

TITLE OF THE INVENTION

Roaming Queries Prior to Association/Authentication

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates, for example, to a mechanism for wireless networks such as IEEE 802.11 to enable roaming queries prior to association/authentication while maintaining the advantages of power saving mechanisms.

DESCRIPTION OF THE RELATED ART

[0002] When wireless local area network (WLAN) access points are shared by multiple service providers (e.g. in the case of airport hotspots in which the airport owns the access point, but service is provided by other operators, such as T-Mobile), a technique called "virtual AP" can be used to allow sharing of the access point. From the mobile station's point of view it is as if there were several different access points. Multiple service set identifiers SSIDs can be used by the same access point to support the different service providers.

[0003] In traditional roaming cases, the mobile station has a roaming client (e.g. T-Mobile™ connection manager, Boingo™ connection manager, or the like) that has a roaming directory. The roaming directory can be a list of SSIDs for access points to which the station can connect. For a mobile station to select the access point and connect, a valid SSID must be used. Thus, the access point should broadcast that SSID and the mobile station should know it. In other words, currently the burden of determining whether the mobile station can or cannot access a given access point based on a roaming agreement is left

completely to the mobile station, and is traditionally solved by downloading a long list of SSIDs to the mobile station.

[0004] With current virtual AP solutions, the access point cannot simultaneously broadcast all the SSIDs supported. Therefore, if the mobile station does not detect a supported SSID in the beacons, the mobile station must perform active scanning: it must send a Probe Request to the access point providing a given SSID. If the access point supports it, it will return a positive answer. When roaming, the list of the mobile station preferred SSIDs can be rather long, which can result in extensive signaling to obtain a valid SSID. For example, a mobile station may have 200 SSIDs, which is not an unusual number, and only the 189th may be supported. Thus, in such a circumstance, the mobile station must perform 189 queries. Optimizations have been proposed according to which a list of SSIDs can be provided in beacons and Probe Response messages. However, the list is still limited, and therefore the problem still exists.

[0005] Some ideas have been presented to extend the Probe Request and Probe Response frames in such a way that the mobile station can query the network for roaming information or alternatively to define two new management frames to carry the request and the reply. Two options are possible: the mobile station queries for what realms are supported (not realistic, e.g. the list may be very long and therefore the solution does not scale), or the mobile station queries the network using its own Roaming ID and the network replies either yes or no. The second option is more realistic, but has a drawback: the access point may have to retrieve the information from the back end before being able to provide the information to the station, since it is not realistic to expect the access point to be preconfigured with all roaming info. Therefore, the access point may not be able to reply instantaneously to the mobile station request. However, it may be necessary that the Probe Response shall be sent to the

mobile station no later than a very short period of time (e.g. 5ms, as currently defined in the WiFi Alliance) from the receipt of the Probe Request. This requirement may be needed for power saving reasons.

[0006] There is the need to allow a mobile station to discover whether it has roaming in a certain access point (AP) without the need for the mobile station to try to authenticate/associate and without requiring continuous probing for different service set identifiers (SSIDs).

[0007] Another scenario in which improvement may be required may be in the support of wireless information services, for example, 802.21 Information Service (IS) in 802.11. The idea is to allow the mobile station to access IS information before authentication/association so that the mobile station can decide whether or not it wants to connect. Support of wireless information services such as 802.21 Information Service may require that Probe Request and Probe Response information carry the queries and replies, such as 802.21 IS queries and replies. Solutions are needed to enable this function, since the queries are typically not processed by the access point but by an information server, such as an 802.21 server in the network, and therefore the reply may not be available within a very short period of time from the receipt of the Probe Request.

[0008] It may also be important to be able to identify services that are available from an access point before attachment, specifically for information defined in wireless network information services standards, such as IEEE 802.21 Information Service.

SUMMARY OF THE INVENTION

[0008a] According to a first aspect of the present invention, there is provided a terminal, comprising: a processor configured to prepare a first request

message regarding information desired from an access point; a transmitter configured to transmit the first request message to the access point; and a receiver configured to receive from the access point a first response message in response to the first request message requesting the terminal to come back, wherein the receiver configured to receive the first response message including a query identifier that references the information desired, wherein the processor is further configured to control the terminal to wait a predetermined amount of time and to prepare a second request message regarding the information desired responsive to the first response message, wherein the transmitter is further configured to transmit the second request message including the query identifier to the access point, and wherein the receiver is further configured to receive a second response message from the access point providing the information desired.

[0008b] According to a second aspect of the present invention, there is provided an access point, comprising: a receiver configured to receive from a terminal a first request message regarding information desired; a processor configured to analyze the first request message and prepare a first response requesting the terminal to come back; and a transmitter configured to transmit to the terminal the first response message, wherein the transmitter is configured to transmit the first response message including a query identifier that references the information desired, wherein the processor is further configured to obtain the information desired from a backend, wherein the receiver is further configured to receive a second request message including the query identifier regarding the information desired responsive to the first response message, wherein the processor is further configured to analyze the second request message and prepare a second response message providing the information desired, and wherein the transmitter is configured to transmit the second response message to

the terminal.

[0008c] According to a third aspect of the present invention, there is provided a terminal, comprising: transmission means for transmitting a first request message to an access point; reception means for receiving from the access point a first response message requesting the terminal to come back; and wait means for waiting a predetermined amount of time, wherein the reception means is configured to receive the first response message including a query identifier that references the information desired, wherein the transmission means is further configured for transmitting to the access point a second request message regarding the information desired responsive to the first response message and including the query identifier, and wherein the reception means is further configured for receiving a second response message from the access point providing the information desired.

[0008d] According to a fourth aspect of the present invention, there is provided an access point, comprising: reception means for receiving from a terminal a first request message regarding information desired; transmission means for transmitting to the terminal a first response message requesting the terminal to come back; and processing means for obtaining the information desired from a backend, wherein the transmission means is configured to transmit the first response message including a query identifier that references the information desired, wherein the reception means is further configured for receiving a second request message including the query identifier regarding the information desired responsive to the first response message, and wherein the transmission means is further configured for transmitting a second response message from the access point providing the information desired.

[0008e] According to a fifth aspect of the present invention, there is provided

a method of providing information in a communication system, the method comprising: sending, by a terminal, to an access point a first request message regarding information desired; receiving, by the terminal, from the access point a first response message requesting the terminal to come back; receiving by the terminal the first response message including a query identifier; sending, by the terminal, to the access point a second request message including the query identifier regarding the information desired responsive to the first response message; and receiving, by the terminal, from the access point a second response message providing the information desired.

[0009] Embodiments of the present invention provide, for example, a method in which an access point receives a query from a station for some information, the access

point identifies whether it has the information desired and informs the station that the station needs to re-request to obtain the information.

[0010] Embodiments of the present invention also provide, for example, a method in which an access point receives a query from a station carrying a request and data for information service such as 802.21 Information Service (IS), the access point identifies whether it has the information desired and informs the station that the station needs to re-request to obtain the reply to the 802.21 IS request.

[0011] Embodiments of the present invention also provide, for example, an apparatus that can be used as an access point. The apparatus includes means for receiving a request for information from a station. The apparatus also include means for processing the request to determine whether the information desired is present in the apparatus. The apparatus further includes means for informing the station that the station needs to re-request in order to obtain the information.

[0012] In informing the station of the need to re-request, a query identifier can be included that can enable the station to re-request without having to repeat the details of the request. Additionally, in informing the station of the need to re-request, a time delay value can be provided to indicate to the station how long to wait before requesting the information again.

[0013] The request can be either a repeated request, or it may be a new request. Thus, the first request and the re-request may be two different kinds of messages.

[0014] Embodiments of the present invention can provide, for example, a terminal including a transmitter and a receiver. The terminal may be configured to prepare a first request message regarding information desired from an access point, transmit the first request message to the access point, receive from the access point a first response message requesting the terminal to come back, wait a predetermined amount of time, transmit to the access point a second response

message regarding the information desired responsive to the first probe response, and receive a second probe response from the access point providing the information desired.

[0015] Embodiments of the present invention additionally provide, for example, an access point including a transmitter and a receiver. The access point is configured to receive from a terminal a first probe request regarding information desired, transmit to the terminal a first probe response requesting the terminal to come back, obtain the information desired from a backend, receive a second probe request regarding the information desired responsive to the first probe response, and transmit a second probe response from the access point providing the information desired.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] In the following, the present invention will be described in greater detail based on preferred embodiments with reference to the accompanying drawings in which:

[0017] Fig. 1 illustrates a signal flow diagram according to an embodiment of the present invention;

[0018] Fig. 2 illustrates a processing flow diagram of an access point according to an embodiment of the present invention;

[0019] Fig. 3 illustrates a signal flow diagram in which the access point refers to an 802.21 information server to retrieve the requested information; and

[0020] Fig. 4 illustrates a simplified block diagram of a communication system according to an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0021] The preferred embodiments will now be described with regard to an example embodiment that includes an access point. The access point may be configured to be shared by multiple networks, and may be able to support IEEE 802.21 Information Service.

[0022] Certain embodiments of the present invention can enable an access point receiving a query from a mobile station for some information elements to reply to the mobile station with an indication that the access point can provide the information requested but that the access point cannot provide it right away. This may occur when the access point does not have the information requested at the moment the request is received and the access point is unable to retrieve the information in real-time. Certain embodiments of the invention enable such an access point to indicate to the mobile station that the mobile station needs to query again for the information. This indication may be referred to as a "come back" indication.

[0023] The access point may optionally return a query identifier (QueryID) to be used by the terminal to query the access point again without the need for indicating again the information elements required. The value of the query identifier may be unique for the access point. Thus, when more than one information element (IE) is requested and is not available instantaneously at the access point, the query can be easily referenced in a subsequent query without the need to repeatedly detail the information desired. Thus, radio resources may be conserved.

[0024] The access point may also optionally return a time value (ComeBackDelay) determined by the access point and indicating how long the terminal ought to wait before querying the access point again.

[0025] The Probe Request/Response messages can be extended by adding

new information elements. A mobile station can specify in a probe request what information elements it is requesting. In a probe response the mobile station can get the requested information if supported by the access point. Some 'fixed' information elements may always be present.

[0026] Figure 1 depicts a flow according to an embodiment of the present invention. The mobile station 110 may send a Probe Request 112 extended to contain a list of IEs (IE1, IE2, IEn) that are being requested. The access point 120 may determine that it cannot return IE_{ji}, IE_{jm} immediately, or that it cannot immediately provide a reply to the mobile station query. This latter situation may occur if, for example, the mobile station 110 has provided a RoamingID. The access point 120 returns in a "come-back" Probe Response 122 the list of info requested minus IE_{ji}, IE_{jm}. The access point 120 may optionally provide the mobile station 110 with a QueryID. The QueryID can serve as a ticket that references the original query in the form of Probe Request 112, and which can be used to reduce the length of a second request from the mobile station 110. The access point 120 may also optionally provide a ComeBackDelay parameter indicating how long the mobile station 110 should wait before sending a "come-back" Probe Request 114, which may be a second request for the same information in order to obtain the missing information.

[0027] The mobile station 110 may wait for a certain amount of time and send a "come-back" Probe Request 114 optionally containing the QueryID to relate the new query to the previous query. The amount of time may be the amount of time indicated by ComeBackDelay, an amount determined by the mobile station 110, or a predetermined amount of time. The access point 120 may then return IE_{ji}, IE_{jm} in a Probe Response 126. If the mobile station 110 does not re-query by sending the come-back Probe Request 114, the access point 120 may delete the information after a certain amount of time to avoid a denial of service

(DoS) attack on the access point 120 resulting from the generation of a multitude of queries in order to consume access point memory.

[0028] Meanwhile, while the mobile station 110 is waiting to re-request, the access point 120 may obtain IE_{ji}, IE_{jm} from a backend 130, by means of a retrieval request 124. The backend 130 may process the retrieval request 124 and return IE_{ji}, IE_{jm} to the access point 120 in a data message 132. The time between the retrieval request 124 and the data message 132 may typically be much greater than 5 ms.

[0029] The mobile station 110 does not need to remain active while waiting to send the "come-back" Probe Request 126, therefore it can save power, as opposed to having to stay active — waiting for an answer to its original Probe Request 112. Because the mobile station 110 re-requests the information, the timing of the re-request can be at the convenience of the mobile station 110.

[0030] If a mobile station is connected to a first access point (AP₁) and is actively exchanging data frames with AP₁, but wants to retrieve information from a target access point (AP₂), the mobile station does not need to remain on the AP₂ channel while waiting to send the "come-back" Probe Request. As with an inactive mobile station, the mobile station can come back to the AP₂ channel when an appropriate amount of time has elapsed. Thus, unnecessary processing within the mobile station can be avoided.

[0031] The access point may retrieve the information using a protocol like Control And Provisioning of Wireless Access Points (CAPWAP) or Authentication, Authorization, and Accounting (AAA).

[0032] The Probe Request can be extended with the Roaming ID provided in a NAI Request Information Element. The Probe Request can also be extended to support a variety of IEs to support information service, such as 802.21 Information Service (IEs can be those defined in 802.21 specifications). The

Probe Request can be further extended to support a QueryID field.

[0033] Similarly, the Probe Response can be extended to support a variety of IEs to support 802.21 Information Service (IEs can be those defined in 802.21 specifications). The Probe Response can be extended to support a QueryID field. The Probe Response can also be extended to support a ComeBackDelay field.

[0034] Certain security considerations should be borne in mind. If the access point stores the results of a query for a given mobile station only until the mobile station sends the "come-back" query, a hacker who intercepts the "come-back" response from the access point to a legitimate mobile station could send a new request to the access point before the legitimate mobile station and cause the access point to purge the information retrieved for the mobile station. Thus, the mobile station/access point would fail on the come-back query because the information is no longer available at the access point. One way to reduce the risk of this attack is for the access point to store the mobile station MAC address. However, a hacker may be able to spoof the mobile station MAC address because the mobile station is not yet authenticated/associated with the access point. Solutions are being introduced to stop MAC hijacking/spoofing in wireless networks such as IEEE 802.11 networks, but they will likely apply only to authenticated/associated mobile stations. Additionally, certain implementations may allow a mobile station to use a well known or random MAC address to send/receive Probe Request/Response messages, thereby preventing a network from tracking a roaming mobile station that performs active scanning (i.e. probing).

[0035] Thus, storing the MAC address of the mobile station associated with a query in the access point would not entirely eliminate the security concern discussed here. A simpler mechanism is for the access point to cache the result

of the query for a time that is predicted to be slightly longer than the time necessary for the mobile station to send the come-back query.

[0036] The present invention may advantageously enable current power saving mechanisms. For example, the mobile station does not need to remain active while waiting to send the "come-back" Probe Request, therefore enabling power saving. Also, if the mobile station is connected to a first access point (API) and is actively exchanging data frames with API, but wants to retrieve information from a target access point (AP2), the mobile station does not need to remain on the AP2 channel while waiting to send the "come-back" Probe Request. Additionally, certain embodiments of the invention do not require the access point to use more memory than it would if it were configured to have all the information available. In fact, the access point can store the result of the query in a generic way so that other queries may be returned the same information (if relevant). Thus, the access point may maintain a cache of frequently requested information, thereby reducing the number of times that a come-back must occur.

[0037] Certain embodiments of the present invention can enable an access point receiving a query from a mobile station for some information elements, the access point not having the information requested at the moment the request is received, and the access point being configured to retrieve the information in real-time, to reply to the mobile station with an indication that the access point is able to provide the information requested but that the access point cannot provide it right away. Also, certain embodiments of the present invention can enable the access point to indicate the terminal that the terminal needs to query again for the information.

[0038] The access point may optionally return a query identifier QueryID (whose value is unique for the access point) to be used by the terminal to query

the access point again without the need for indicating again the information elements required (this may be useful when more than one information element IE is requested and is not available instantaneously at the access point, and performing a new query by providing again the list of IEs would imply a waste of radio resources). The access point may optionally return also a time value ComeBackDelay determined by the access point and indicating how long the terminal shall wait before querying the access point again.

[0039] As shown in Figure 2, an access point may receive 210 a request for information from a mobile station. The access point may then decide 220 whether the information can be provided immediately. If it can, the access point may provide 230 the information. Otherwise, the access point may suggest 240 that the mobile station re-request the information at a later time.

[0040] As explained above, when the access point suggests 240 that the mobile station re-request the information at a later time, the access point may provide a query ID to help simplify the re-request and a delay value or window that may enable the mobile station to send the re-request at an expedient time.

[0041] As shown in Figure 3, the mobile station may send a probe request to the access point requesting data. The access point may return a come-back probe response to the mobile station, providing a query ID and a come back delay. The query ID may uniquely identify the query with a serial number. The query ID may be used by the mobile station to reference the original query. The come back delay may specify a delay in seconds or fractions thereof that the mobile station should wait before requesting the data again. During the delay, while the mobile station is waiting to request the data again, the access point may query an information server such as an 802.21 information server for the data. The information server may reply with the data, but may take significantly longer than 5 msec to reply. The delay may be designed to

account for the length of time that it is expected that the information server will take to reply. After the delay has completed, the mobile station sends a come-back probe request to the access point. The come-back probe request may simply identify the previous request using the query ID provided by the access point. The access point can then respond with the desired information.

[0042] Figure 3 illustrates an embodiment of the present invention including an information server such as an 802.21 information server 330. The mobile station 310 may send a Probe Request 312 including Type_of_802.21_IS_query and 802.21_query_data. The access point 320 may determine that it cannot return the requested data immediately and return in a “come-back” Probe Response 322 optionally including a QueryID and a ComeBackDelay. The determining and return the come-back Probe Response 322 may occur within an approximately 5 ms window.

[0043] The mobile station 310 may wait for a certain amount of time, which may correspond to the ComeBackDelay information, and may send a “come-back” Probe Request 314 optionally containing the QueryID to relate the new query to the previous query. The access point 320 may then return Type_of_802.21_IS_reply and 802.21_reply_data in a Probe Response 326.

[0044] Meanwhile, while the mobile station 310 is waiting during the ComeBackDelay time, the access point 320 may submit 802.21_query_data in an 802.21_IS_query 324 to an 802.21 Server 330. The 802.21 Server 330 may process the 802.21_IS_query 324 and return 802.21_reply_data in an 802.21_IS_reply 332 to the access point 320. The time between the 802.21_IS_query 324 and the 802.21_IS_reply 332 may typically be much greater than 5 ms.

[0045] Figure 4 shows an embodiment of a communication system 400 according to an embodiment of the present invention. As illustrated a mobile

station 410 may be able to communicate with an access point 420 over a communication medium 440, which may, for example, be a wireless connection through air or space.

[0046] The mobile station 410 may include a transmitter 412 configured to send probe requests, a receiver 418 configured to receive probe responses and a processor 415. The processor 415 may be configured for a variety of tasks such as generating the probe requests, analyzing the probe responses, and controlling the receiver 418 and transmitter 412. The processor 415 may be implemented in hardware, software or some combination thereof, and may include a general purpose computer, an application specific integrated circuit (ASIC) or other hardware.

[0047] The access point 420 may include a transmitter 422 configured to send probe responses, a receiver 428 configured to receive probe requests and a processor 425. The processor 425 may be configured for a variety of tasks such as generating the probe responses, analyzing the probe requests, and controlling the receiver 428 and transmitter 422. The processor 425 may be implemented in hardware, software or some combination thereof, and may include a general purpose computer, an application specific integrated circuit (ASIC) or other hardware.

[0048] The access point 420 may also be equipped with a backend 430.

Although the backend 430 is shown attached to the access point 420, there is no requirement that the backend 430 be physically connected to the access point 420, and so the backend, which also may include a similar circuitry to the processors 415 and 425, may be located at the convenience of the implementer of the system.

[0049] The backend 430 may have various components and capabilities. For example, the backend 430 may include an informational database to assist the

access point 420. The backend 430 may also be configured to communicate with the access point 420 and respond to queries from the access point 420.

[0050] Although the invention is described with regard to request messages that are probe requests and response messages that are probe responses, it should be noted that other management frames could be used in place of the probe requests and probe responses. Such management frames can include management frames that do not carry user data. Accordingly, the invention is not limited to the particular form of the messages used.

[0051] It is noted that the present invention is not restricted to the above preferred embodiments but can be variously modified as would be apparent to one of ordinary skill in the art.

[0052] Thus, one having ordinary skill in the art will readily understand that the invention as discussed above may be practiced with steps in a different order, and/or with hardware elements in configurations that are different than those that are disclosed. Therefore, although the invention has been described based upon these preferred embodiments, it would be apparent to those of skill in the art that certain modifications, variations, and alternative constructions would be apparent, while remaining within the spirit and scope of the invention. In order to determine the metes and bounds of the invention, therefore, reference should be made to the claims.

WHAT IS CLAIMED IS:

1. A terminal, comprising:

a processor configured to prepare a first request message regarding information desired from an access point;

a transmitter configured to transmit the first request message to the access point; and

a receiver configured to receive from the access point a first response message in response to the first request message requesting the terminal to come back,

wherein the receiver configured to receive the first response message including a query identifier that references the information desired,

wherein the processor is further configured to control the terminal to wait a predetermined amount of time and to prepare a second request message regarding the information desired responsive to the first response message,

wherein the transmitter is further configured to transmit the second request message including the query identifier to the access point, and

wherein the receiver is further configured to receive a second response message from the access point providing the information desired.

2. The terminal of claim 1, wherein receiver configured to receive the first response message including a come back delay field, wherein the come back delay field defines the predetermined amount of time.

3. The terminal of claim 1, wherein the transmitter is configured to transmit management frames as the first request message and the second request message and the receiver is configured to receive management frames as the first response message and the second response message.
4. The terminal of claim 1, wherein the transmitter is configured to transmit probe requests as the first request message and the second request message and the receiver is configured to receive probe responses as the first response message and the second response message.
5. The terminal of claim 1, wherein the processor is configured to place the terminal in a sleep mode between receiving the first response message and sending the second request message.
6. An access point, comprising:
 - a receiver configured to receive from a terminal a first request message regarding information desired;
 - a processor configured to analyze the first request message and prepare a first response requesting the terminal to come back; and
 - a transmitter configured to transmit to the terminal the first response message,

wherein the transmitter is configured to transmit the first response message including a query identifier that references the information desired,

wherein the processor is further configured to obtain the information desired from a backend,

wherein the receiver is further configured to receive a second request message including the query identifier regarding the information desired responsive to the first response message,

wherein the processor is further configured to analyze the second request message and prepare a second response message providing the information desired, and

wherein the transmitter is configured to transmit the second response message to the terminal.

7. The access point of claim 6, wherein the first response message comprises a come back delay field, wherein the come back delay field defines when the second probe request is sent by the terminal.

8. The access point of claim 6, wherein the access point is further configured to determine whether the information can be provided substantially immediately, before transmitting the first response message.

9. The access point of claim 6, wherein the processor is further configured to

identify the information desired by reference to the query identifier.

10. The access point of claim 6, wherein the receiver is configured to receive management frames as the first request message and the second request message and the transmitter is configured to transmit management frames as the first response message and the second response message.

11. The access point of claim 6, wherein the receiver is configured to receive probe requests as the first request message and the second request message and the transmitter is configured to transmit probe responses as the first response message and the second response message.

12. The access point of claim 6, wherein the access point is configured to obtain the information desired from a remote information server.

13. A terminal, comprising:

transmission means for transmitting a first request message to an access point;

reception means for receiving from the access point a first response message requesting the terminal to come back; and

wait means for waiting a predetermined amount of time,

wherein the reception means is configured to receive the first response message including a query identifier that references the information desired,

wherein the transmission means is further configured for transmitting to the access point a second request message regarding the information desired responsive to the first response message and including the query identifier, and

wherein the reception means is further configured for receiving a second response message from the access point providing the information desired.

14. An access point, comprising:

reception means for receiving from a terminal a first request message regarding information desired;

transmission means for transmitting to the terminal a first response message requesting the terminal to come back; and

processing means for obtaining the information desired from a backend, wherein the transmission means is configured to transmit the first response message including a query identifier that references the information desired,

wherein the reception means is further configured for receiving a second request message including the query identifier regarding the information desired responsive to the first response message, and

wherein the transmission means is further configured for transmitting a second response message from the access point providing the information desired.

15. A method of providing information in a communication system, the method comprising:

sending, by a terminal, to an access point a first request message regarding information desired;

receiving, by the terminal, from the access point a first response message requesting the terminal to come back;

receiving by the terminal the first response message including a query identifier;

sending, by the terminal, to the access point a second request message including the query identifier regarding the information desired responsive to the first response message; and

receiving, by the terminal, from the access point a second response message providing the information desired.