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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 June 2004 (03.06.2004)

PCT

(10) International Publication Number
WO 2004/047397 A3

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US2003/036291

(22) International Filing Date: 13 November 2003 (13.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/426,756	15 November 2002 (15.11.2002)	US
10/346,988	17 January 2003 (17.01.2003)	US

(71) Applicant: CISCO TECHNOLOGY, INC. [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors: REBO, Richard, D.; 3800 Rosemount Blvd., Apt. 101F, Fairlawn, OH 44333 (US). GRISWOLD, Victor, J.; 2673 St. Albans Circle NW, North Canton, OH 44720 (US).

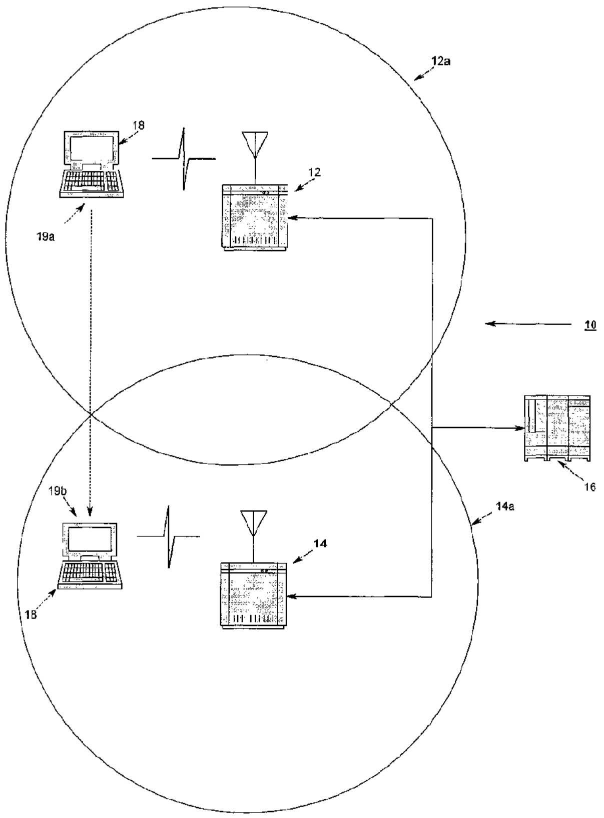
(74) Agent: GARRED, John, X.; Tucker Ellis & West LLP, 925 Euclid Avenue, 1150 Huntington Building, Cleveland, OH 44115-1475 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, 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, 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, UZ, VC, VN, YU, ZA, ZM, ZW.

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

[Continued on next page]

(54) Title: A METHOD FOR FAST, SECURE 802.11 RE-ASSOCIATION WITHOUT ADDITIONAL AUTHENTICATION, ACCOUNTING, AND AUTHORIZATION INFRASTRUCTURE



(57) Abstract: A method wherein an access point authenticates itself with neighboring access points and establishes secure and mutually authenticated communication channels with its neighboring access points. When an access point learns of a neighboring access point, it initiates an authentication with an authentication server through the neighboring access point. Once access points have mutually authenticated each other, whenever a station authenticates itself with a first access point, the first access point communicates the station's authentication context information, for example session key and session identifier, to each neighboring access point. Thus, when the station roams to a neighboring access point, the neighboring access point presents the station with a reauthentication protocol, for example LEAP reauthentication, and if the reauthentication is successful, communication between the station and the neighboring access point takes place immediately and no new EAP authentication needs to occur.

WO 2004/047397 A3

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
5 August 2004

Express Mail Label No. EV 310449675 US

TITLE OF THE INVENTION

A Method for Fast, Secure 802.11 Re-association Without Additional Authentication, Accounting, and Authorization Infrastructure

CROSS-REFERENCE TO RELATED APPLICATIONS.

This application claims the benefit of U.S. Provisional Application No. 60/ , filed November 15, 2002.

BACKGROUND OF THE INVENTION

The present invention relates generally to authentication protocols for roaming clients, and more specifically to a protocol for use by 802.11 wireless stations to quickly associate with a new access point while roaming.

Most current 802.11 network-level authentication protocols require a substantial amount of real time to re-establish a wireless station's connectivity to the network after that station roams from one access point (AP) to another access point. Typically, when a station associates with a first access point, it has to be authenticated through a central authentication server. When the station roams to a new access point, the station must again authenticate itself with the authentication server which does a full challenge request and response. A new accounting session is then established. This method relies on the initial authentication as a means for key rotation and generates a new accounting session for each roam, causing an unnecessary session teardown and restart.

This delay in re-establishing connectivity greatly impacts 802.11 Quality of service (QoS) to the point that some upper-level protocols, such as Voice-over-IP (VoIP), actually fail. Furthermore, each roam commonly necessitates interaction with a site's Authentication, Accounting, and Authorization (AAA) servers, resulting in a significant increase in server load, to the point at which some servers fail to provide the necessary rate of authentications requests for the 802.11 stations.

Other attempts to resolve this issue have utilized a variety of approaches. One approach is to use AP to AP communications to forward station AAA data, but these fail to use strong authentication between the APs. Another approach is to use "proxy" AAA servers closer in the network to the APs and stations, but these approaches generally require the addition of new network infrastructure devices at each network subnet. For some sites, this is an unacceptable cost, and other sites may not be able to incur the additional management burden.

Thus, the need exists for a secure method for authenticating a station when the station roams from one access point to another that decreases traffic to the authentication server.

BRIEF SUMMARY OF THE INVENTION

In view of the aforementioned needs, the invention contemplates a pre-authentication method wherein an access point authenticates itself with neighboring access points and establishes secure and mutually authenticated communication channels with its neighboring access points. When an access point learns of a neighboring access point, it initiates an authentication with an authentication server through the neighboring access point. In a preferred embodiment, the first access point initiates a Lightweight Extensible Authentication Protocol (LEAP) authentication with the second access point via an Authentication, Accounting, and Authorization (AAA) server.

Once access points have mutually authenticated each other, whenever a station authenticates itself with a first access point, the first access point communicates the station's authentication context information, for example session key and session identifier, to each neighboring access point. Thus, when the station roams to a neighboring access point, the neighboring access point presents the station with a reauthentication protocol, for example LEAP reauthentication, and if the reauthentication is successful, communication between the station and the neighboring access point takes place immediately.

One advantage of the present invention is that it requires no new devices or services to be added to the site's network. Another advantage of the present invention is that access points are mutually authenticated via a mechanism which is cryptographically as secure as the mechanism used for any client station on the network. The present invention does not require access points to be considered "more trusted than clients," which is a common security hole in most prior art implementations. Yet another advantage of the present invention is that it requires very little new protocol support implemented on the client stations. Still another advantage of the present invention is that the protocol leverages use of network history to optimize future network operations. Still yet another advantage of the present invention is that the protocol significantly diminishes the load on a site's AAA infrastructure.

Still other objects of the present invention will become readily apparent to those skilled in this art from the following description wherein there is shown and described a preferred embodiment of this invention, simply by way of illustration of one of the modes best suited for to carry out the invention. As it will be realized, the invention is capable of other different embodiments and its several details are capable of modifications in various obvious aspects all without from the invention. Accordingly, the drawing and descriptions will be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings incorporated in and forming a part of the specification, illustrates several aspects of the present invention, and together with the description serve to explain the principles of the invention. In the drawings:

FIG 1 is a block diagram of an 802.11 network with two access points;

FIG 2 is a block diagram showing the steps when a station roams from a first access point to a second access point;

FIG 3 is a block diagram illustrating the steps when a station roams from a first access point to a second access point after the first and second access points have established a secure and mutually authenticated communications channel between the first access point and the second access point.

DETAILED DESCRIPTION OF INVENTION

Throughout this description, the preferred embodiment and examples shown should be considered as exemplars, rather than limitations, of the present invention.

Referring first to Figure 1, there is shown a typical Extended Service Set

(ESS) 10. The ESS 10 comprises two access points (AP) 12, 14, each access point 12, 14 having a basic service set, 12a and 14a respectively associated with it. When a client or station (STA) 18, typically a wireless station or WSTA, is within a BSS, it communicates with the AP associated with that BSS. Typically the BSSs 12a and 14a have an overlap region and the STA 18 communicates with the AP, 12 or 14, it receives the strongest signal from. As shown in Figure 1, the STA 18 communicates via wireless communications to the APs 12 and 14. The APs 12 and 14 are connected via a secure, typically wired connection to an Authentication, Accounting, and Authorization (AAA) server 16. In the preferred embodiment, the AAA server 16 is a Remote Authentication Dial-In User Server (RADIUS server); however, other types of server's with authentication capabilities are acceptable.

As shown in Figure 1, the client, or station (STA), 18 will associate with an AP 12 while at a first position 19a. When the STA 18 first associates with an AP in the network, it must first authenticate itself. If the STA 18 starts at the first position 19a as shown in Figure 1, then AP 12 will authenticate the STA via a communication with the AAA server 16.

When the STA 18 moves from the first position 19a to a second position 19b, it then has to associate with AP 14. In the prior art, this entailed AP 14 communicating with the AAA server 16 to authenticate the STA 18.

However, the present invention utilizes a reauthentication protocol designed to reduce the volume of communication between the APs 12 and 14 and the AAA server 16. Initial, client (or station), extensible authentication protocol (EAP) authentication with the site's AAA server proceeds as is done currently. When the client roams from a first access point to a second access point, if the second access point does not already have knowledge of the client's current AAA session, the client must perform a EAP authentication again, as is done in the prior art, and the second access point will issue a multicast Deregistration Notice to its subnet, as is done in the prior art. Note that even when AP 14 already knows of STA 18's AAA context, it must still issue the multicast Deregistration Notice to update the Ethernet network's switch forwarding tables. It is just via this mechanism that AP 12 learns that a STA roamed from it to AP 14.

Upon observing the Deregistration Notice from the second access point, unlike the prior art, the first access point will add the second access point to its Roaming

Neighborhood table and will authenticate itself with the second access point by initiating an EAP, or preferably a Lightweight Extensible Authentication Protocol (LEAP), authentication with the AAA server through the second access point. Upon success of the EAP or LEAP authentication of the first access point via the second access point to the AAA server, the first access point and the second access point have established a secure and mutually authenticated communications channel. For all subsequent EAP or LEAP clients associated to the first access point, the first access point will securely forward the subsequent client's authentication context information, session key and session identifier, to each access point in its Roaming Neighborhood with which it is actively authenticated. Then, upon any subsequent roam from the first access point to the second access point, the client will then be presented with a LEAP Reauthentication protocol upon its association with the second access point. If the LEAP reauthentication is successful, then communication can take place immediately and no new EAP authentication needs to occur.

After the access points have established a secure and mutually authenticated communications channel, then similar to what occurs when a new client associates with the first access point, when a client associates with the second access point, the second access point will securely forward the client's authentication context information, session key, and session identifier, to each access point in its Roaming Neighborhood with which it is actively authenticated. The access points only forward the client data when the client actually associate with them. Thus, when the second access point receives the client data from the first access point, it will not forward the data to the access points in its roaming table until the client actually roams and associates with the second access point. When the client roams from the second access point to the first access point, the client is presented with a LEAP Reauthentication protocol upon its association with the first access point.

For embodiments using RADIUS accounting, a couple of options exist. For the simplest implementation, the first access point can close the client's current accounting session upon receiving the Deregistration Notice. The second access point can then initiate a new accounting session for the client, this may be concurrent with requesting an "early renew" reauthentication for the client, which would not induce a loss in connectivity. A more sophisticated implementation would involve a Mobility Context Transfer from the first access point to the second access point of the client's current accounting records.

Referring now to Figure 2, there is shown a process 200 contemplated by the present invention. The process 200 begins at step 202 wherein a station, STA 18, authenticates itself with a first access point, AP 12. The authentication could be by conventional EAP or other authentication protocols such as LEAP. At step 204, the station moves from a first position 19a in the within the first access point 12 to a second position 19b of the second access point 14. At step 206 the second access point 12 checks to determine whether it has knowledge of the station's 18 current AAA session. If the second access point 14 is aware of the station's 18 AAA session, then the second access point 14 presents an EAP, LEAP or other reassociation protocol to the station 18, and then as shown at step 210 communication between the second access point 14 and the station 18 takes place immediately.

If however, at step 206 the second access point 14 is unaware of the station's 18 current AAA session, then as shown at step 212 the station authenticates with the 2nd Access Point. As shown in step 214, the second access point 14 then issues a multicast Deregistration Notice to its subnet. Then as shown in step 216, the first access point 12, upon receiving the Deregistration Notice sent by the second access point 14, adds the second access point 14 to its Roaming Neighborhood table and initiates a LEAP authentication with the AAA server through the second access point 14. As shown in step 218, upon successful authentication of the first access point 12 with the second access point 14, the first access point 12 and second access point 14 establish a secure, mutually authenticated communications channel with each other.

Referring now to Figure 3, there is shown a process 300 that occurs when a second station associates with the first access point after the first access point 12 and second access point 14 have already established a secure, mutually authenticated communication channel. The process 300 begins at step 302 when the second station (not shown) associates with the first access point 12. The second station would authenticate using EAP, LEAP, or other authentication protocol. After the second station is authenticated by the first access point 12, the first access point 12 securely forwards the second station's authentication context information, session key and session identifier, to each access point in its roaming table, including second access point 14, as shown in step 304. At step 306 the second station roams to the second access point. 14. Because at step 304 the second access point 14 received the second station's authentication context information, the second access point 14 presents the second station with a LEAP Reauthentication protocol. If at step 310 the second station is validated, then as shown in step 312 communication between the second station and the second access point 312 begins immediately. As shown in step 314, the second access point 14 then securely forwards the second station's context information to each access point in its Roaming Neighborhood.

If at step 310 the second station is not validated by the second access point, then as shown at step 316 the station must attempt authentication as an initial authentication.

With the present invention, security of passing client credentials between access points is provided by mutual LEAP authentication of the access points. There is no obvious security hole of passing client session data in the clear over the wired network as is possible under pre-authentication protocols. The access points have no shared secrets in common between them. The only shared secret is individual shared secrets between each access point and the AAA server, not network wide. The compromise of one access point does not provide a shared secret network-wide access.

LEAP latency in mutual authentication between access points is avoided by pre-authenticating access points within each other's roaming neighborhood. The roaming neighborhood is based on actual client roaming patterns, and should generally comprise only two to four other access points. Specification of the Roaming Neighborhood can be either transient, wherein the Roaming Neighborhood is regenerated each time an access point restarts, or could be persistent.

For the pre-authentication to function properly with RADIUS servers, the RADIUS server must be configured to allow "multiple simultaneous logons" of access point devices.

Though operation of this mechanism is restricted to roaming with the same administrative subnet of each pair of access points, that is not a restriction on client roaming if Virtual Local Area Networks (VLANs) are enabled. In other words, if access points are on a separate VLAN from clients, the present invention supports client inter-subnet mobility.

Although the invention has been shown and described with respect to a certain preferred embodiment, it is obvious that equivalent alterations and modifications will occur to others skilled in the art upon the reading and understanding of this specification. The present invention includes all such equivalent alterations and modifications.

What is Claimed is:

1. A method for authenticating a client by a first access point, the steps comprising:

associating a client;

receiving a deregistration notice from a second access point when the client associates with the second access point; and

authenticating the first access point by the second access point;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

2. The method of claim 1 wherein the associating step further comprises authenticating the client by the first access point with an authentication server.

3. The method of claim 2 wherein the authentication server is a Remote Authentication Dial-In User Server.

4. The method of claim 1, the steps further comprising adding the second access point to a Roaming Neighborhood Table.

5. The method of claim 1, wherein the authenticating step is initiated by the first access point.

6. The method of claim 1, wherein the authenticating step further comprises using an authentication server to mutually authenticate the first access point and the second access point with each other.

7. The method of claim 1, the steps further comprising:

associating a second client with the first access point; and

forwarding the second client's authentication context information to the second access point.

8. The method of claim 7, wherein the authentication context information

comprises a session key and a session identifier.

9. The method of claim 1, the steps further comprising

receiving context information from a second access point for a second client;

receiving an association request from the second client; and

presenting reauthentication protocol to the second client.

10. The method of claim 9 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

11. A method for authenticating a client by an access point, the steps comprising:

receiving an association request from the client;

sending a multicast deregistration notice;

authenticating the client;

receiving an authentication request from a second access point; and

authenticating the second access point.

12. The method of claim 11 wherein the authenticating the client step uses an authentication server.

13. The method of claim 12 wherein the authenticating the second access point uses the authentication server.

14. The method of claim 13 wherein the authentication server is a Remote Authentication Dial-In User Server.

15. The method of claim 1, the steps further comprising adding the second access point to a Roaming Neighborhood Table.

16. The method of claim 11, the steps further comprising:

associating a second client with the access point; and

forwarding the second client's authentication context information to the second access point.

17. The method of claim 16, wherein the authentication context information comprises a session key and a session identifier.

18. The method of claim 11, the steps further comprising

receiving context information from a second access point for a second client;

receiving an association request from the second client; and

presenting reauthentication protocol to the second client.

19. The method of claim 18 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

20. The method of claim 1 wherein the client having an accounting session, the steps further comprising:

closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

initiating a new accounting session for the client.

21. The method of claim 20, the steps further comprising requesting an early renew reauthentication for the client.

22. The method of claim 21 wherein the requesting step is performed concurrently with the initiating step.

23. The method of claim 1, wherein the client having a current accounting session comprising current accounting records, the steps further comprising transferring the accounting records from the first access point to the second access point..

24 A method for authenticating clients to access points of a network, the steps comprising:

associating a client to a first access point, the client authenticated by the first access point via an authentication server;

associating the client to a second access point, the second access point sending a multicast deregistration notice and authenticating the client via an authentication server; and

the first access point initiating an authentication with the second access point after the first access point receives the multicast deregistration notice;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

25 The method of claim 24 wherein the authentication server is a Remote Authentication Dial-In User Server.

26 The method of claim 24 the steps further comprising adding the second access point to a Roaming Neighborhood Table by the first access point.

27. The method of claim 24, the steps further comprising:

associating a second client with the first access point; and

forwarding the second client's authentication context information to the second access point.

28. The method of claim 27, wherein the authentication context information comprises a session key and a session identifier.

29. The method of claim 27, the steps further comprising

roaming by the client from the first access point to the second access point;

receiving an association request from the second client by the second access point; and

presenting reauthentication protocol to the second client by the second access point.

30. The method of claim 29 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

31. The method of claim 24 wherein the client having an accounting

session, the steps further comprising:

closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

initiating a new accounting session for the client.

32. The method of claim 31, the steps further comprising requesting an early renew reauthentication for the client.

33. The method of claim 32 wherein the requesting step is performed concurrently with the initiating step.

34. The method of claim 24, wherein the client having current accounting session comprising accounting records, the steps further comprising transferring the accounting records from the first access point to the second access point..

35. A computer-readable medium of instructions, comprising:

means for associating a client;

means for receiving a deregistration notice from a second access point when the client associates with the second access point; and

means for authenticating a first access point by the second access point;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

36. The computer-readable medium of instructions of claim 35 wherein the means for associating further comprises means for authenticating the client by the first access point with an authentication server.

37. The computer-readable medium of instructions of claim 35 wherein the authentication server is a Remote Authentication Dial-In User Server.

38. The computer-readable medium of instructions of claim 35, further comprising means for adding the second access point to a Roaming Neighborhood Table.

39. The computer-readable medium of instructions of claim 35, wherein the means for authenticating of the first access point initiates an authentication process.

40. The computer-readable medium of instructions of claim 35, the authenticating means further comprises using an authentication server to mutually authenticate the first access point and the second access point with each other.

41. The computer-readable medium of instructions of claim 40, further comprising:

means for associating a second client with the first access point; and

means for forwarding the second client's authentication context information to the second access point.

42. The computer-readable medium of instructions of claim 41, wherein the authentication context information comprises a session key and a session identifier.

43. The computer-readable medium of instructions of claim 35, further comprising

means for receiving context information from a second access point for a second client;

means for receiving an association request from the second client; and

means for presenting a reauthentication protocol to the second client.

44. The computer-readable medium of instructions of claim 43 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

45. A computer-readable medium of instructions, comprising:

means for receiving an association request from a client;

means for sending a multicast deregistration notice;

means for authenticating the client;

means for receiving an authentication request from a second access point; and

means for authenticating the second access point.

46. The computer-readable medium of instructions of claim 45 wherein the means for authenticating uses an authentication server.

47. The computer-readable medium of instructions of claim 46 wherein the means for authenticating the second access point uses the authentication server.

48. The computer-readable medium of instructions of claim 47 wherein the authentication server is a Remote Authentication Dial-In User Server.

49. The computer-readable medium of instructions of claim 45, further comprising means for adding the second access point to a Roaming Neighborhood Table.

50. The computer-readable medium of instructions of claim 45, further comprising:

means for associating a second client; and

means for forwarding the second client's authentication context information to the second access point.

51. The computer-readable medium of instructions of claim 50, wherein the authentication context information comprises a session key and a session identifier.

52. The computer-readable medium of instructions of claim 45, further comprising:

means for receiving context information from the second access point for a second client;

means for receiving an association request from the second client; and

means for presenting a reauthentication protocol to the second client.

53. The computer-readable medium of instructions of claim 52 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

54. The computer-readable medium of instructions of claim 35 wherein the client having an accounting session, further comprising:

means for closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

means for initiating a new accounting session for the client.

55. The computer-readable medium of instructions of claim 54, further comprising means for requesting an early renew reauthentication for the client.

56. The computer-readable medium of instructions of claim 54 wherein the means for requesting an early renew reauthentication operates concurrently with the means for initiating a new accounting session.

57. The computer-readable medium of instructions of claim 35, wherein the client having a current accounting session comprising current accounting records, further comprising means for transferring the accounting records from the first access point to the second access point.

58. A computer-readable medium of instructions, comprising:

means for associating a client to a first access point, the client authenticated by the first access point via an authentication server;

means for associating the client to a second access point, the second access point sending a multicast deregistration notice and authenticating the client via an authentication server; and

means for the first access point initiating an authentication with the second access point after the first access point receives the multicast deregistration notice;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

59. The computer-readable medium of instructions of claim 58 wherein the authentication server is a Remote Authentication Dial-In User Server.

60. The computer-readable medium of instructions of claim 58 further comprising means for adding the second access point to a Roaming Neighborhood Table by the first access point.

61. The computer-readable medium of instructions of claim 58, further comprising:

means for associating a second client with the first access point; and

means for forwarding the second client's authentication context information to the second access point.

62. The computer-readable medium of instructions of claim 61, wherein the authentication context information comprises a session key and a session identifier.

63. The computer-readable medium of instructions of claim 61, further comprising:

means for roaming by the client from the first access point to the second access point;

means for receiving an association request from the second client by the second access point; and

means for presenting reauthentication protocol to the second client by the second access point.

64. The computer-readable medium of instructions of claim 63 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

65. The computer-readable medium of instructions of claim 58 wherein the client having an accounting session, further comprising:

means for closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

means for initiating a new accounting session for the client.

66. The computer-readable medium of instructions of claim 65, further comprising means for requesting an early renew reauthentication for the client.

67. The computer-readable medium of instructions of claim 66 wherein the means for requesting an early renew reauthentication operates concurrently with the means for initiating a new accounting session.

68. The computer-readable medium of instructions of claim 58, wherein the client having current accounting session comprising accounting records, further comprising means for transferring the accounting records from the first access point to the second access point.

69. An access point, comprising:

means for associating a client;

means for receiving a deregistration notice from a second access point when the client associates with the second access point; and

means for authenticating a first access point by the second access point;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

70. The access point of claim 69 wherein the means for associating further comprises means for authenticating the client by the first access point with an authentication server.

71. The access point of claim 69 wherein the authentication server is a Remote Authentication Dial-In User Server.

72. The access point of claim 69, further comprising means for adding the second access point to a Roaming Neighborhood Table.

73. The access point of claim 69, wherein the means for authenticating of the first access point initiates an authentication process.

74. The access point of claim 69, the authenticating means further comprises using an authentication server to mutually authenticate the first access point and the second access point with each other.

75. The access point of claim 74, further comprising:

means for associating a second client; and

means for forwarding the second client's authentication context information to the second access point.

76. The access point of claim 75, wherein the authentication context information comprises a session key and a session identifier.

77. The access point of claim 69, further comprising

means for receiving context information from a second access point for a second client;

means for receiving an association request from the second client; and

means for presenting a reauthentication protocol to the second client.

78. The access point of claim 77 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

79. An access point, comprising:

means for receiving an association request from a client;

means for sending a multicast deregistration notice;

means for authenticating the client;

means for receiving an authentication request from a second access point; and

means for authenticating the second access point.

80. The access point of claim 79 wherein the means for authenticating uses

an authentication server.

81. The access point of claim 80 wherein the means for authenticating the second access point uses the authentication server.

82. The access point of claim 81 wherein the authentication server is a Remote Authentication Dial-In User Server.

83. The access point of claim 79, further comprising means for adding the second access point to a Roaming Neighborhood Table.

84. The access point of claim 79, further comprising:

means for associating a second client with the access point; and

means for forwarding the second client's authentication context information to the second access point.

85. The access point of claim 84, wherein the authentication context information comprises a session key and a session identifier.

86. The access point of claim 79, further comprising:

means for receiving context information from a second access point for a second client;

means for receiving an association request from the second client; and

means for presenting reauthentication protocol to the second client.

87. The access point of claim 86 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

88. The access point of claim 69 wherein the client having an accounting session, further comprising:

means for closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

means for initiating a new accounting session for the client.

89. The access point of claim 88, further comprising means for requesting an early renew reauthentication for the client.

90. The access point of claim 89 wherein the means for requesting an early renew reauthentication operates concurrently with the means for initiating a new accounting session.

91. The access point of claim 69, wherein the client having a current accounting session comprising current accounting records, further comprising means for transferring the accounting records from the first access point to the second access point.

92. A access point, comprising:

means for associating a client to a first access point, the client authenticated by the first access point via an authentication server;

means for associating the client to a second access point, the second access point sending a multicast deregistration notice and authenticating the client via an authentication server; and

means for the first access point initiating an authentication with the second access point after the first access point receives the multicast deregistration notice;

wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

93. The access point of claim 92 wherein the authentication server is a Remote Authentication Dial-In User Server.

94. The access point of claim 92 further comprising means for adding the second access point to a Roaming Neighborhood Table by the first access point.

95. The access point of claim 92, further comprising:

means for associating a second client with the first access point; and

means for forwarding the second client's authentication context information to the second access point.

96. The access point of claim 95, wherein the authentication context information comprises a session key and a session identifier.

97. The access point of claim 95, further comprising:

means for roaming by the client from the first access point to the second access point;

means for receiving an association request from the second client by the second access point; and

means for presenting reauthentication protocol to the second client by the second access point.

98. The access point of claim 97 wherein the reauthentication protocol is a Lightweight Extensible Authentication Protocol reauthentication protocol.

99. The access point of claim 92 wherein the client having an accounting session, further comprising:

means for closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

means for initiating a new accounting session for the client.

100. The access point of claim 99, further comprising means for requesting an early renew reauthentication for the client.

101. The access point of claim 100 wherein the means for requesting an early renew reauthentication operates concurrently with the means for initiating a new accounting session.

102. The access point of claim 92, wherein the client having current accounting session comprising accounting records, further comprising means for transferring the accounting records from the first access point to the second access point..

103. An access point, comprising:

a wireless communication system;

a second communication system for communicating with a second access point and an authentication server; and

computer readable instructions stored on a computer readable medium communicatively coupling the wireless communication system to the second communication system;

wherein when a client associates with the access point via the wireless communication system, the computer readable instructions uses the second communication system to authenticate the wireless station;

wherein when the client associates with the second access point, the access point receives a deregistration notice from the second access point, the computer readable instructions further comprising instructions for mutually authenticating with the second access point; and wherein a secure, mutually authenticated communications channel is established between the first access point and the second access point.

104. The access point of claim 103 wherein the authentication server is a Remote Authentication Dial-In User Server.

105. The access point of claim 103, the computer readable instructions further comprising instructions for adding the second access point to a Roaming Neighborhood Table.

106. The access point of claim 103, wherein when a second client associates with the second access point, the first access point receives a message via the second communication system with the second client's authentication context information.

107. The access point of claim 106, wherein the authentication context information comprises a session key and a session identifier.

108. The access point of claim 103 wherein the client having an accounting

session, further comprising:

means for closing the client's accounting session by the first access point upon receiving the deregistration notice from the second access point; and

means for initiating a new accounting session for the client.

109. The access point of claim 103 wherein the client having an accounting session further comprising further comprising means for transferring the accounting records from the first access point to the second access point.

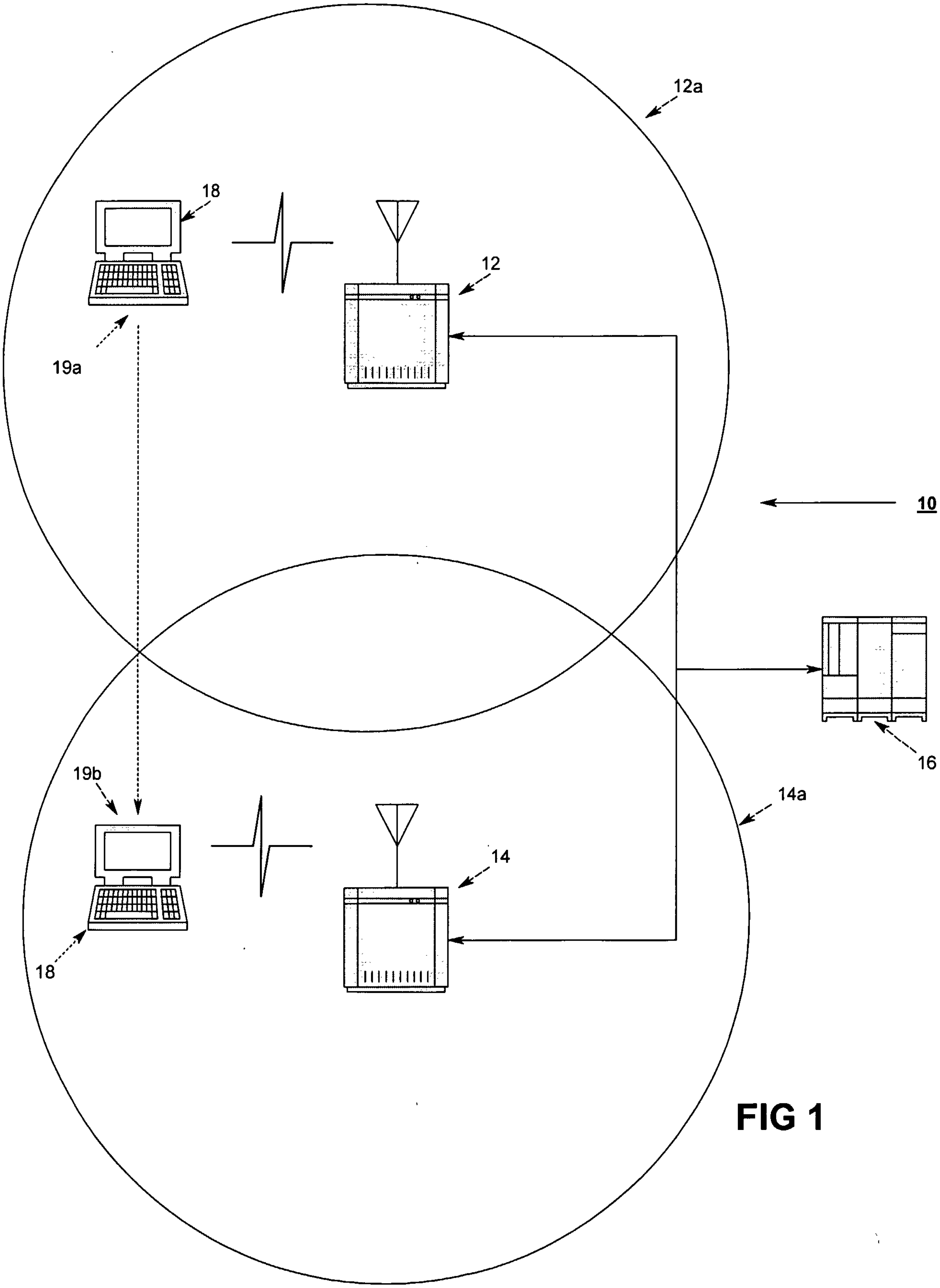


FIG 1

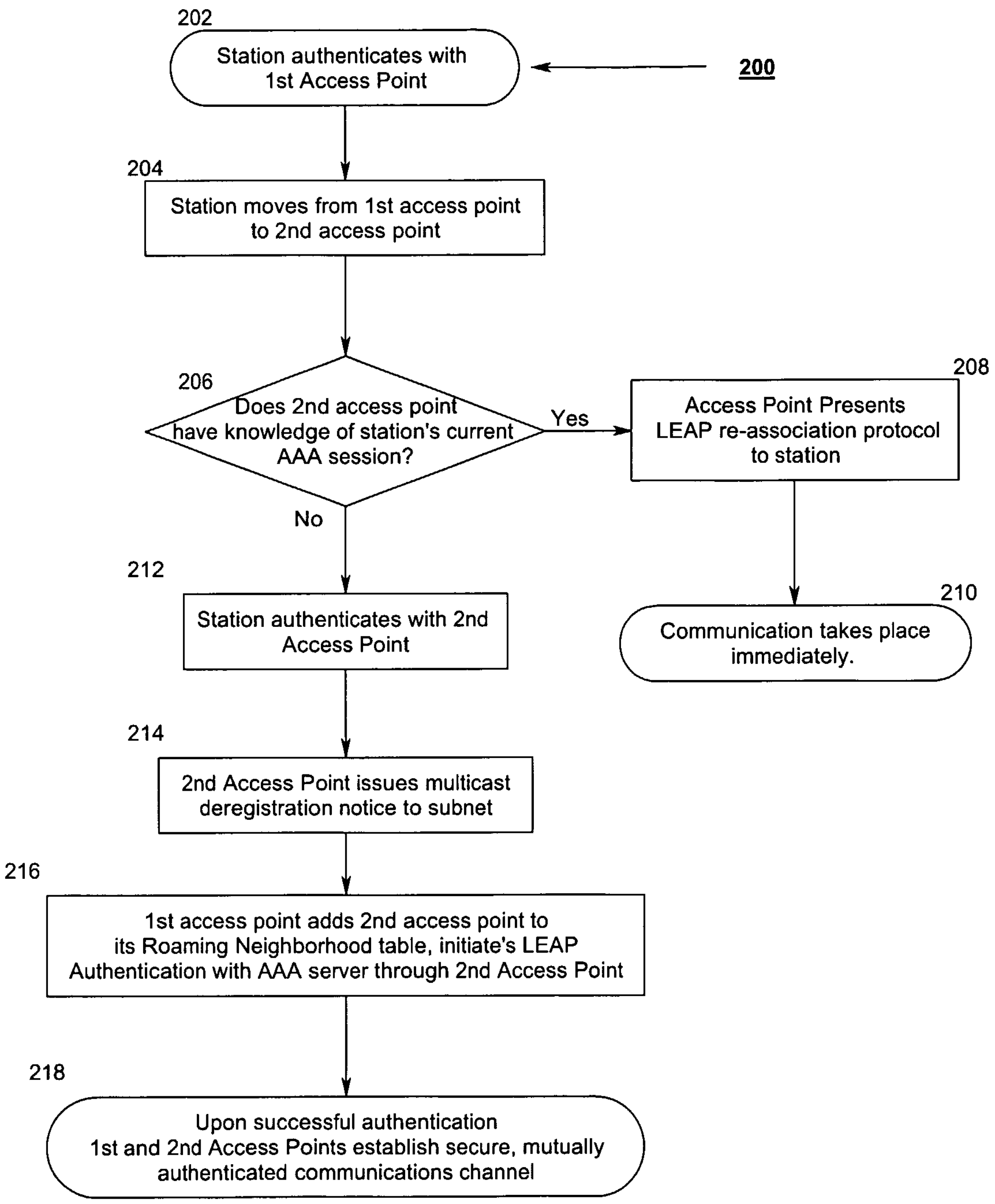

200
202
Station authenticates with 1st Access Point
204
Station moves from 1st access point to 2nd access point
206
Does 2nd access point have knowledge of station's current AAA session?
Yes
208
Access Point Presents LEAP re-association protocol to station
210
Communication takes place immediately.
No
212
Station authenticates with 2nd Access Point
214
2nd Access Point issues multicast deregistration notice to subnet
216
1st access point adds 2nd access point to its Roaming Neighborhood table, initiate's LEAP Authentication with AAA server through 2nd Access Point
218
Upon successful authentication 1st and 2nd Access Points establish secure, mutually authenticated communications channel

FIG 2

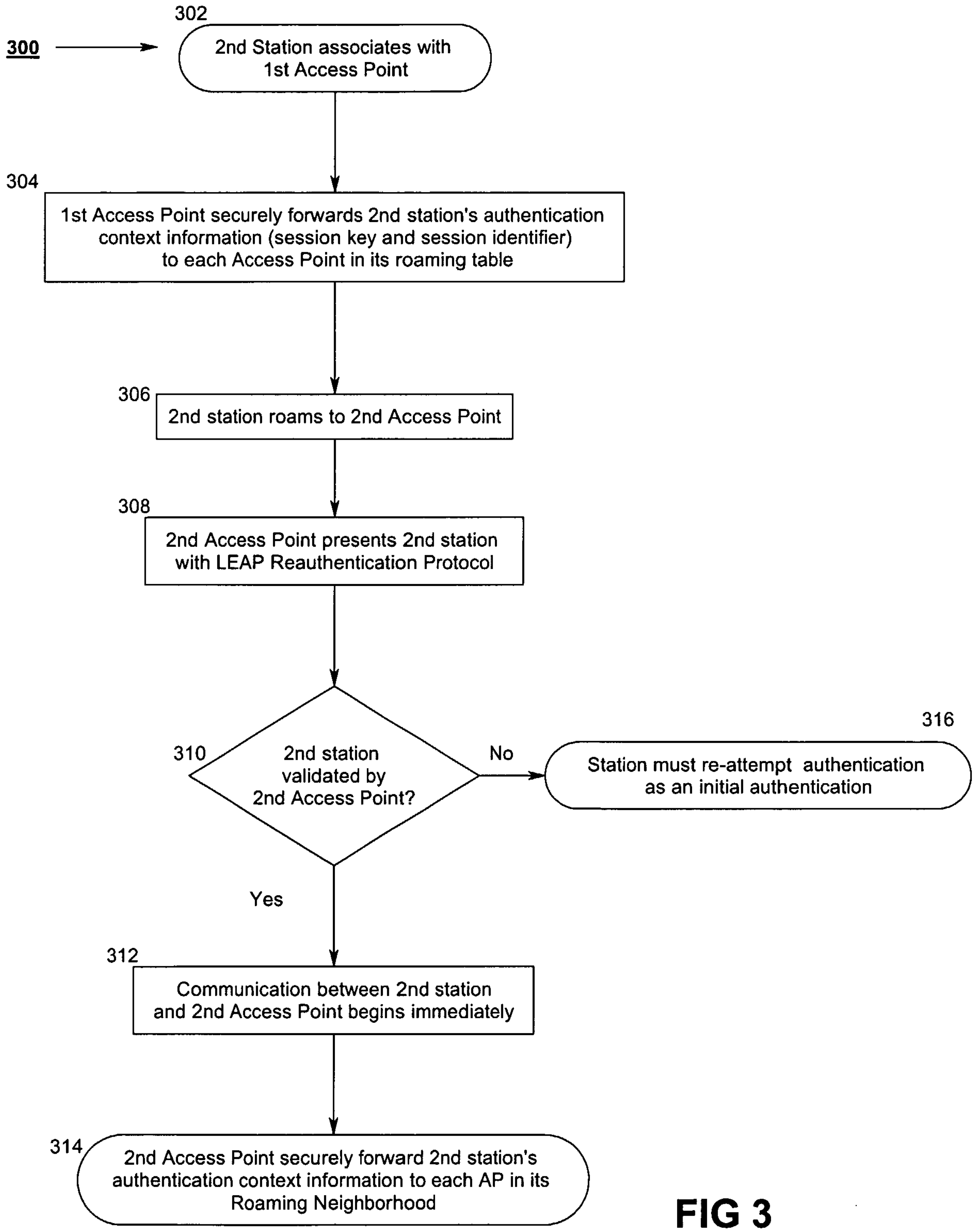

300
302
2nd Station associates with 1st Access Point
304
1st Access Point securely forwards 2nd station's authentication context information (session key and session identifier) to each Access Point in its roaming table
306
2nd station roams to 2nd Access Point
308
2nd Access Point presents 2nd station with LEAP Reauthentication Protocol
310
2nd station validated by 2nd Access Point?
No
316
Station must re-attempt authentication as an initial authentication
Yes
312
Communication between 2nd station and 2nd Access Point begins immediately
314
2nd Access Point securely forward 2nd station's authentication context information to each AP in its Roaming Neighborhood

FIG 3