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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2005 (04.08.2005)

PCT

(10) International Publication Number
WO 2005/069784 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2004/042078

(22) International Filing Date:
14 December 2004 (14.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/754,402 9 January 2004 (09.01.2004) US

(71) Applicant *(for all designated States except US)*: **CRANITE SYSTEMS, INC.** [US/US]; 6620 Via Del Oro, 2nd Floor, San Jose, CA 95119 (US).

(72) Inventor: **VOLPANO, Dennis, Michael**; 17555 Sugarmill Road, Salinas, CA 93908 (US).

(74) Agents: **GLENN, Michael, A.** et al.; Glenn Patent Group, 3475 Edison Way, Suite L., Menlo Park, CA 94025 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, 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, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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

(54) Title: PUBLIC ACCESS POINT

(57) Abstract: The invention instantiates a Personal VLAN bridge, using IEEE Std. 802.11 elements. The result is a bridge, referred to as a public access point, that is better suited for implementing public wireless data networks than the IEEE Std. 802.11 architecture. The invention also provides a location-update protocol for updating the forwarding tables of bridges that connect public access points together. The invention further provides a method for more controlled bridging, which is referred to as fine bridging.

WO 2005/069784 A2

Public Access Point

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to wireless public access to electronic networks. More particularly, the invention relates to an architecture that permits the creation of virtual basic service sets from within a physical access point for an electronic network.

DESCRIPTION OF THE PRIOR ART

Public WiFi hotspots are deployed using traditional IEEE Std. 802.11-compliant access points with some exceptions. However, the IEEE Std. 802.11 architecture and security model are unsuitable for public use. Stations associated with an access point (AP) share an 802.11 Basic Service Set (BSS), or wireless LAN. Unless all members of a BSS are trustworthy, no station in the BSS is safe from attacks initiated by other members. Such attacks include stealing the basic service and any confidential information provided by subscribers to get the service, such as passwords and credit card information. Other attacks include disruptions in network integrity and quality of service. It is unrealistic to expect all members of a public BSS, *i.e.* one that is comprised of stations associated with a public AP, to be trustworthy. Therefore, stations are vulnerable in a public BSS.

Sharing a public BSS presents another threat. Members of the BSS can contaminate other member stations with worms or Trojan horses. The port-based DCOM RPC attack, MSBlaster, and Welchia worms are good examples. The threat is more acute with a public BSS which is an electronic cesspool. How can a station cope with the threats?

Stations in the BSS might fend for themselves with defenses such as personal firewalls. Alternatively, a public WiFi provider might deploy a security model that protects subscribers from one another. One approach is to prevent inter-station communication. This is an untenable solution though. Stations that trust each other should be allowed to communicate among themselves, even in a public setting. Stations, for instance, should be able to access a file server on the same local LAN in a meeting held at a convention center. This is the usual practice at standards meetings, for example. Yet if this type of sharing is permitted, then under IEEE Std. 802.11, it becomes easy for an intruder to render the entire BSS inoperable. This was demonstrated at the 2001 Usenix Security Conference and at the 2001 DEFCON conference in Las Vegas. No security model today for wireless LAN can support this type of sharing without introducing vulnerabilities.

It would be advantageous to provide a security model for wireless LAN that can support sharing of a single physical BSS without introducing vulnerabilities or compromising security among stations using the BSS.

SUMMARY OF THE INVENTION

The invention provides a security model for wireless LANs that can support sharing of a single physical BSS by stations without introducing vulnerabilities or compromising station security. Thus, a new kind of access point is provided, which is referred to herein as a Public Access Point (PAP). The PAP has a different security architecture than that prescribed by IEEE Std. 802.11. The PAP architecture permits the creation of virtual Basic Service Sets from within a single physical AP. An arbitrary number of virtual service sets can be created, and any number of end stations can belong to a virtual BSS. A PAP appears to end stations as multiple physical 802.11 access points, one for each virtual BSS. Therefore, a PAP is fully interoperable with any 802.11 end station.

As an example of a PAP's use, consider a convention center. Different meetings may use 802.11-enabled projectors. The PAP allows provisioning of separate LAN segments for each meeting, providing separate link privacy and integrity for each. Using only IEEE Std. 802.11 instead, a meeting projector and all stations capable of

projecting with it must use a private access point or an *ad hoc* WLAN, and manage WLAN membership, authentication and keying material. Otherwise, anyone could project with the projector, or worse, intercept valid projector traffic before it is displayed so that it can be monitored or corrupted by an outsider.

Besides the security management burden associated with prior art approaches being too high, meeting planners prefer to leverage local access points rather than installing and configuring their own at every venue. The PAP can administer all security. With it, all end stations in each meeting, which includes the shared projector and any local file servers, are effectively associated with a virtual 802.11 access point for that meeting, and all virtual access points arise from the same physical PAP.

The invention also provides a location-update protocol for updating the forwarding tables of bridges that connect public access points together.

The invention further provides a method for more controlled bridging, which is referred to as fine bridging.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block schematic diagram of an IEEE Std.. 802.11 protocol entity;

Fig. 2 is a block schematic diagram of an IEEE Std.. 802.11 configuration infrastructure;

Fig. 3 is a block schematic diagram of a public access point architecture according to the invention;

Fig. 4 is a block schematic diagram of a policy for access ibility within a three-station virtual BSS, one of which is an AP, according to the invention;

Fig. 5 is a block schematic diagram of a policy among four stations where stations *A* and *B* share server stations *S* and *D* but *A* and *B* are not allowed to access each other according to the invention;

Fig. 6 is a block schematic diagram of the policy in Figure 3, modified so that an edge from *B* to *A* is added to the policy according to the invention; and

Fig. 7 is a block schematic diagram of an IEEE Std. 802.1Q bridge that eliminates direct communication between edge hosts connected to the infrastructure system via port-based VLAN assignment, egress filtering, and shared VLAN learning (SVL).

DETAILED DESCRIPTION OF THE INVENTION

Public Access Point

In U.S. patent application serial No. 10/057,566, a protocol is described whereby an end station can create a virtual bridged LAN (VLAN) that clones an existing VLAN by duplicating the existing VLAN's tagged and untagged member sets. Further, the new VLAN is unique by virtue of its unique security association. The association provides cryptographic keying material that keeps packets belonging to the VLAN private and permits their VLAN membership to be verified cryptographically by a keyed MAC. The new VLAN is owned by its creator. The owner controls which stations can join and discover the VLAN, as well as the VLAN's lifetime. Therefore, the VLAN is called a personal virtual bridged LAN (PVLAN).

One embodiment of the invention provides a refinement of the PVLAN that uses only standard elements of IEEE Std. 802.11-1999 (see Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, ISO/IEC 8802-11:1999(E), ANSI/IEEE Std. 802.11, 1999 edition; and Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Medium Access Control (MAC) Security Enhancements, IEEE Std. 802.11i/D7.0, Draft amendment to ISO/IEC 8802-11:1999(E), ANSI/IEEE Std. 802.11, 1999 edition).

See also, Figure 1, which is a block schematic diagram of an IEEE Std. 802.11 protocol entity; and Figure 2, which is a block schematic diagram of an IEEE Std. 802.11 configuration infrastructure, in which each BSS (BSS-A, BSS-B) comprises respective access point (AP-A, AP-B) and associated stations (A1/A2, B1/B2). No modification of the behavior of any 802.11-compliant end station that does not act as an access point is required by the invention. The refinement instantiates a PVLAN to a virtual 802.11 BSS and affects only the access point.

Fig. 3 is a block schematic diagram of a public access point architecture according to the invention. A virtual 802.11 BSS, *e.g.* BSS-1 or BSS-2, comprises a set of stations, each with a hardware (MAC) address (see Figure 1), that share a unique security association, called the group security association. A security association consists of an encryption key and an authentication code key.

Exactly one of the stations in a virtual BSS is a public access point (PAP) 31. It bridges the 802.11 Wireless Medium (WM) 32 and the 802.11 Distribution System Medium (DSM) 33.

A unique unicast security association exists for every station in a virtual BSS. It is shared between the station and the PAP of that virtual BSS.

Each virtual BSS, *e.g.* BSS-1 or BSS-2 has its own identifier, or BSSID. It is a virtual MAC address of the PAP belonging to that BSS. The PAP receives any frame from the WM destined for one of its virtual MAC addresses, and transmits a frame to the WM using one of its virtual MAC addresses as the source MAC address of the frame.

A collection of virtual basic service sets is supported by a shared TSF (Timing Synchronization Function), DCF (Distributed Coordination Function), and optionally a PCF (Point Coordination Function), at a single PAP. There is a single NAV (Network Allocation Vector) and PC (Point Coordinator) at each PAP. Such sharing is possible because the 802.11 virtual carrier-sense, medium reservation mechanism is designed to work with multiple basic service sets that use the same channel overlap. This sort of overlap may occur among virtual basic service sets supported by a

single-channel PAP. The virtual service sets may use one channel and therefore may overlap at a PAP.

A PAP can belong to more than one virtual BSS. See BSS-1, BSS-2 on Figure 1. Any station that is not a PAP can belong to at most one virtual BSS.

A virtual 802.11 BSS can be bridged with another virtual BSS through the connection of their public access points by a virtual bridged LAN. The PAP of each virtual BSS connects to the Distribution System (DS) via a trunked or untagged port of a VLAN-aware bridge. Frames transmitted to the DS may carry VLAN tags known to the DSM. A PAP may maintain a DSM VLAN mapping that maps a VLAN tag to a virtual BSSID.

There are presently two kinds of virtual BSS: Class-1 and Class-3 virtual BSS. A PAP supports exactly one Class-1 virtual BSS and one or more multiple Class-3 virtual basic service sets. The Class-1 virtual BSS is the only virtual BSS a station is allowed to occupy while it is in 802.11 State 1 or 2, as governed by the PAP. When in State 3, a station is allowed to join a Class-3 virtual BSS. The Class-3 virtual BSS may be determined by the kind of authentication, *e.g.* Open System or Shared Key, used to authenticate the station.

The Class-1 virtual BSSID is the BSSID field of every Class 1 and Class 2 frame that has such a field. It is also the receiver or transmitter address field, where appropriate, for Class 1 and Class 2 frames.

Every virtual BSS has identical beacon frame content except for the Timestamp, Beacon interval, Capability information Privacy (Protected) bit, Service Set Identifier (SSID), security capability element, and Traffic Indication Map (TIM) element fields.

A PAP does not have to beacon for a Class-3 virtual BSS if it does not support PS (Power-Save) mode for end stations in that BSS. If it does beacon for a Class-3 BSS, then the SSID element in every beacon specifies the broadcast SSID. These steps prevent any Class-3 virtual BSS from being identified through beaconing.

Only a Class-1 virtual BSS beacon has an SSID element with a non-broadcast SSID field. A station can associate with the Class-1 virtual BSS only. The station uses the non-broadcast SSID in the SSID element of an Association or Reassociation Request frame.

U.S. patent application serial No. 10/057,566 identifies PVLAN join and discovery steps. With a PVLAN represented as a virtual BSS, these steps are instantiated as follows:

Join

Every station is by default a member of the Class-1 virtual BSS at a PAP. The PAP can either authenticate the user of the station or the station itself in the Class-1 virtual BSS. If successful, the station enters 802.11 State 2 at that PAP. At this time, the PAP and station may exchange Class 1 and Class 2 frames while in the Class-1 virtual BSS.

Class 1 frames are not protected cryptographically. Class 2 frames may be protected cryptographically if the station and PAP share a unicast security association after successful authentication. The PAP and station may also share a group security association after authentication. The group security association is for that Class-3 virtual BSS to which the station belongs if it completes an 802.11 Association with the PAP.

Before the station and PAP can exchange Class 3 frames, the station must

1) request Association with the Class-1 virtual BSS from State 2; and

2) switch to a Class-3 virtual BSS.

The PAP switches the station to a Class-3 virtual BSS by responding to the station's Association Request with an Association Response MMPDU whose source address (Address 2 Field) or BSSID (Address 3 Field) is the Class-3 virtual BSSID for that

virtual BSS. The Association Response's Capability information field may have its Privacy (Protected) bit set to one.

The Class-3 virtual BSS is determined in one of three ways:

1) an authentication server in the DS specifies a DSM VLAN for the user and the PAP maps it to a Class-3 virtual BSSID using its DSM VLAN mapping;

2) an authentication server in the DS specifies a Class-3 virtual BSS for the user; or

3) the PAP creates a new Class-3 virtual BSS for the user; the PAP may inform an authentication server of the new virtual BSS and provide it with rules for allowing other stations to join the new BSS.

Discovery

The Class-1 virtual BSS is discovered through 802.11 beacon or Probe Response management frames where the BSSID field (Address 3 field) and source address field (Address 2 field) are each set to the Class-1 virtual BSSID. The Privacy (Protected) bit of the Capability information field in these frames is set to zero. The TIM element of the beacon applies to the Class-1 virtual BSS. Only the Class-1 virtual BSS is advertised through beacon frames.

Data frame (MPDU) Distribution

A PAP implements the MAC Protocol Data Unit (MPDU) bridge protocol. For an MPDU received from either the DSM or the WM, the protocol is defined by the following two cases:

1. *MPDU received from the DSM.* There are two subcases (Note: The two subcases handle delivery of the received MPDU to the local LLC of the PAP because the station of every PAP belongs to at least one virtual BSS):

   a. The received MPDU has no VLAN tag or a null VLAN tag. The MPDU from the DSM is relayed to a virtual BSS if the destination address is the address of a station that belongs to the virtual BSS and the station is associated with the PAP, or if the destination address is a group address, the virtual BSS has a station that belongs to the group and the station is associated with the PAP. All stations belong to the broadcast group.

   b. The received MPDU has a non-null VLAN tag. The virtual BSS to which the MPDU is relayed is identified by the virtual BSSID to which the non-null VLAN tag is mapped under the PAP's DSM VLAN mapping. If the mapping is undefined for the given tag, the MPDU is not relayed.

   Any virtual BSS to which a received MPDU is relayed has a BSSID which forms the source address (Address 2 field) of the 802.11 MPDU that is relayed to that virtual BSS.

2. *MPDU received from the WM.* The received 802.11 MPDU is relayed to the virtual BSS identified by the Address 1 field of the MPDU if the destination address (Address 3 field of MPDU) is the address of a station that belongs to the identified virtual BSS and the station is associated with the PAP, or if the destination address is a group address. Otherwise, the frame is not relayed to any virtual BSS. The Address 1 field of the received 802.11 MPDU is the source address (Address 2 field) of the 802.11 MPDU that is relayed to the virtual BSS identified by the Address 1 field.

   The received MPDU is also relayed to the DSM if the destination address (Address 3 field of MPDU) is the address of a station that is not associated with the PAP, or if the destination address is a group address. The MPDU

relayed to the DSM has a VLAN tag if the DS is VLAN aware, and is untagged otherwise. The VLAN tag is the pre-image of the Address 1 field of the received MPDU under the PAP's DSM VLAN mapping.

Encryption and decryption process

Encryption and decryption applies 802.11 Data frames and Management frames of subtype Association Request/Response, Reassociation Request/Response, Disassociation and Deauthentication.

The encryption process used by a PAP before sending an 802.11 Data or Management frame to the WM involves two major steps:

- identifying a security association for the frame; and

- then using the association to construct an expanded frame for transmission according to some encipherment and authentication code protocols.

Different encipherment and authentication code protocols can be used for broadcast and multicast traffic among virtual basic service sets, and different encipherment and authentication code protocols can be used for directed (unicast) traffic among stations in a single virtual BSS.

If the frame destination address (Address 1 field) is the address of a station then the unicast security association shared between that station and the PAP is used in the expansion. If the frame is a Data frame and its destination address is a group address then the MPDU bridge protocol identifies a destination virtual BSS for the frame. The group security association for the identified virtual BSS is used in the expansion.

A non-PAP station transmits an 802.11 MPDU of type Data or Management to the DS using the unicast security association it shares with the PAP in its virtual BSS.

When receiving an 802.11 Data or Management frame from the WM, the PAP attempts to decipher and verify the integrity of the frame using the unicast security association for the station identified by the source address (Address 2 field) of the MPDU.

When receiving an 802.11 MPDU of type Data or Management from a PAP, a non-PAP station attempts to decipher and verify the integrity of the frame using the unicast security association it shares with the PAP if the destination address of the frame (Address 1 field) is the address of the station, and using the group security association of its Class-3 virtual BSS if the destination address of the frame is a group address.

Location-update protocol

The invention also comprises a location-update protocol for updating the forwarding tables of bridges, or other interconnection media, connecting Public Access Points together.

Given multiple Public Access Points attached to different bridges in a spanning tree of a bridged LAN and an end station that associates with one of them and then reassociates with a new PAP, the new PAP sends a directed Bridge Protocol Data Unit (BPDU) (called a relocation PDU) to the PAP with which the station was previously associated. The destination address of the BPDU is the Current AP address of the Reassociation Request frame, which is a Class-3 virtual BSSID. The source address is the hardware address of the station.

Upon receiving a relocation MPDU at a particular port, a bridge updates its forwarding table with an entry that binds the receiving port to the source address of the MPDU.

A receiving bridge forwards a relocation MPDU to its designated root port unless the MPDU arrived on that port or the receiving bridge is the root of the spanning tree. If it is received at the designated root port of a bridge or by the root bridge then it is forwarded according to the learned forwarding table of the bridge, which may involve flooding the MPDU to all ports except the receiving port.

Fine bridging

One embodiment of the invention discussed above refines a PVLAN to a virtual BSS. Under the MPDU bridge protocol, any station in a virtual BSS can send a directed or group-addressed frame to any other station in that virtual BSS. This may be undesirable. A meeting in a conference center, for instance, may have its own virtual BSS but not all attendees trust each other. By sharing the same virtual BSS, some attendees can launch worms or viruses. Trying to thwart these attacks by assigning each attendee to a unique virtual BSS prevents attendees from being able to share a server. Ideally, the server is shared by all meeting participants, yet no participant should be able to access, *i.e.* send frames to, another participant. The Public Access Point described above cannot provide this level of access control. An AP supporting fine bridging can provide it.

See also, Figure 7, which is a block schematic diagram of an IEEE Std. 802.1Q bridge that connects a set of edge hosts to an infrastructure system such as a LAN. Untagged frames arriving from edge hosts are assigned to VLAN A by virtue of port-based VLAN assignment (PVID A) and untagged frames arriving from the infrastructure system are assigned to VLAN B (PVID B). The egress rules depicted allow for frames belonging to A or B to egress to the infrastructure while only those belonging to B are allowed to egress to the edge hosts. In this way, edge hosts are prevented from communicating directly with one another.

Fine bridging decouples identification of a broadcast or multicast domain with a BSS.

Under fine bridging, the bridging behavior of an AP is determined by a policy expressed as a directed graph. The nodes of the graph are stations and there is an

edge from a station *A* to a station *B* if and only if station *A* must be able to access station *B*, in other words, station *B* must be able to receive directed or group frames from station *A*.

For a given policy, the broadcast domain for a node is itself and all nodes it must access. The broadcast domain set of the policy is the set of broadcast domains for its nodes.

In an implementation of a policy, there is a group security association per broadcast domain. Further, each station (node) possesses the group security association of the broadcast domain for itself in the policy, and of every other broadcast domain in the policy of which it is a member. The former association may be used by the station for sending group frames and the latter associations for receiving group frames.

The accessibility within a three-station virtual BSS, one of which is an AP, is captured by the policy shown in Figure 2. Each node in the policy has {*A*, *B*, *AP*} as its broadcast domain. Thus, there is only one broadcast domain for the policy which is what one would expect given that the policy reflects a virtual BSS. Each station knows the group security association for the domain, and can send and receive group frames under that association.

Figure 3 captures a policy among four stations where stations *A* and *B* share server stations *S* and *D* but *A* and *B* are not allowed to access each other.

The policy has broadcast domains B1: {*A*, *S*, *D*}, B2: {*B*, *S*, *D*} and B3: {*D*, *A*, *S*, *B*}. Station *A* knows the group security association for B1, to send group frames, and the group security association for B3 to receive group frames sent by *S* and *D*. Station *D* knows the group security association for B3, to send group frames and to receive them from *S*, and the group security associations for both B1 and B2 to receive group frames from *A* and *B* respectively.

If the policy in Figure 3 were modified so that an edge from, say *B*, to *A* were added to the policy, as illustrated in Figure 4, then domain B2 would be eliminated and only B1 and B3 would remain.

If an edge from *A* to *B* were added to the policy in Figure 4 then domains B1, B2 and B3 would collapse into the single domain B3 for the policy.

The provision of other policy variations are within the ability of those skilled in the art.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. A security apparatus for a wireless LAN, comprising:

a plurality of end stations; and

a Public Access Point (PAP) for providing a plurality of virtual Basic Service Sets (BSS) from within a single physical access point (AP);

wherein any number of said end stations can belong to a virtual BSS;

wherein said PAP appears to said end stations as multiple physical access points, one AP for each virtual BSS.

2. The apparatus of Claim 1, said PAP provisioning a plurality of separate LAN segments while providing separate link privacy and integrity for each of said LAN segments.

3. The apparatus of Claim 1, wherein all of said end stations, and any local file servers and other devices associated with said LAN, are associated with a virtual access point; and wherein all virtual access points arise from a same physical PAP.

4. The apparatus of Claim 1, further comprising:

a plurality of PAPs; and

a location-update protocol for updating forwarding tables of bridges that connect said PAPs together.

5. The apparatus of Claim 1, further comprising:

a finebridging method for limiting communications between all said end stations that belong to a virtual BSS.

6. A security apparatus for a wireless LAN, comprising:

a plurality of 802.11 end stations;

a Public Access Point (PAP), said PAP comprising a personal virtual bridged LAN (PVLAN) instantiated into a virtual 802.11 Basic Service Set (BSS) from within a single physical access point (AP).

7. A secure wireless network, comprising:

a virtual 802.11 Basic Service Set (BSS);

a plurality of stations, each of said stations having a hardware (MAC) address;

all said stations in said virtual BSS sharinga group security association; and

one of said stations in said virtual BSS comprising a public access point (PAP).

8. The network of Claim 7, said group security association of each station comprising:

an encryption key and an authentication code key.

9. The network of Claim 7, wherein exactly one of said stations in said virtual BSS is a public access point for bridging an 802.11 Wireless Medium (WM) and an 802.11 Distribution System Medium (DSM).

10. The network of Claim 7, said group security association further comprising:

a unique unicast security association for every station in said virtual BSS;

wherein said security association is shared between each station and said PAP of said virtual BSS.

11. The network of Claim 7, further comprising:

a plurality of virtual BSSs, wherein each virtual BSS has its own identifier, (BSSID).

12. The network of Claim 11, said BSSID comprising:

a virtual MAC address for said virtual BSS.

13. The network of Claim 12, wherein said PAP receives a frame from an 802.11 Wireless Medium (WM) destined for one of its virtual MAC addresses; and wherein

said PAP transmits a frame to said WM using one of its virtual MAC addresses as a source MAC address of said frame.

14. The network of Claim 7, further comprising:

a plurality of virtual BSSs supported by a shared TSF (Timing Synchronization Function), DCF (Distributed Coordination Function), and, optionally, a PCF (Point Coordination Function), at a single PAP.

15. The network of Claim 7, each PAP further comprising:

a single NAV (Network Allocation Vector) and PC (Point Coordinator).

16. The network of Claim 7, wherein a PAP can belong to more than one virtual BSS.

17. The network of Claim 7, wherein any station that is not a PAP can belong to at most one virtual BSS.

18. The network of Claim 7, further comprising:

a virtual bridged LAN (VLAN) for bridging a virtual BSS with another virtual BSS by connection of each virtual BSS's PAP.

19. The network of Claim 18, wherein the PAP of each virtual BSS connects to a Distribution System (DS) via a trunked or untagged port of a VLAN-aware bridge.

20. The network of Claim 19, wherein frames transmitted to said DS carry VLAN tags known to a Distribution System Medium (DSM).

21. The network of Claim 20, wherein said PAP maintains a DSM VLAN mapping that maps a VLAN tag to a virtual BSS identifier (BSSID).

22. The network of Claim 7, said virtual BSS comprising any of:

a Class-1 and a Class-3 virtual BSS;

wherein a PAP supports exactly one Class-1 virtual BSS and one or more multiple Class-3 virtual BSSs;

wherein a Class-1 virtual BSS is the only virtual BSS which a station is allowed to occupy while it is in 802.11 State 1 or 2, as governed by said PAP;

wherein when in State 3, a station is allowed to join a Class-3 virtual BSS; and

wherein a Class-3 virtual BSS is determined by the kind of authentication used to authenticate said station.

23. The network of Claim 22, wherein a Class-1 virtual BSSID is the BSSID field of every Class 1 and Class 2 frame that has such a field.

24. The network of Claim 22, wherein a Class-1 virtual BSSID is the receiver or transmitter address field, where appropriate, for Class 1 and Class 2 frames.

25. The network of Claim 7, wherein every virtual BSS has identical beacon frame content except for a Timestamp, Beacon interval, Capability information Privacy (Protected) bit, Service Set Identifier (SSID), security capability element, and Traffic Indication Map (TIM) element fields.

26. The network of Claim 22, wherein said PAP does not have to beacon for a Class-3 virtual BSS if it does not support Power-Save (PS) mode for end stations in that BSS;

wherein if said PAP does beacon for a Class-3 BSS, then an SSID element in every beacon specifies a broadcast SSID;

wherein a Class-3 virtual BSS is prevented from being identified through beaconing.

27. The network of Claim 26, wherein only a Class-1 virtual BSS beacon has an SSID element with a non-broadcast SSID field;

wherein a station can associate with a Class-1 virtual BSS only;

28. The network of Claim 22, wherein every station is by default a member of a Class-1 virtual BSS at a PAP;

wherein said PAP can either authenticate a user of said station or said station itself in said Class-1 virtual BSS;

wherein if successful, said station enters 802.11 State 2 at said PAP; and

wherein said PAP and said station can then exchange Class 1 and Class 2 frames while in said Class-1 virtual BSS.

29. The network of Claim 28, wherein Class 2 frames are protected cryptographically if said station and said PAP share a unicast security association after successful authentication.

30. The network of Claim 29, wherein said PAP and said station share a group security association after authentication;

wherein said group security association is for a Class-3 virtual BSS to which said station belongs if it completes an 802.11 Association with said PAP.

31. The network of Claim 30, wherein before said station and said PAP can exchange Class 3 frames, said station must request Association with said Class-1 virtual BSS from State 2; and switch to a Class-3 virtual BSS.

32. The network of Claim 31, wherein said PAP switches said station to a Class-3 virtual BSS by responding to said station's Association Request with an Association Response MMPDU whose source address (Address 2 Field) or BSSID (Address 3 field) is a Class-3 virtual BSSID for that virtual BSS.

33. The network of Claim 32, wherein said Class-3 virtual BSS is determined in one of the following ways:

an authentication server in said DS specifies a DSM VLAN for a user and said PAP maps it to a Class-3 virtual BSSID using its DSM VLAN mapping;

an authentication server in said DS specifies a Class-3 virtual BSS for said user; or

said PAP creates a new Class-3 virtual BSS for said user;

wherein said PAP may inform an authentication server of a new virtual BSS and provide it with rules for allowing other stations to join said new BSS.

34. The network of Claim 22, wherein a Class-1 virtual BSS is discovered through 802.11 beacon or Probe Response management frames, where a BSSID field

(Address 3 field) and source address field (Address 2 field) are each set to a Class-1 virtual BSSID.

35. The network of Claim 22, wherein said PAP implements a MAC Protocol Data Unit (MPDU) bridge protocol which, for an MPDU received from either said DSM or said WM, said protocol addresses either of:

an MPDU received from said DSM, wherein:

a received MPDU has no VLAN tag or a null VLAN tag;

said MPDU from said DSM is relayed to a virtual BSS if said MPDU destination address is an address of a station that belongs to said virtual BSS and said station is associated with said PAP; or

if said MPDU destination address is a group address, said virtual BSS has a station that belongs to said group and said station is associated with said PAP; or

a received MPDU has a non-null VLAN tag;

said virtual BSS to which said MPDU is relayed is identified by said virtual BSSID to which said non-null VLAN tag is mapped under said PAP's DSM VLAN mapping; and

if said mapping is undefined for a given tag, said MPDU is not relayed;

wherein any virtual BSS to which a received MPDU is relayed has a BSSID which forms a source address (Address 2 field) of the 802.11 MPDU that is relayed to that virtual BSS; or

an MPDU received from said WM, wherein:

a received 802.11 MPDU is relayed to a virtual BSS identified by Address 1 field of said MPDU if said MPDU destination address (Address 3 field of MPDU) is an address of a station that belongs to said identified virtual BSS and said station is associated with said PAP; or

if said MPDU destination address is a group address;

otherwise, said frame is not relayed to any virtual BSS;

wherein Address 1 field of a received 802.11 MPDU is a source address (Address 2 field) of an 802.11 MPDU that is relayed to said virtual BSS identified by said Address 1 field.

36. The network of Claim 35, wherein said received MPDU is also relayed to said DSM if said destination address (Address 3 field of MPDU) is an address of a station that is not associated with said PAP; or

if said destination address is a group address;

wherein said MPDU relayed to said DSM has a VLAN tag if said DS is VLAN aware, and is untagged otherwise; and

wherein said VLAN tag is a pre-image of said Address 1 field of said received MPDU under said PAP's DSM VLAN mapping.

37. The network of Claim 22, further comprising:

means for performing encryption and decryption by applying 802.11 Data frames and Management frames of subtype Association Request/Response, Reassociation Request/Response, Disassociation and Deauthentication.

38. The network of Claim 37, wherein said encryption process used by said PAP before sending an 802.11 Data or Management frame to said WM comprises a mechanism that performs the steps of:

identifying a security association for said frame; and

then using said association to construct an expanded frame for transmission according to an encipherment and authentication code protocol.

39. The network of Claim 38, wherein if a frame destination address (Address 1 field) is the address of a station then a unicast security association shared between that station and said PAP is used in said frame expansion; and

wherein if said frame is a Data frame and its destination address is a group address then said MPDU bridge protocol identifies a destination virtual BSS for said frame, wherein a group security association for said identified virtual BSS is used in said frame expansion.

40. The network of Claim 39, wherein a non-PAP station transmits an 802.11 MPDU of type Data or Management to said DSM using a unicast security association it shares with said PAP in its virtual BSS.

41. The network of Claim 40, wherein when receiving an 802.11 Data or Management frame from said WM, said PAP attempts to decipher and verify integrity of said frame using a unicast security association for a station identified by a source address (Address 2 field) of said MPDU.

42. The network of Claim 41, wherein when receiving an 802.11 MPDU of type Data or Management from said PAP, a non-PAP station attempts to decipher and verify integrity of said frame using a unicast security association it shares with said PAP if a destination address of said frame (Address 1 field) is an address of said station, and by using a group security association of its Class-3 virtual BSS if said destination address of said frame is a group address.

43. A location-update method for updating forwarding tables of bridges, or other interconnection media, that connect Public Access Points (PAPs) together, where multiple PAPs are attached to different bridges in a spanning tree of a bridged LAN and an end station associates with one of said PAPs and then reassociates with a new PAP, comprising the steps of:

said new PAP sending a directed Bridge Protocol Data Unit (BPDU) to said PAP with which said station was previously associated;

wherein destination address of said BPDU is current access point (AP) address of a Reassociation Request frame, which is a Class-3 virtual BSS identifier (BSSID); and

wherein source address is a hardware address of said station;

upon receiving a relocation MPDU at a particular port, a bridge updating its forwarding table with an entry that binds a receiving port to a source address of said MPDU; and

said receiving bridge forwarding a relocation MPDU to its designated root port, unless said MPDU arrived on that port or said receiving bridge is a root of said spanning tree;

wherein if said MPDU is received at said designated root port of said bridge or by a root bridge then it is forwarded according to a learned forwarding table of said bridge, which optionally comprises flooding said MPDU to all ports except said receiving port.

44. A fine bridging method for a wireless network, comprising the steps of:

decoupling identification of a broadcast or multicast domain with a Basic Service Set (BSS); and

determining bridging behavior of an access point (AP) by a policy expressed as a directed graph;

wherein for a given policy, a broadcast domain for a node is itself and all nodes it must access;

wherein said broadcast domain set of said policy is a set of broadcast domains for its nodes; and

wherein nodes of said graph are stations and there is an edge from a first station to a second station if and only if said first station must be able to communicate with, or access said second station, such that said second station must be able to receive directed or group frames from said first station.

45. The method of Claim 43, further comprising the step of:

providing a group security association per broadcast domain.

46. The method of Claim 45, wherein each station (node) possesses a first group security association of a broadcast domain for itself in said policy, and a second set of group security associations, one for every other broadcast domain in said policy of which said station is a member.

47. The method of Claim 46, wherein said first group security association is used by said station for sending group frames and said second set of group security associations is used for receiving group frames.

48. The network of Claim 42, wherein broadcast and multicast traffic in different virtual basic service sets is protected with different encipherment or authentication-code protocols in said network.

49. The Network of Claim 42, where unicast traffic between a PAP and a station and between said PAP and another station in a virtual BSS is protected with different encipherment or authentication-code protocols in said virtual BSS.

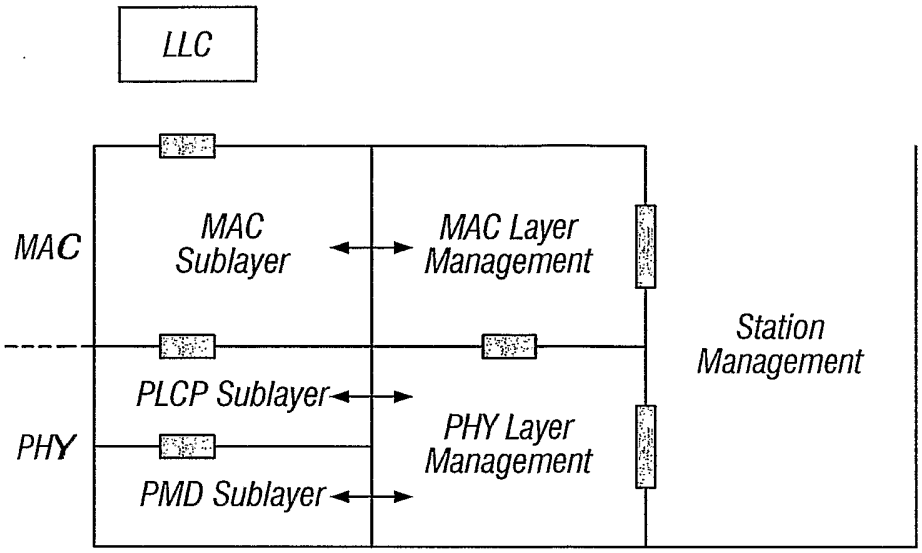

FIG. 1
(Prior Art)

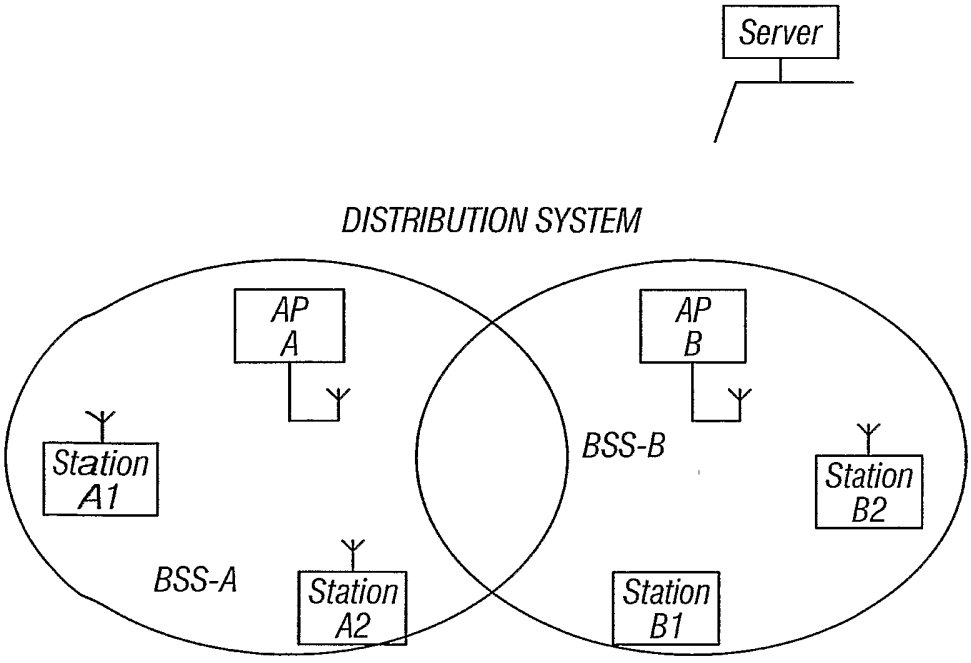

FIG. 2
(Prior Art)

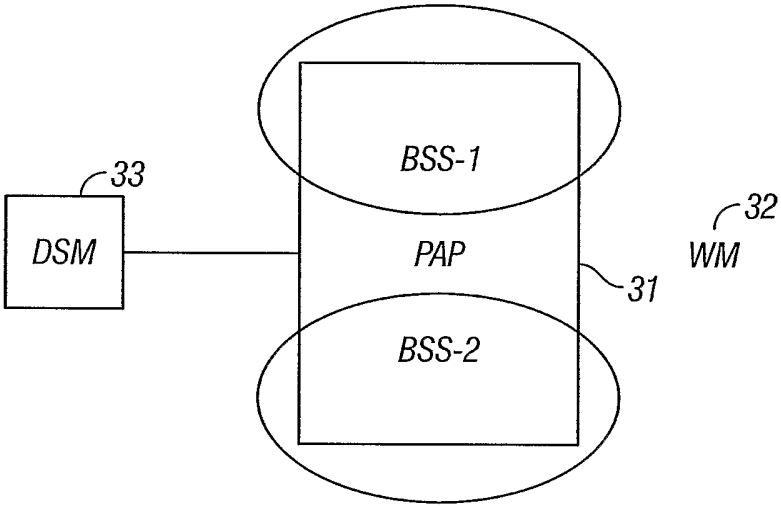

FIG. 3

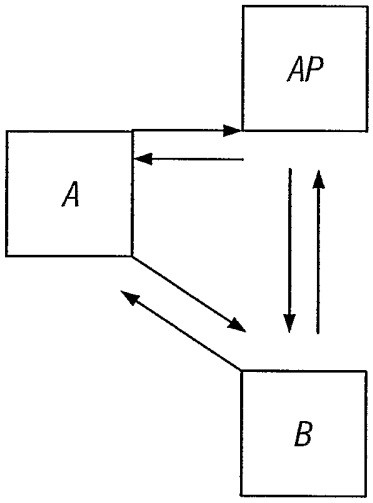

FIG. 4

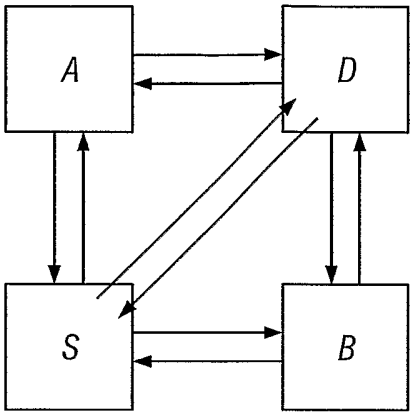

FIG. 5

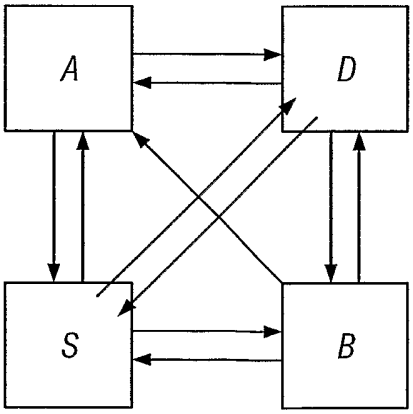

FIG. 6

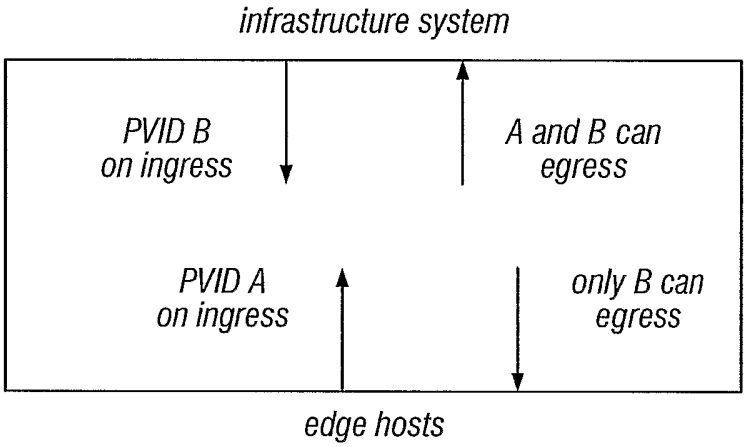

FIG. 7
(Prior Art)