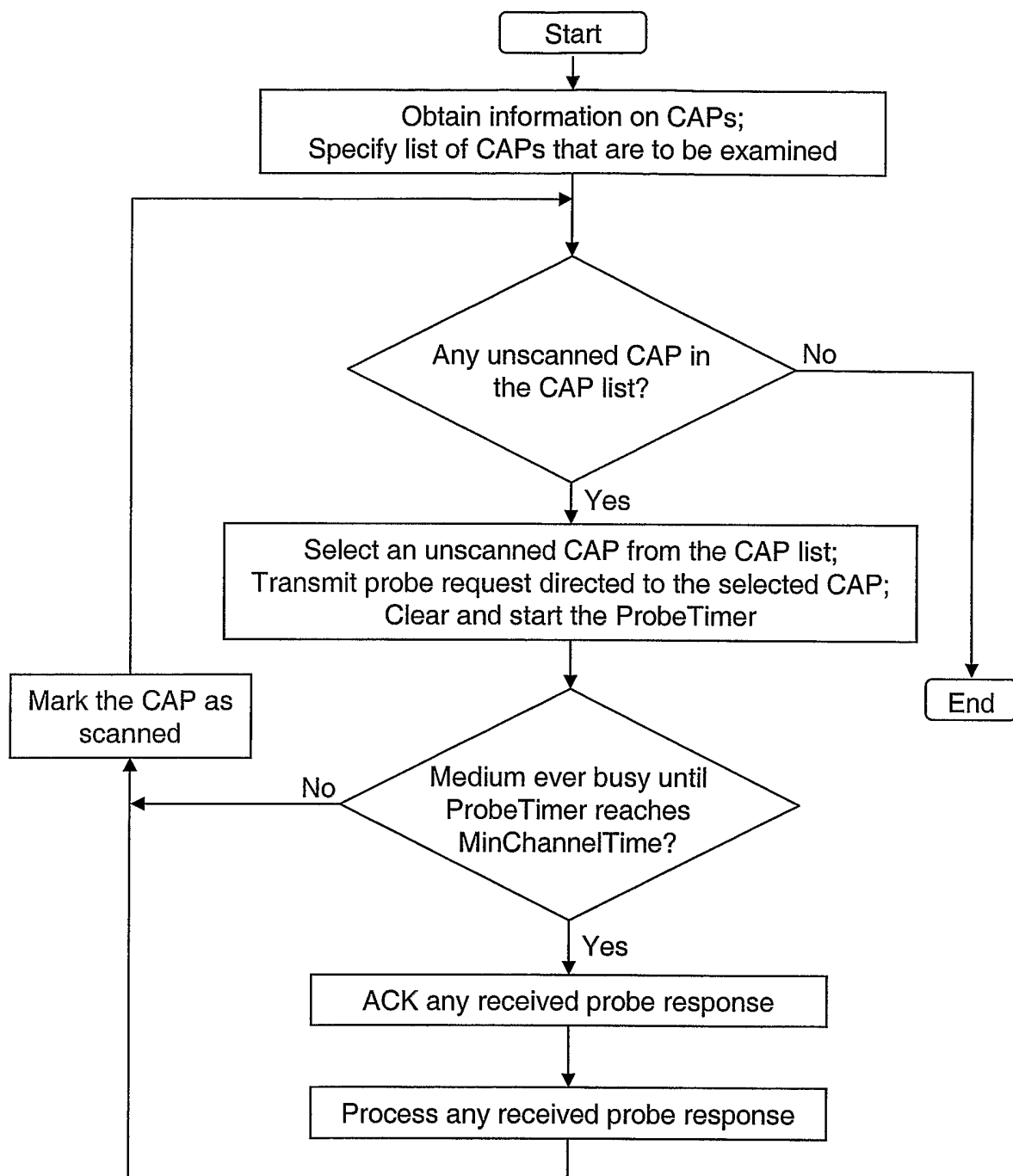


FIG. 18

19/28

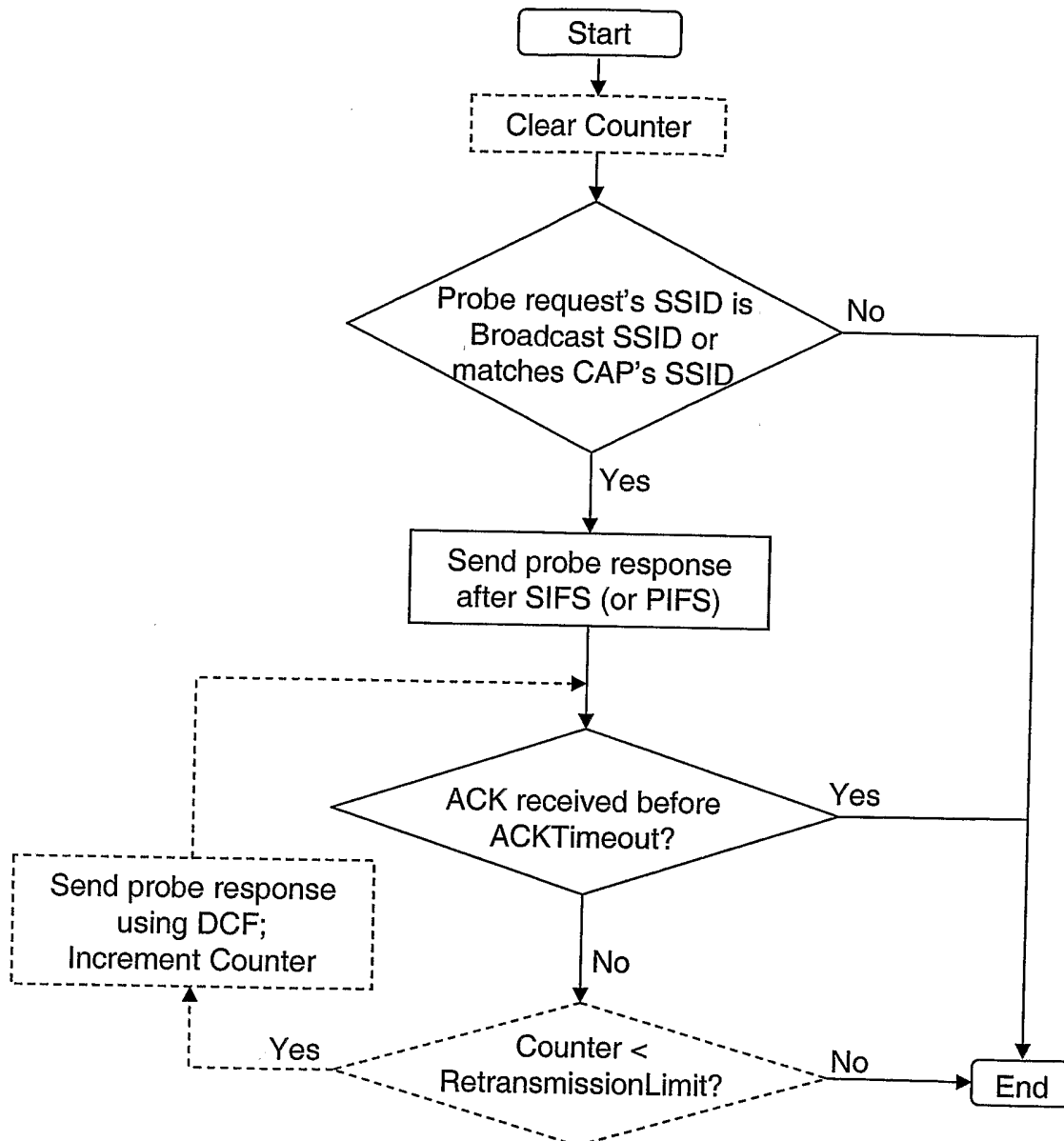


FIG. 19

20/28

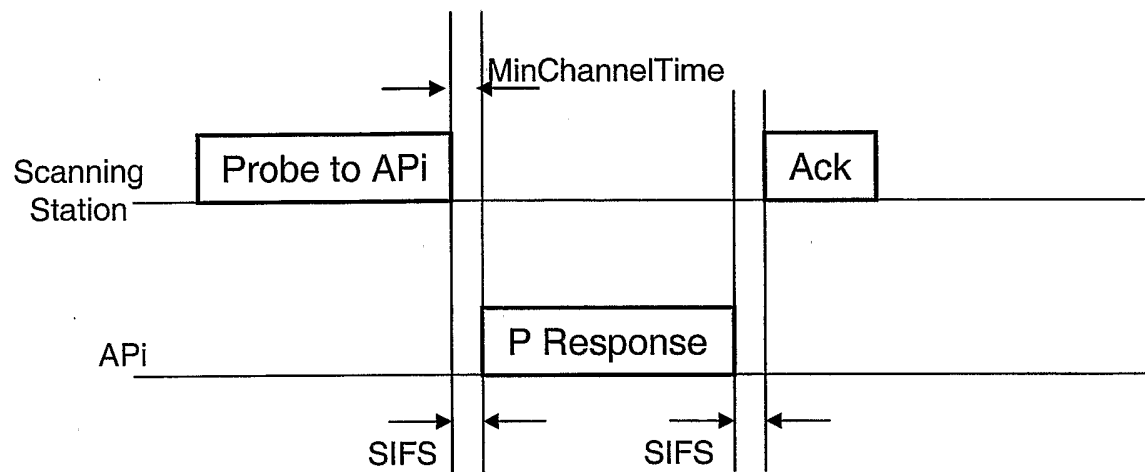


FIG. 20

21/28

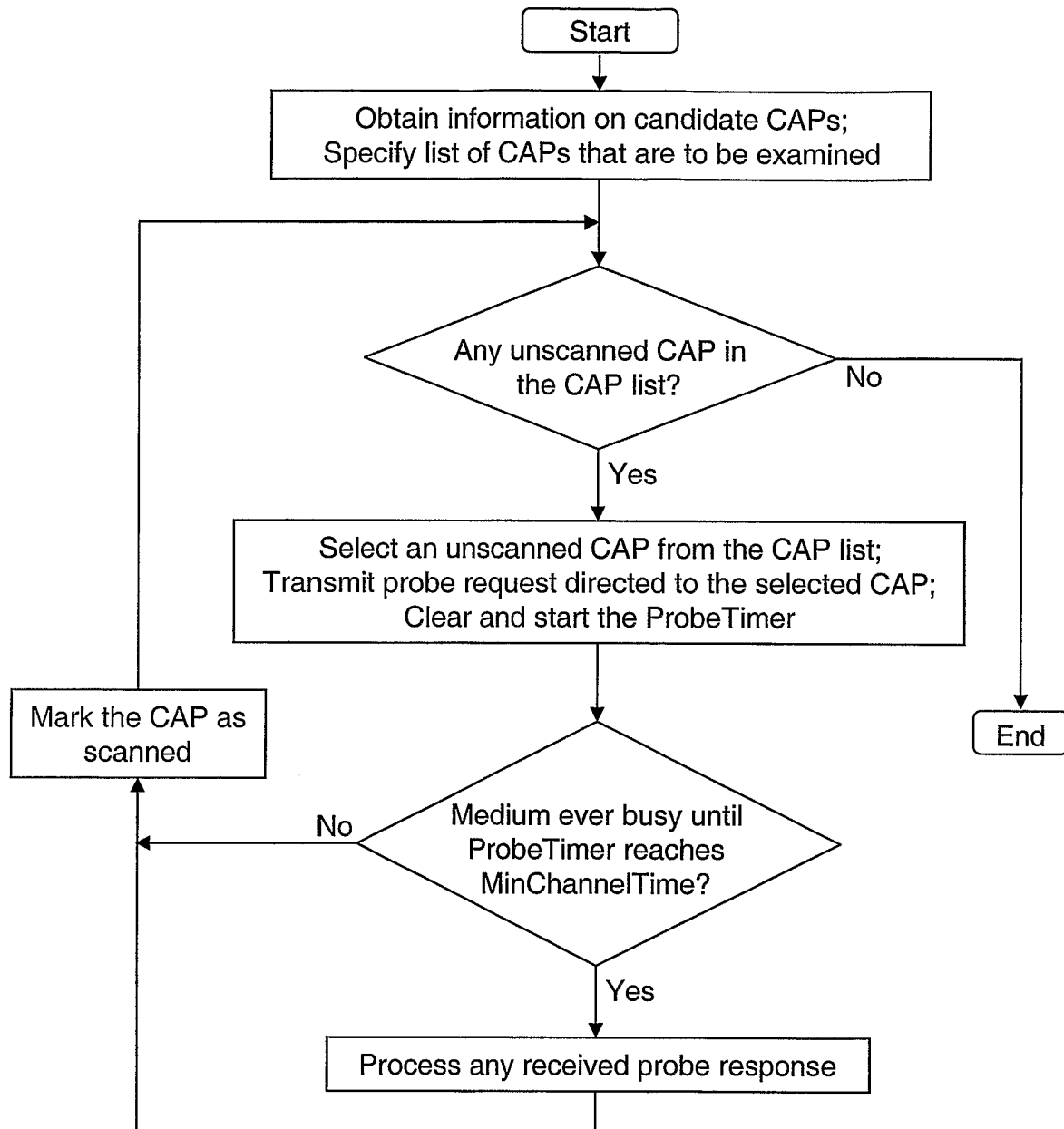


FIG. 21

22/28

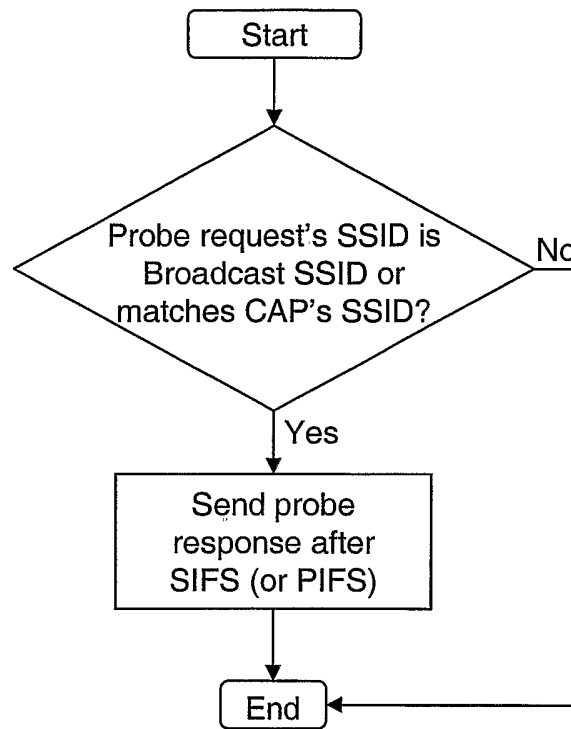


FIG. 22

23/28

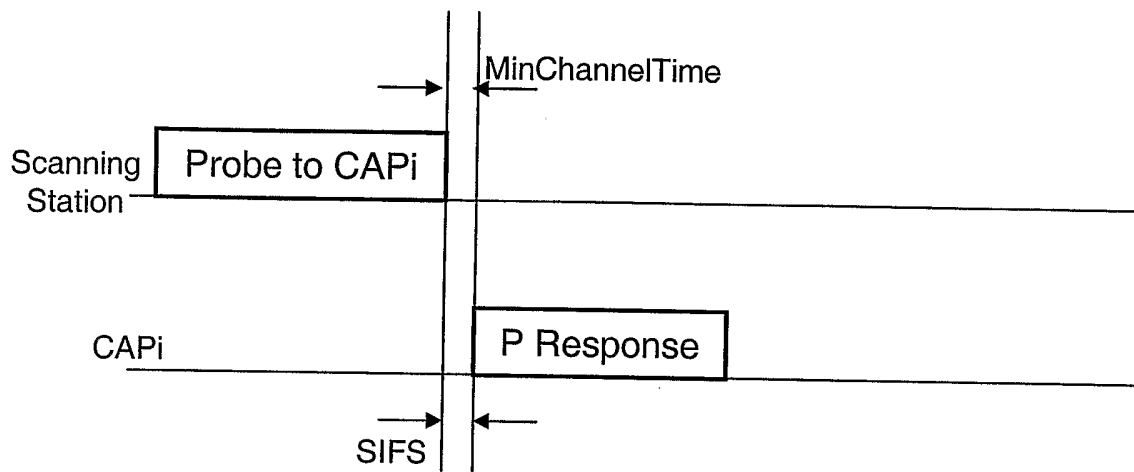


FIG. 23

24/28

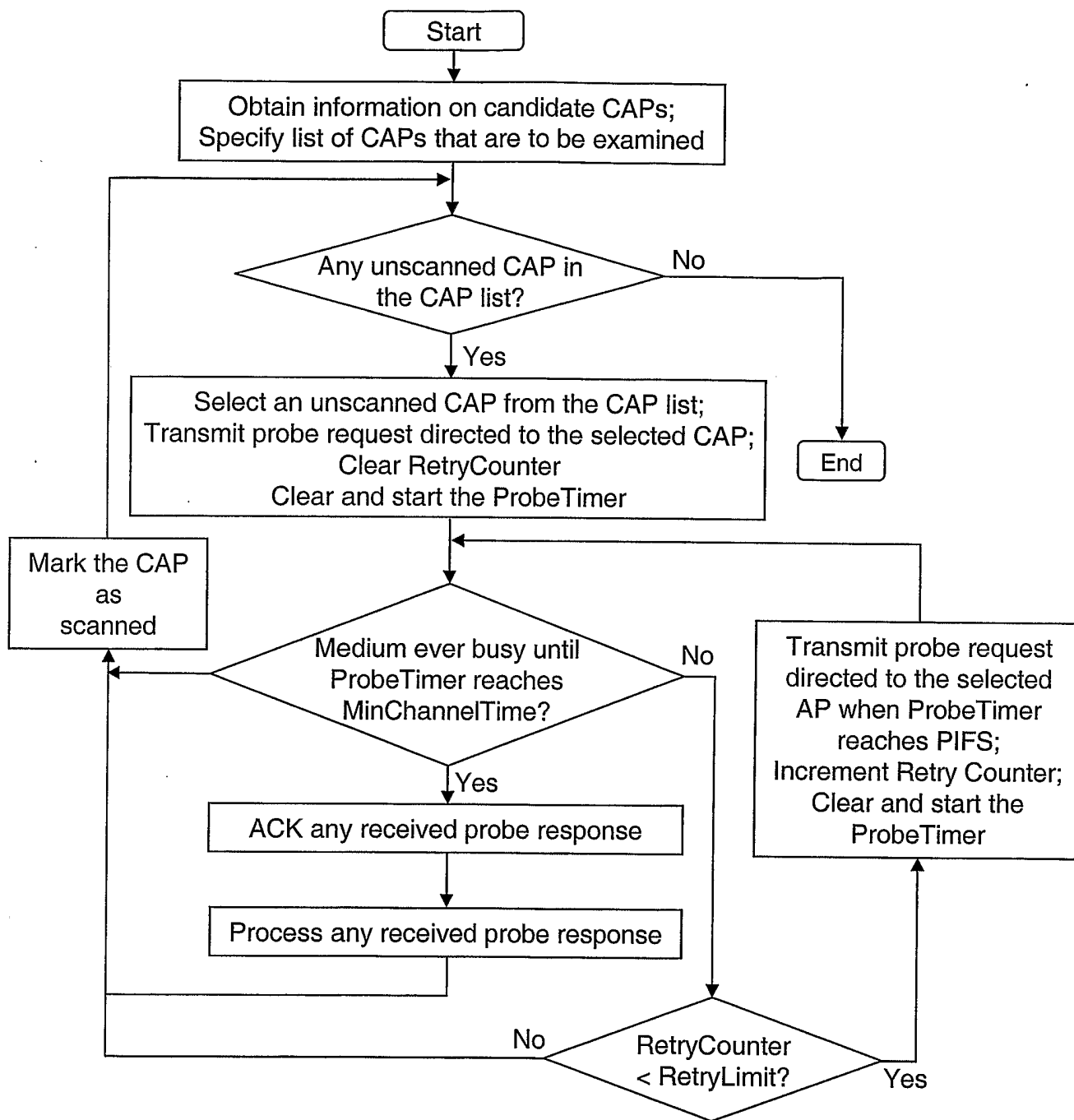


FIG. 24

25/28

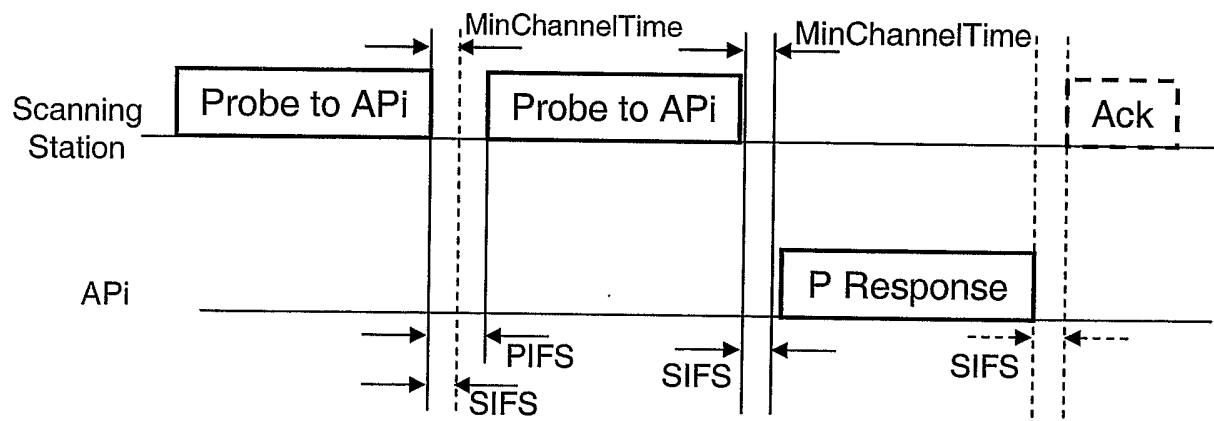


FIG. 25

26/28

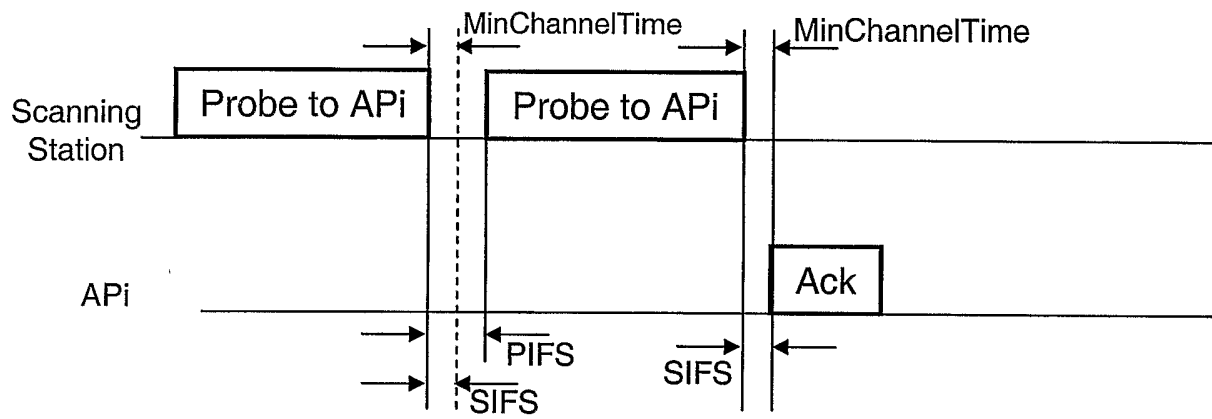


FIG. 26

27/28

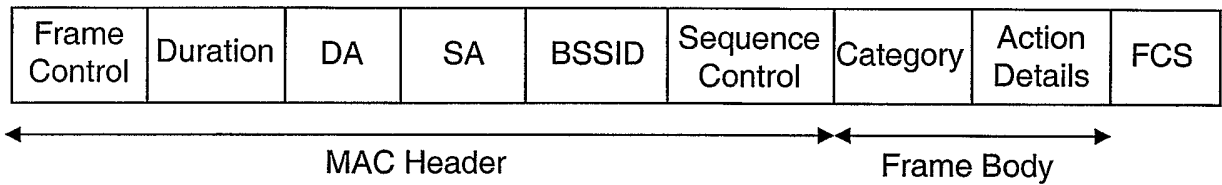


FIG. 27

28/28

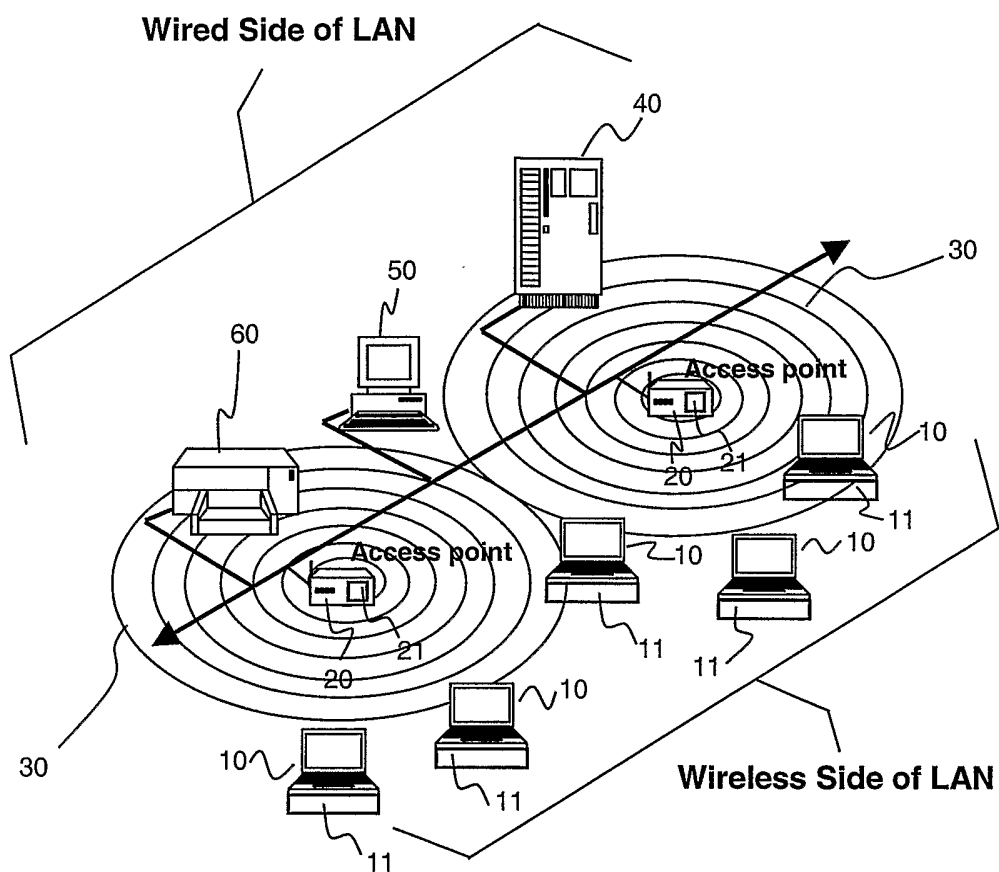


FIG. 28

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US20/04010390

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20; H04B 7/00

US CL : 455/424, 515, 516

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 455/424, 515, 516

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P --- Y, P	US 2002/0183061 A1 (MOORE) 05 December 2002 (05.12.2002), column 1 lines 0008-0010. column1 lines 0004-0007.	1-20 ----- 21-47
Y, P	US 2004/0114535 A1 (HOFFMANN et al) 17 JUNE 2004 (17.06.2004), column 1 lines 0006-0011.	21-47

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

☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

"T"

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

"X"

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

"Y"

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

"&"

document member of the same patent family

Date of the actual completion of the international search

31 July 2004 (31.07.2004)

Date of mailing of the international search report

27 AUG 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703) 305-3230

Authorized officer

Sheila B. Smith

Telephone No. (703)305-0104

Handwritten signature