

802.11 WIRELESS SECURITY IN BUSINESS NETWORKS



With the increasing deployment of 802.11 wireless networks in business environments, IT organizations are working to implement security mechanisms that are equivalent to those existing today for wire-based networks. An important aspect of this is the need to provide secure access to the network for valid users. Existing wired network jacks are located inside buildings already secured from unauthorized access through the use of keys, badge access, and so forth. A user must gain physical access to the building in order to plug a client computer into a network jack. In contrast, a wireless access point (AP) may be accessed from off the premises if the signal is detectable (for instance, from a parking lot adjacent to the building). Thus, wireless networks require secure access to the AP and the ability to isolate the AP from the internal private network prior to user authentication into the network domain.

This article begins by discussing the basic access control methods that form the basis of the 802.11 architecture. These methods are best suited to small networks with low-to-medium security requirements. The article then presents the more-robust virtual private network (VPN)-based security solution that provides better security and scales well to large networks. The article concludes with a possible future solution based on the upcoming 802.1X security standard, which enables port-level access control.

Basic 802.11 Security

There are currently three basic methods to secure access to an AP that are built into 802.11 networks:

- Service set identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or all of these methods may be implemented, but all three together provide a more robust solution. (Network administrators may also choose not to implement any of these methods.)

SSID

Network access control can be implemented using an SSID associated with an AP or group of APs. The SSID provides a mechanism to “segment” a wireless network into multiple networks serviced by one or more APs. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID. A building might be segmented into multiple networks by floor or department. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the AP is configured to “broadcast” its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the AP. In addition, because users typically configure their own client systems with the appropriate SSIDs, they are widely known and easily shared. (It is strongly recommended that APs be configured with broadcast mode disabled.)

MAC Address Filtering

While an AP or group of APs can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client is not allowed to associate with the AP.

MAC address filtering (along with SSIDs) provides improved security, but is best suited to small networks where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date.

This administrative overhead limits the scalability of this approach.

WEP-Based Security

Wireless transmissions are easier to intercept than transmissions over wired networks. The 802.11 standard currently specifies the WEP security protocol to provide encrypted communication between the client and an AP. WEP employs the symmetric key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG).

Under WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. The 802.11 standard does not specify a key management protocol, so all WEP keys on a network must be managed manually. Support for WEP is standard on most current 802.11 cards and APs. WEP security is not available in ad hoc (or peer-to-peer) 802.11 networks that do not use APs.

WEP specifies the use of a 40-bit encryption key and there are also implementations of 104-bit keys. The encryption key is concatenated with a 24-bit "initialization vector," resulting in a 64- or 128-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted.

Recently, WEP encryption has been proven to be vulnerable to attack. Scripting tools exist that can be used to take advantage of weaknesses in the WEP key algorithm to successfully attack a network and discover the WEP key. The industry and IEEE are working on solutions to this problem, and the Advanced Encryption Standard (AES) has been identified as a possible replacement encryption technology for WEP.

Meanwhile, despite the weaknesses of WEP-based security, it can still be a component of the security solution used in small, tightly managed networks with low-to-medium security requirements. In these cases, 128-bit WEP should be implemented in conjunction with MAC address filtering and SSID (with the broadcast feature disabled). Customers should change WEP keys on a regular schedule to minimize risk.

For networks with high security requirements, the VPN solution discussed in the next section is preferable. The

VPN solution is also preferable for large networks, in which the administrative burden of maintaining WEP encryption keys on each client system and AP, as well as MAC addresses on each AP, makes these solutions impractical. In addition, because all clients and APs use the same WEP encryption key, a lost or stolen client system requires that all keys be changed.

The point at which the number of wireless client systems becomes unmanageable varies depending on the organization's ability to administer the network, the choice of security methods (SSID, WEP, and MAC address filtering) and its tolerance for risk. If MAC address filtering is used on a wireless network, the fixed upper limit is established by the maximum number of MAC addresses that can be programmed into each AP used in an installation. In some cases, this upper limit is 255. However, the manageable number of clients when using MAC address filtering is likely to be considerably less than 255 clients for many organizations.

Figure 1 depicts WEP-based security with MAC address filtering.

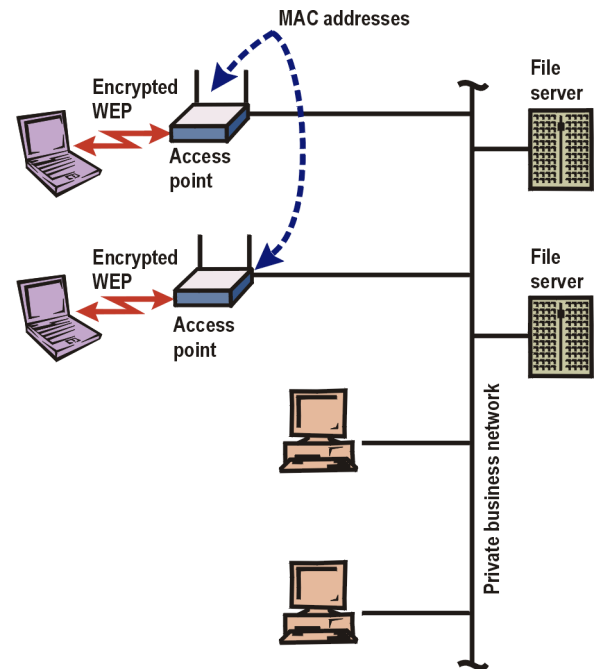


Figure 1. 802.11 Security Using SSID, MAC Address Filtering, and WEP

VPN Wireless Security

For business networks, a VPN solution for wireless access is currently the most suitable alternative to WEP and MAC address filtering. VPN solutions are already widely deployed to provide remote workers with secure access to the network via the Internet. In this remote user application, the VPN provides a secure, dedicated path (or “tunnel”) over an “untrusted” network—in this case, the Internet. Various tunneling protocols, including the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) are used in conjunction with standard, centralized authentication solutions, such as Remote Authentication Dial-In User Service (RADIUS) servers.

The same VPN technology can also be used for secure wireless access. In this application, the “untrusted” network is the wireless network. The APs are configured for open access with no WEP encryption, but wireless access is isolated from the enterprise network by the VPN server and a VLAN between the APs and the VPN servers. (The APs should still be configured with SSIDs for network segmentation.) Authentication and full encryption over the wireless network is provided through the VPN servers that also act as gateways to the private network. Unlike the WEP key and MAC address filtering approaches, the VPN-based solution is scalable to a very large number of users.

Figure 2 shows how VPN connections can provide flexible access to a private network. Remote workers can use a dial-up, cable modem, or Digital Subscriber Line (DSL) connection to the Internet and then establish a VPN connection to the private network. Public wireless APs in locations such as airports can also be used to establish a VPN connection back to the private network. Finally, on-campus 802.11 wireless access can be implemented via a secure VPN connection. The user login interface is the same for each of these scenarios, so that the user has a consistent login interface.

The VPN approach has a number of advantages:

- Currently deployed on many enterprise networks.
- Scalable to a large number of 802.11 clients.
- Low administration requirements for 802.11 APs and clients. The VPN servers can be centrally administered.

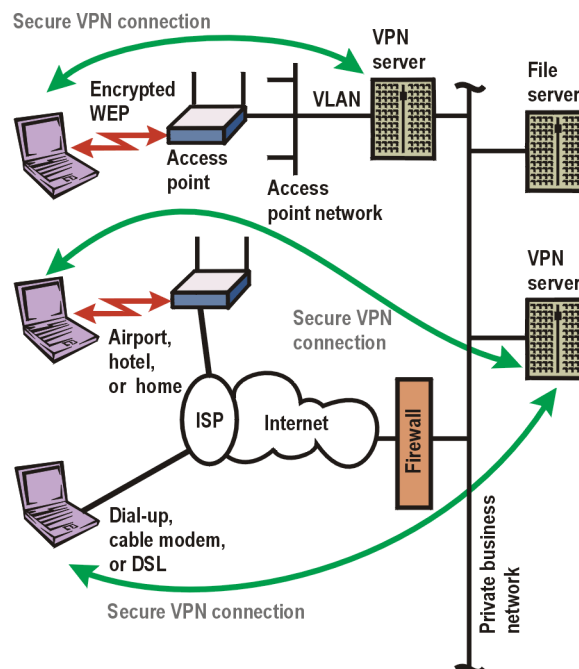


Figure 2. 802.11 VPN Wireless Security

- Traffic to the internal network is isolated until VPN authentication is performed.
- WEP key and MAC address list management becomes optional because of security measures created by the VPN channel itself.
- Consistent user interface in different locations such as at home, at work, and in an airport.

A drawback to current VPN solutions is the lack of support for multicasting. See “Multicasting to Wireless Clients” later in this article.

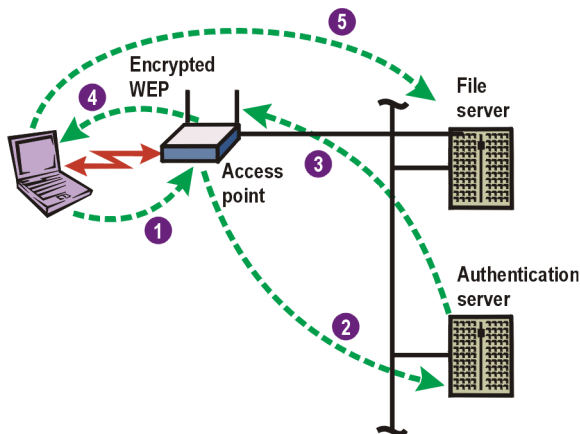
Another minor drawback is that roaming between wireless networks is not completely transparent. Users receive a logon dialog when roaming between VPN servers on a network or when the client system resumes from standby mode.

It is highly recommended that all VPN client computers be equipped with personal firewall protection. (See “Firewall Protection” later in this article.)

Future Direction: Port-Based Network Access With 802.1X

On the horizon is a draft IEEE standard, 802.1X, for generic, extensible port-based authentication. The specification is general: it applies to both wireless and wired Ethernet networks. In the context of an 802.11

wireless network, 802.1X is used to securely establish an authenticated association between the client and the AP. Generally, the scenario would be as follows. The user of an 802.11 wireless client system (rather than the client system itself) requests access to an AP. The AP passes the request to a centralized authentication server that handles the authentication exchange and, if successful, provides an encryption key to the AP. The AP uses the key to securely transmit a unicast session or multicast/global encryption key to the client. At this point, the client has access to the network, and transmissions between the client and AP are encrypted. (Currently, WEP is the only encryption method supported by the 802.11 standard, but AES is being considered as a replacement method.) At this point, the user may log on to the network domain. Figure 3 summarizes this process.



1. User requests authentication. AP prevents network access.
2. Encrypted credentials sent to authentication server (RADIUS).
3. Authentication server validates user and grants access rights.
4. AP port is enabled and WEP keys are assigned to client (encrypted).
5. Wireless client accesses general network services securely.

**Figure 3. Possible Future 802.1X/
RADIUS Architecture**

802.1X does not require a specific protocol for authentication. Instead, it specifies that the Extensible Authentication Protocol (EAP) will be used. EAP is an encapsulation protocol that allows different authentication protocols to be selected and used. Effectively, EAP serves as a conduit for other authentication protocols such as RADIUS, Kerberos, and Secure IDs.

The 802.1X draft standard also includes a management specification for complete end-to-end management of the 802.1X protocol.

The 802.1X approach has the following advantages:

- Standards-based.
- Flexible authentication: administrators may choose the type of authentication method used.
- Scalable to large enterprise networks.
- Centrally managed.
- Encryption keys are dynamically generated and propagated.
- Because authentication is central, rather than at each AP, roaming can be made as transparent as possible. At most, the user may be asked for alternate credentials if an AP requires alternate identification.

The 802.1X standard was finalized in June 2001 and future Microsoft® Windows® operating systems are expected to include native 802.1X support.

802.1X and VPNs

802.1X is designed to authenticate and distribute encryption keys (currently WEP) between the wireless client and an AP. It is not designed to be a generalized VPN solution suitable for secure remote access. Thus, VPNs are still required for remote access using public APs (in airports or hotels) and from remote or home offices.

Multicasting to Wireless Clients

Multicasting is a technique used to deliver data efficiently in real time from one source to many users over a network. In some large networks, a portion of the network bandwidth is used for multicasting applications such as streaming audio and video applications (press conferences, training classes, and so forth) to groups of users. These data streams, if "unicast" (that is, transmitted individually) to each end user, would be a much greater burden on the network. Multicasting uses network bandwidth more efficiently by transmitting these types of data as one common data stream over the backbone. In most cases, network switches then deliver individual data streams to each client connected to them.

Multicasting requirements must be carefully considered when designing an 802.11 wireless network. While multicasting is supported in 802.11 networks, current bandwidth limitations at the AP, as well as WEP key management issues, restrict the ability to deliver these data streams efficiently and securely to wireless clients. Current 802.11b (also referred to as Wi-Fi) APs have a maximum theoretical bandwidth of 11 Mbps, which must be shared by all clients accessing the AP. Depending on its volume, multicasting traffic can reduce the AP's available bandwidth significantly. In addition, if WEP encryption is used to secure the wireless network, a separate key must be configured on each client to support multicasting (in addition to the key required for unicast traffic). Further, current VPN solutions only support multicast by unicasting the data stream individually to each wireless VPN client. Because of these limitations, multicasting to wireless clients can be problematic in real-world, secure deployments.

The 802.1X draft standard addresses some of these multicasting issues by enabling dynamic encryption key management. Keys can be issued and managed in real time—provided authentication succeeds—so that dynamic multicast key distribution becomes possible in large organizations.

Firewall Protection

In addition to the security solutions presented in this article, all 802.11 client systems should be equipped with

personal firewall software protection. Like PCs with “always on” cable modem and DSL Internet access connections, 802.11 clients can be vulnerable to hacker attacks from other users connected to the AP. The nature of these attacks may vary, but the goal of firewall software is to protect the roaming user's confidential local data against as many possible attacks as are currently known and understood.

Summary

As 802.11 networks proliferate and mature, robust security solutions are required. The basic 802.11 security solutions that are available “out of the box”—SSID, MAC address filtering, and WEP—are suitable for small, tightly managed networks with low-to-medium security requirements. For networks with high security requirements, the weaknesses in WEP encryption require a more robust solution. In addition, the manual task of maintaining MAC addresses and WEP keys becomes overwhelming as the number of wireless clients increase. For larger networks, or for networks with high security requirements, a VPN solution based on currently available technology provides a very scalable solution for 802.11 networks. VPN for wireless is also a logical extension of the remote access VPN capability found in most large businesses today. Finally, on the horizon is 802.1X, a standards-based solution for port-level authentication for any wired or wireless Ethernet client system.