



IEEE 802.11 Wireless LAN Security with Microsoft Windows

*Microsoft Corporation
Published: June 2006*

Abstract

Although wireless LAN networks provide freedom of movement, they also require you to address security issues that are not as prevalent on a private cabling system for a wired LAN technology such as Ethernet. The main security issues are the authentication of wireless clients and the encryption and data integrity of wireless LAN frames. This article discusses the security issues of IEEE 802.11 wireless networks and shows how Microsoft® Windows® operating systems can be used to make 802.11 wireless networks as secure as the current set of 802.11-related technologies allow.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

Introduction	1
Wireless Security with the IEEE 802.11 Standard	2
Authentication	2
Open System Authentication.....	2
Shared Key Authentication	2
Encryption and Data Integrity	3
WEP	4
WEP Encryption Process	4
WEP Decryption Process	5
Security Issues with the IEEE 802.11 Standard	6
Authentication with the IEEE 802.1X Standard	7
Elements of 802.1X	7
Port access entity	7
Authenticator	7
Supplicant.....	8
Authentication Server.....	8
Controlled and Uncontrolled Ports.....	8
EAP Overview	9
EAP Over RADIUS	10
EAP-TLS Authentication	10
IEEE 802.1X Authentication Process for EAP-TLS.....	11
PEAP-MS-CHAP v2 Authentication.....	14
MS-CHAP v2 Overview	14
PEAP with MS-CHAP v2 Operation	14
PEAP Fast Reconnect.....	19
802.1X and 802.11 Security Issues	20
Wi-Fi Protected Access (WPA)	21
WPA Security Features	21
Authentication	21
Encryption	22
Data Integrity.....	22
Required Software Changes for WPA Support	22
Wireless Access Points.....	23
Wireless Network Adapters	23
Wireless Clients.....	23
Supporting a Mixed Environment	24
Wi-Fi Protected Access 2	25
Recommended Security Configurations	26
Attacks on Wireless Networks	27
Summary	28
Related Links	29

Introduction

Wireless networks broadcast their network data using radio signals. Unlike wired networking technologies such as Ethernet, it is difficult to control access to the wireless networking media. For example, with wired networks you must have physical access to a network jack. If you use wireless networks, you do not even need to be in the building; you can access the wireless network from across the street. The difference between wired and wireless networks is illustrated in the following comparison:

- With wired networks, the medium is private. You do not have to worry about who is connecting because the assumption is that unauthorized users cannot gain access to a network plug. You also do not have to ensure that the traffic is made confidential, because the traffic is sent over a private cabling system that is not accessible to unauthorized users.
- With wireless networks, the medium is public. Anyone with the proper wireless equipment that is within association range can connect. The network traffic must also be made confidential because the unauthorized user can receive wireless frames without being present in physically securable areas.

Therefore, for wireless LANs, security is a required element of the technology, its implementation, and its deployment. Properties of secure communications for wireless networks consist of the following:

- **Authentication** Before being allowed to exchange data traffic with the wireless network, the wireless network node must be identified and (depending on the authentication method) must submit credentials that can be validated.
- **Encryption** Before sending a wireless data packet, the wireless network node must encrypt the data to ensure data confidentiality.
- **Data integrity** Before sending a wireless data packet, the wireless network node must include information in the packet so the receiver can determine that the contents of the packet were not modified in transit.

Wireless Security with the IEEE 802.11 Standard

The original IEEE 802.11 standard defined authentication, encryption, and data integrity for wireless traffic. As we will discuss, the original authentication, encryption, and data integrity proved to be relatively weak and cumbersome for widespread public and private deployment. Subsequent sections of this article describe the additional standards that provide stronger authentication methods and discuss enhancements to the originally defined encryption and data integrity methods or replacements for them.

Authentication

IEEE 802.11 defines the following types of authentication, discussed in the following sections:

- Open system authentication
- Shared key authentication

Open System Authentication

Open system authentication does not provide authentication, only identification using the wireless adapter's media access control (MAC) address. This authentication is used when no authentication is required, and it is the default authentication algorithm that uses the following process (shown in Figure 1):

1. The authentication-initiating wireless client sends an Open System Authentication Request message, which contains the MAC address as the source address of the 802.11 frame.
2. The receiving wireless node responds with an Open System Authentication Response message that indicates either success (the authentication-initiating wireless client is authenticated) or failure.

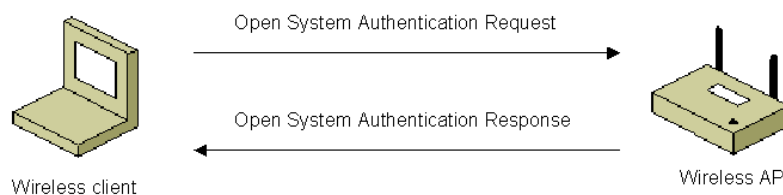


Figure 1 Open system authentication

Some wireless APs allow you to configure a list of MAC addresses of wireless clients that are authorized. However, this does not provide security for a wireless network because an attacker can easily capture wireless packets and then use the MAC address of a valid wireless client as its own.

Shared Key Authentication

Shared key authentication verifies that an authentication-initiating station has knowledge of a shared secret. The IEEE 802.11 standard currently assumes that the shared secret is delivered to the participating wireless clients by means of a secure channel that is independent of IEEE 802.11. In practice, this secret is a sequence of characters typed during the configuration of the wireless AP and the wireless client.

Shared key authentication uses the following process (shown in Figure 2):

1. The authentication-initiating wireless client sends a Shared Key Authentication Request frame.

2. The authentication-enforcing wireless node responds with a Shared Key Authentication Response frame that contains challenge text.
3. The authentication-initiating wireless node responds with a Shared Key Authentication Request frame that contains an encrypted form of the challenge text, which is encrypted using Wired Equivalent Privacy (WEP) (the encryption method used on 802.11 wireless networks) and the shared key authentication key.
4. The authentication-enforcing wireless node decrypts the encrypted challenge text in the Shared Key Authentication Request frame using WEP and the shared key authentication key. If the decrypted challenge text matches the originally sent challenge text, the authentication-enforcing wireless node sends a Shared Key Authentication Response frame that indicates authentication success. Otherwise, the authentication-enforcing wireless node sends a Shared Key Authentication Response frame that indicates authentication failure.

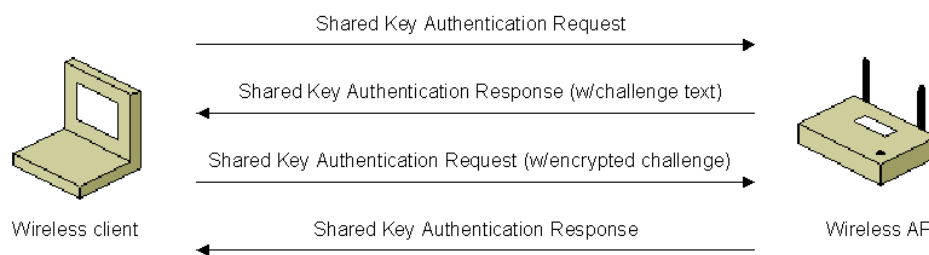


Figure 2 Shared key authentication

Because the shared key authentication secret must be manually distributed and typed, this method of authentication does not scale appropriately in large infrastructure mode networks (for example, corporate campuses and public places).

Another serious problem with shared key authentication is that for configuration simplicity, the shared key authentication key is the same as the WEP encryption key used to encrypt all data between the authentication-initiating wireless client and the authentication-enforcing wireless node. The shared key authentication exchange includes a plaintext (the challenge text) and ciphertext (the encrypted challenge text) exchange with an indication of success. An attacker can capture a successful shared key authentication exchange and determine the shared key authentication key, which is also the WEP encryption key, through cryptanalysis methods. When the WEP encryption key is determined, the attacker has full access to the wireless network and can begin attacking wireless nodes. Therefore, the use of shared key authentication is highly discouraged, even for small office/home office (SOHO) wireless networks.

For more information about SOHO wireless networks, see [Step-by-Step Guide for Secure Wireless Deployment for Small Office/Home Office or Small Organization Networks](#) and [Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business](#).

Encryption and Data Integrity

Due to the broadcast nature of wireless LAN networks, eavesdropping and remote sniffing of wireless LAN frames is very easy. Wired Equivalent Privacy (WEP) is defined by the IEEE 802.11 standard and is intended to provide a level of data confidentiality and integrity that is equivalent to a wired network.

WEP

WEP provides data confidentiality services by encrypting the data sent between wireless nodes. Setting a WEP flag in the MAC header of the 802.11 frame indicates that the frame is encrypted with WEP encryption. WEP provides data integrity by including an integrity check value (ICV) in the encrypted portion of the wireless frame.

WEP defines two shared keys:

- **Multicast/global key** The multicast/global key is an encryption key that protects multicast and broadcast traffic from a wireless AP to all of its connected wireless clients.
- **Unicast session key** The unicast session key is an encryption key that protects unicast traffic between a wireless client and a wireless AP and multicast and broadcast traffic sent by the wireless client to the wireless AP.

WEP encryption uses the RC4 symmetric stream cipher with 40-bit and 104-bit encryption keys. Although 104-bit encryption keys are not specified in the 802.11 standard, many wireless AP vendors support them.

Some implementations that advertise the use of 128-bit WEP encryption keys are just adding a 104-bit encryption key to the 24-bit initialization vector (IV) and calling it a 128-bit key. The IV is a field in the header of each 802.11 frame that is used during the encryption and decryption process.

WEP Encryption Process

To encrypt the payload of an 802.11 frame, the following process is used (shown in Figure 3):

1. A 32-bit ICV is calculated for the frame data.
2. The ICV is appended to the end of the frame data.
3. A 24-bit IV is generated and appended to the WEP encryption key.
4. The combination of [IV+WEP encryption key] is used as the input of a pseudo-random number generator (PRNG) to generate a bit sequence that is the same size as the combination of [data+ICV].
5. The PRNG bit sequence, also known as the key stream, is bit-wise exclusive ORed (XORed) with [data+ICV] to produce the encrypted portion of the payload that is sent between the wireless access point (AP) and the wireless client.
6. To create the payload for the wireless MAC frame, the IV is added to the front of the encrypted[data+ICV], along with other fields.

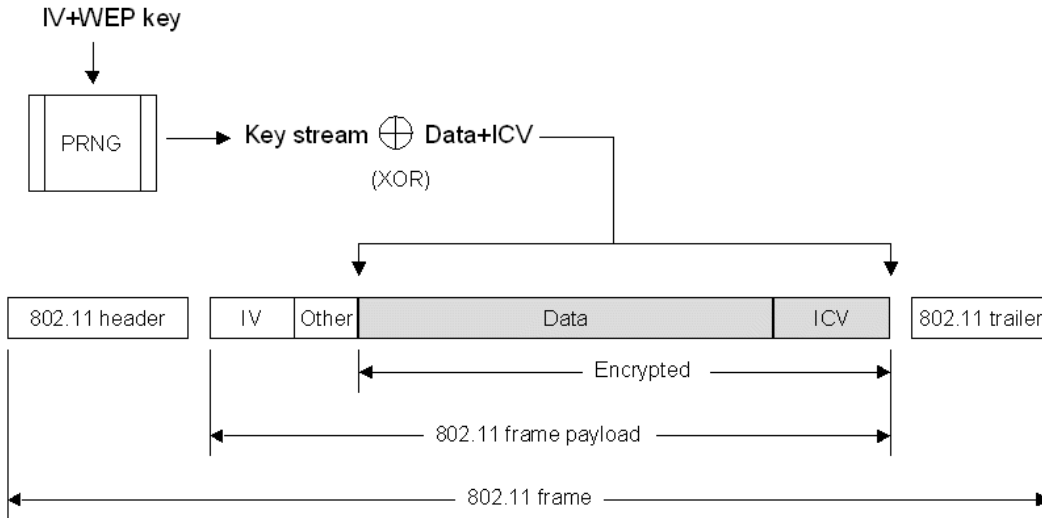


Figure 3 WEP encryption process

WEP Decryption Process

To decrypt the 802.11 frame data, the following process is used (shown in Figure 4):

1. The IV is obtained from the front of the IEEE 802.11 payload.
2. The IV is appended to the WEP encryption key.
3. The [IV+WEP encryption key] is used as the input of the same PRNG to generate a bit sequence of the same size as the combination of the data and the ICV. This process produces the same key stream as that of the sending wireless node.
4. The PRNG bit sequence is XORed with the encrypted[data+ICV] to decrypt the [data+ICV] portion of the payload.
5. The ICV calculation for the data portion of the payload is run, and its result is compared with the value included in the incoming frame. If the values match, the data is considered to be valid (sent from the wireless client and unmodified in transit). If they do not match, the frame is silently discarded.

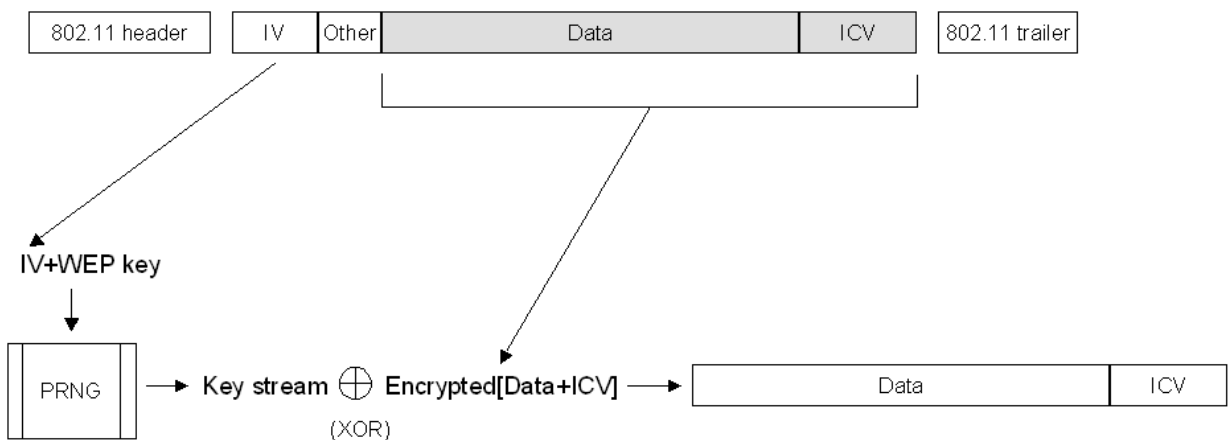


Figure 4 WEP decryption process

Although the secret key remains constant over a long duration, the IV is changed periodically and as frequently as every frame. The periodicity at which IV values are changed depends on

the degree of privacy required of the WEP algorithm. The ideal method of maintaining the effectiveness of WEP is changing the IV after each frame.

Security Issues with the IEEE 802.11 Standard

The main problem with WEP is that the determination and distribution of WEP encryption keys are not defined. WEP keys must be distributed by using a secure channel outside of the 802.11 protocol. In practice, WEP keys are text strings that must be manually configured using a keyboard for both the wireless AP and wireless clients. Obviously, this key distribution system does not scale well to an enterprise organization and is not secure.

Additionally, there is no defined mechanism to change the WEP encryption keys either per authentication or periodically for an authenticated connection. All wireless APs and clients use the same manually configured WEP key for multiple sessions. With multiple wireless clients sending a large amount of data, an attacker can remotely capture large amounts of WEP ciphertext and use cryptanalysis methods to determine the WEP key.

The lack of a WEP key management protocol is a principal limitation to providing 802.11 security, especially in infrastructure mode with a large number of stations. Some examples of this type of network include corporate and educational campuses and public places such as airports and malls. The lack of automated authentication and key determination services also affects operation in ad hoc mode, in which users may wish to engage in peer-to-peer collaborative communication in areas such as conference rooms.

The security issues that exist with the original 802.11 standard are the following:

- Rogue wireless APs.
- No per-user identification and authentication.
- No mechanism for central authentication, authorization, and accounting.
- Some implementations derive WEP keys from passwords, resulting in weak WEP keys.
- No support for extended authentication methods. For example, token cards, certificates/smart cards, one-time passwords, biometrics, and so on.
- No support for key management. For example, rekeying global keys and dynamic per-station or per-session key management.

The solution for these shortcomings of the originally defined IEEE 802.11 standard is the IEEE 802.1X standard.

Authentication with the IEEE 802.1X Standard

The IEEE 802.1X standard defines port-based, network access control used to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard was designed for wired Ethernet networks, it has been adapted for use on 802.11 wireless LANs.

Elements of 802.1X

IEEE 802.1X defines the following terms, as described in the following sections:

- Port access entity
- Authenticator
- Supplicant
- Authentication server

Figure 5 shows these components for a wireless LAN network.

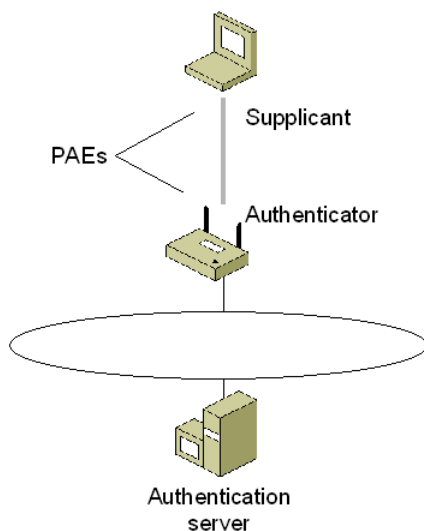


Figure 5 The components of IEEE 802.1X authentication

Port access entity

A LAN port, also known as port access entity (PAE), is the logical entity that supports the IEEE 802.1X protocol that is associated with a port. A PAE can adopt the role of the authenticator, the supplicant, or both.

Authenticator

An authenticator is a LAN port that enforces authentication before allowing access to services accessible using that port. For wireless connections, the authenticator is the logical LAN port on a wireless AP through which wireless clients in infrastructure mode gain access to other wireless clients and the wired network.

Supplicant

The supplicant is a LAN port that requests access to services accessible using the authenticator. For wireless connections, the supplicant is the logical LAN port on a wireless LAN network adapter that requests access to the other wireless clients and the wired network by associating with and then authenticating itself to an authenticator.

Whether for wireless connections or wired Ethernet connections, the supplicant and authenticator are connected by a logical or physical point-to-point LAN segment.

Authentication Server

To verify the credentials of the supplicant, the authenticator uses an authentication server, which checks the credentials of the supplicant on behalf of the authenticator and then responds to the authenticator, indicating whether or not the supplicant is authorized to access the authenticator's services. The authentication server can be the following:

- A component of the access point. In this case, the wireless AP must be configured with the sets of user credentials corresponding to authorized supplicants that will be attempting to connect (this is typically not implemented for wireless APs).
- A separate entity. In this case, the AP forwards the credentials of the connection attempt to a separate authentication server. Typically, a wireless AP uses the Remote Authentication Dial-In User Service (RADIUS) protocol to send a connection request message to a RADIUS server.

Controlled and Uncontrolled Ports

The authenticator's port-based access control defines the following different types of logical ports that access the wired LAN via a single physical LAN port:

- **Uncontrolled port** The uncontrolled port allows an uncontrolled exchange between the authenticator (the wireless AP) and other networking devices on the wired network—regardless of any wireless client's authorization state. Frames sent by the wireless client are never sent using the uncontrolled port.
- **Controlled port** The controlled port allows data to be sent between a wireless client and the wired network only if the wireless client is authorized by 802.1X. Before authentication, the switch is open and no frames are forwarded between the wireless client and the wired network. When the wireless client is successfully authenticated using IEEE 802.1X, the switch is closed, and frames can be sent between the wireless client and nodes on the wired network.

Figure 6 shows the different types of ports.

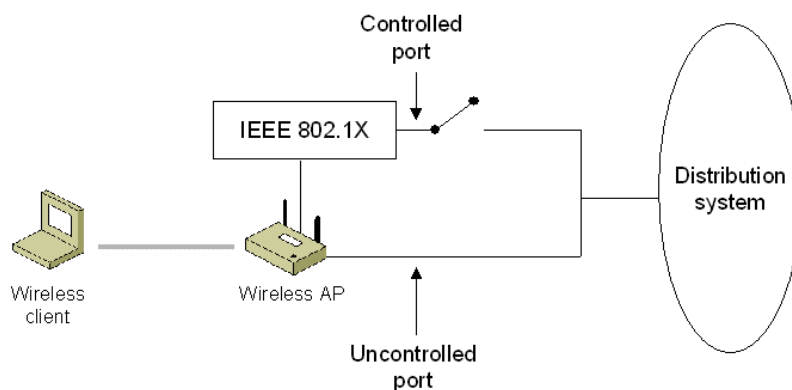


Figure 6 Controlled and uncontrolled ports for IEEE 802.1X

On an authenticating Ethernet switch, the wired Ethernet client can send Ethernet frames to the wired network as soon as authentication is complete. The switch identifies the traffic of a specific wired Ethernet client using the physical port to which the Ethernet client is connected. Typically, only a single Ethernet client is connected to a physical port on the Ethernet switch. Because multiple wireless clients contend for access to the same channel and send data using the same channel, an extension to the basic IEEE 802.1X protocol is required to allow a wireless AP to identify the secured traffic of a particular wireless client. The wireless client and wireless AP do this through the mutual determination of a per-client unicast session key. Only authenticated wireless clients have knowledge of their per-client unicast session key. Without a valid unicast session key tied to a successful authentication, a wireless AP silently discards the traffic sent from the wireless client.

To provide a standard authentication mechanism for IEEE 802.1X, the IEEE chose the Extensible Authentication Protocol (EAP). EAP is a Point-to-Point Protocol (PPP)-based authentication mechanism that was adapted for use on point-to-point LAN segments. EAP messages are normally sent as the payload of PPP frames. To adapt EAP messages to be sent over Ethernet or wireless LAN segments, the IEEE 802.1X standard defines EAP over LAN (EAPOL), a standard encapsulation method for EAP messages.

EAP Overview

EAP was originally created as an extension to PPP that allows for development of arbitrary network access authentication methods. With typical PPP authentication protocols, a specific authentication mechanism is chosen during the link establishment phase. During the connection authentication phase, the negotiated authentication protocol is used to validate the connection. The authentication protocol itself is a fixed series of messages sent in a specific order. With EAP, the specific authentication mechanism is not chosen during the link establishment phase of the PPP connection. Instead, each PPP peer negotiates to perform EAP during the connection authentication phase. When the connection authentication phase is reached, the peers negotiate the use of a specific EAP authentication scheme known as an EAP type. EAP is described in RFC 2284.

After the EAP type is agreed upon, EAP allows for an open-ended exchange of messages between the access client and the authenticating server (the RADIUS server) that can vary based on the parameters of the connection. The conversation consists of requests for authentication information and the responses. The length and detail of the authentication conversation is dependent upon the EAP type.

Architecturally, EAP is designed to allow authentication plug-in modules at both the access client and authenticating server ends of a connection. To add support for a new EAP type, install an EAP type library file on both the access client and the authenticating server. This presents vendors with the opportunity to supply a new authentication scheme at any time. EAP provides the highest flexibility to allow for more secure authentication methods.

You can use EAP to support authentication schemes such as Generic Token Card, One Time Password (OTP), MD5-Challenge, Transport Layer Security (TLS) for smart card and certificate support, as well as any future authentication technologies. EAP is a critical technology component for secure connections.

In addition to support within PPP, EAP is also supported within the IEEE 802 link layer. IEEE 802.1X defines how EAP is used for authentication by IEEE 802 devices, including IEEE

802.11b wireless APs and Ethernet switches. IEEE 802.1X differs from PPP in that only EAP authentication methods are supported.

For secure wireless connections, Windows-based wireless clients support EAP-Transport Layer Security (EAP-TLS) and Protected EAP (PEAP)-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2). For more information, see "EAP-TLS Authentication" and "PEAP-MS-CHAP v2 Authentication" in this article.

EAP Over RADIUS

EAP over RADIUS is not an EAP type, but the passing of EAP messages of any EAP type by the access server to a RADIUS server for authentication. An EAP message sent between the access client and access server is formatted as the EAP-Message RADIUS attribute (RFC 2869, section 5.13), and sent in a RADIUS message between the access server and the RADIUS server. The access server becomes a pass-through device passing EAP messages between the access client and the RADIUS server. Processing of EAP messages occurs at the access client and the RADIUS server, not at the access server, as shown in Figure 7.

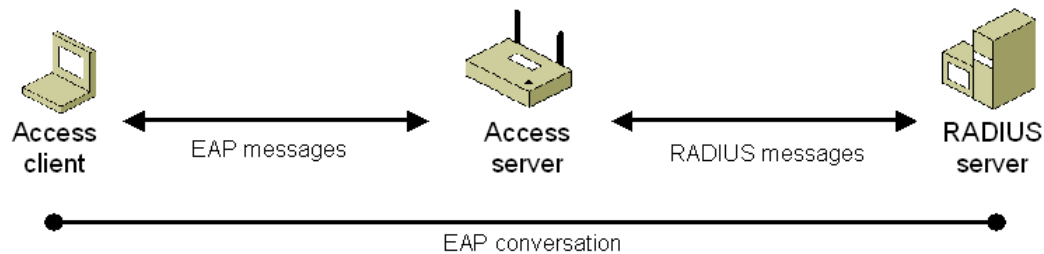


Figure 7 EAP over RADIUS

EAP over RADIUS is used in environments where RADIUS is used as the authentication provider. An advantage of using EAP over RADIUS is that EAP types do not need to be installed at each access server, only at the RADIUS server. However, the access server must support the negotiation of EAP as an authentication protocol and the passing of EAP messages to a RADIUS server.

In a typical use of EAP over RADIUS, the access server is configured to use EAP and to use RADIUS as its authentication provider. When a connection attempt is made, the access client negotiates the use of EAP with the access server. When the client sends an EAP message to the access server, the access server encapsulates the EAP message as the EAP-Message attribute of a RADIUS Access-Request message and sends it to its configured RADIUS server. The RADIUS server processes the EAP message in the EAP-Message attribute and sends an EAP response message as a RADIUS Access-Challenge message with the EAP-Message attribute to the access server. The access server then forwards the EAP message to the access client.

EAP-TLS Authentication

EAP-Transport Layer Security (EAP-TLS) is an EAP type that is used in certificate-based security environments. If you are using smart cards for remote access authentication, you must use the EAP-TLS authentication method. The EAP-TLS exchange of messages provides mutual authentication, integrity-protected cipher suite negotiation, and secured private key exchange and determination between the access client and the authenticating server. EAP-TLS provides the strongest authentication method. EAP-TLS is described in RFC 2716.

EAP-TLS using registry-based user and computer certificates is the preferred authentication method for Windows-based wireless connectivity for the following reasons:

- EAP-TLS does not require any dependencies on the user account's password.
- EAP-TLS authentication occurs automatically, usually with no intervention by the user.
- EAP-TLS uses certificates, which is a relatively strong authentication scheme.
- The EAP-TLS exchange is protected with public key cryptography and is not susceptible to offline dictionary attacks.
- The EAP-TLS authentication process results in mutually determined keying material for data encryption and signing.

Note EAP-TLS authentication with smart cards is not supported for wireless connections in Windows XP with no service packs installed.

IEEE 802.1X Authentication Process for EAP-TLS

The following is the EAP-TLS authentication process for a wireless client authenticating to a wireless AP configured to use a RADIUS server as its authentication server:

1. Association and request for identity

If the wireless AP observes a new wireless client associating with it, the wireless AP transmits an EAP-Request/Identity message to the wireless client. Alternately, when a wireless client associates with a new wireless AP, it transmits an EAP-Start message. If the IEEE 802.1X process on the wireless AP receives an EAP-Start message from a wireless client, it transmits an EAP-Request/Identity message to the wireless client.
2. EAP-Response/Identity response

If there is no user logged on to the wireless client, it transmits an EAP-Response/Identity message containing the computer name. For Windows-based wireless clients, the FQDN of the computer account is sent. If there is a user logged on to the wireless client, it transmits an EAP-Response/Identity message containing the user name. For Windows-based wireless clients, the UPN of the user account is sent.

The wireless AP forwards the EAP-Response/Identity message to the RADIUS server in the form of a RADIUS Access-Request message.
3. EAP-Request from the RADIUS server (Start TLS)

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-TLS, requesting a start to the TLS authentication process.

The wireless AP forwards the EAP message to the wireless client.
4. EAP-Response from the wireless client (TLS Client Hello)

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS, indicating the TLS client hello.

The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.
5. EAP Request from the RADIUS server (RADIUS server's certificate)

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-TLS, and includes the RADIUS server's certificate chain.

The wireless AP forwards the EAP message to the wireless client.
6. EAP-Response from the wireless client (wireless client's certificate)

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS, and includes the wireless client's certificate chain.

- The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.
7. EAP-Request from the RADIUS server (Cipher suite, TLS complete)

The RADIUS server sends an EAP-Request message with the EAP-Type set to EAP-TLS, and includes the cipher suite and an indication that TLS authentication message exchanges are complete.

The wireless AP forwards the EAP message to the wireless client.
 8. EAP-Response from the wireless client

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-TLS. The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.
 9. EAP-Success from the RADIUS server

The RADIUS server derives the per-client unicast session key and the signing key from the keying material that is a result of the EAP-TLS authentication process. Next, the RADIUS server sends a RADIUS Access-Accept message containing an EAP-Success message and the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes to the wireless AP.

The wireless AP uses the key encrypted in the MS-MPPE-Send-Key attribute as the per-client unicast session key for data transmissions to the wireless client (truncated to the appropriate WEP key length). The wireless AP uses the key encrypted in the MS-MPPE-Recv-Key attribute as a signing key for data transmissions to the wireless client that require signing (truncated to the appropriate WEP key length).

The wireless client derives the per-client unicast session key (the same value as the decrypted MS-MPPE-Send-Key attribute in the RADIUS message sent to the wireless AP) and the signing key (the same as value as the decrypted MS-MPPE-Recv-Key attribute in the RADIUS message sent to the wireless AP) from the keying material that is a result of the EAP-TLS authentication process. Therefore, both the wireless AP and the wireless client are using the same keys for both the encryption and signing of unicast data.

The wireless AP forwards the EAP-Success message to the wireless client. The EAP-Success message does not contain the per-station unicast session or signing keys.
 10. Multicast/global encryption key to the wireless client

The wireless AP derives the multicast/global encryption key by generating a random number or by selecting it from a previously set value. Next, the wireless AP sends an EAPOL-Key message to the wireless client containing the multicast/global key that is encrypted using the per-client unicast session key.

The Key field of the IEEE 802.1X EAPOL-Key message is RC4-encrypted using the per-client unicast session key and portions of the message are signed with Hashed Message Authentication Code-Message Digest 5 (HMAC-MD5) using the per-client unicast signing key.

Upon receiving the EAPOL-Key message, the wireless client uses the per-client unicast session key to verify the signed portions of the EAPOL-Key message and decrypt the multicast/global key. Next, the wireless LAN network adapter driver indicates the per-client unicast session key, the per-client unicast signing key, and the multicast/global key to the wireless LAN network adapter. After the keys have been indicated, the wireless client begins protocol configuration using the wireless adapter (such as using DHCP to obtain an IP address configuration).

When the wireless AP changes the multicast/global key, it generates and sends EAPOL-Key messages to its connected wireless clients. Each EAPOL-Key message contains the new

multicast/global key encrypted with the particular wireless client's per-client unicast session key.

Figure 8 summarizes this process.

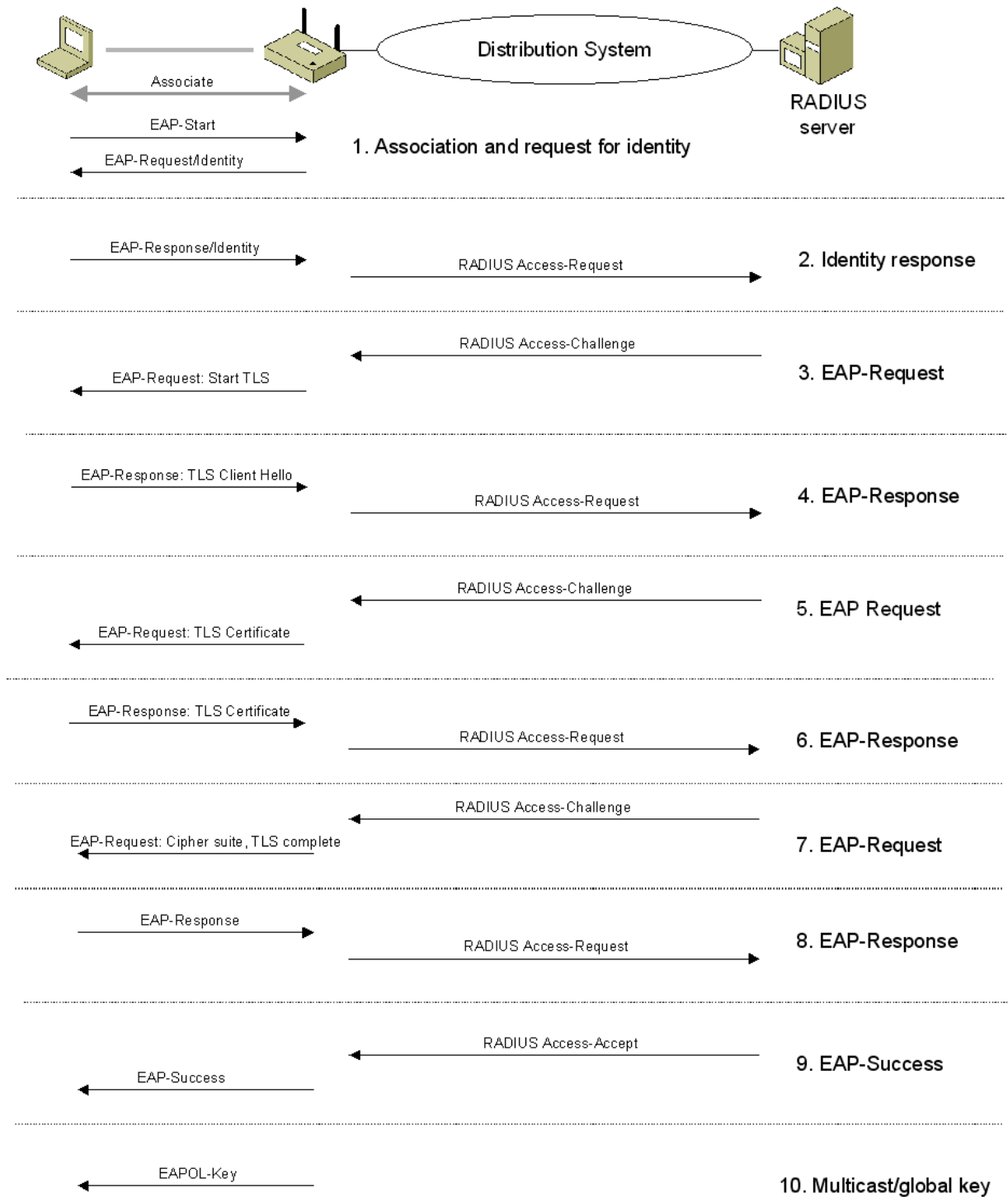


Figure 8 EAP-TLS and the IEEE 802.1X authentication process

PEAP-MS-CHAP v2 Authentication

Although EAP provides authentication flexibility through the use of EAP types, the entire EAP conversation might be sent as clear text (unencrypted). A malicious user with access to the media can inject packets into the conversation or capture the EAP messages from a successful authentication for analysis. This is especially problematic for wireless connections, in which the malicious user can be located outside of your business. EAP occurs during the IEEE 802.1X authentication process, before wireless frames are encrypted with WEP.

Protected EAP (PEAP) is an EAP type that addresses this security issue by first creating a secure channel that is both encrypted and integrity-protected with TLS. Then, a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication in wireless environments.

MS-CHAP v2 Overview

MS-CHAP v2 is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS-CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections.

Although MS-CHAP v2 provides better protection than previous PPP-based challenge-response authentication protocols, it is still susceptible to an offline dictionary attack. A malicious user can capture a successful MS-CHAP v2 exchange and methodically guess passwords until determining the correct one. By converting the MS-CHAP v2 authentication protocol to an EAP type and using it in combination with PEAP, the strong security of the TLS channel protects the MS-CHAP v2 exchange.

PEAP with MS-CHAP v2 Operation

The PEAP authentication process occurs in two parts. The first part is the use of EAP and the PEAP EAP type to create an encrypted TLS channel. The second part is the use of EAP and a different EAP type to authenticate network access. This section examines PEAP with MS-CHAP v2 operation, using as an example, a wireless client that attempts to authenticate to a wireless AP that uses a RADIUS server for authentication and authorization.

The following steps are used to create the PEAP TLS channel:

1. Association and request for identity

If the wireless AP observes a new wireless client associating with it, the wireless AP transmits an EAP-Request/Identity message to the wireless client. Alternately, when a wireless client associates with a new wireless AP, it transmits an EAP-Start message. If the IEEE 802.1X process on the wireless AP receives an EAP-Start message from a wireless client, it transmits an EAP-Request/Identity message to the wireless client.

2. EAP-Response/Identity from the wireless client

The wireless client transmits an EAP-Response/Identity message containing the computer or the user name.

The wireless AP forwards the EAP-Response/Identity message to the RADIUS server in the form of a RADIUS Access-Request message.

3. EAP-Request from the RADIUS server (Start PEAP)
The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to PEAP, requesting a start to the PEAP authentication process. The wireless AP forwards the EAP message to the wireless client.
 4. EAP-Response from the wireless client (TLS Client Hello)
The wireless client sends an EAP-Response message with the EAP-Type set to PEAP, indicating the TLS client hello.
The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.
 5. EAP Request from the RADIUS server (RADIUS server's certificate)
The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to PEAP, and includes the RADIUS server's certificate chain. The wireless AP forwards the EAP message to the wireless client.
 6. EAP-Response from the wireless client (Cipher suite, TLS complete)
The wireless client sends an EAP-Response message with the EAP-Type set to PEAP, and includes the cipher suite and an indication that TLS authentication message exchanges are complete.
The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.
 7. EAP-Request from the RADIUS server (Cipher suite, TLS complete)
The RADIUS server sends an EAP-Request message with the EAP-Type set to PEAP, and includes the cipher suite and an indication that TLS authentication message exchanges are complete.
The wireless AP forwards the EAP message to the wireless client.
- Figure 9 shows the authentication process that creates the encrypted PEAP channel.

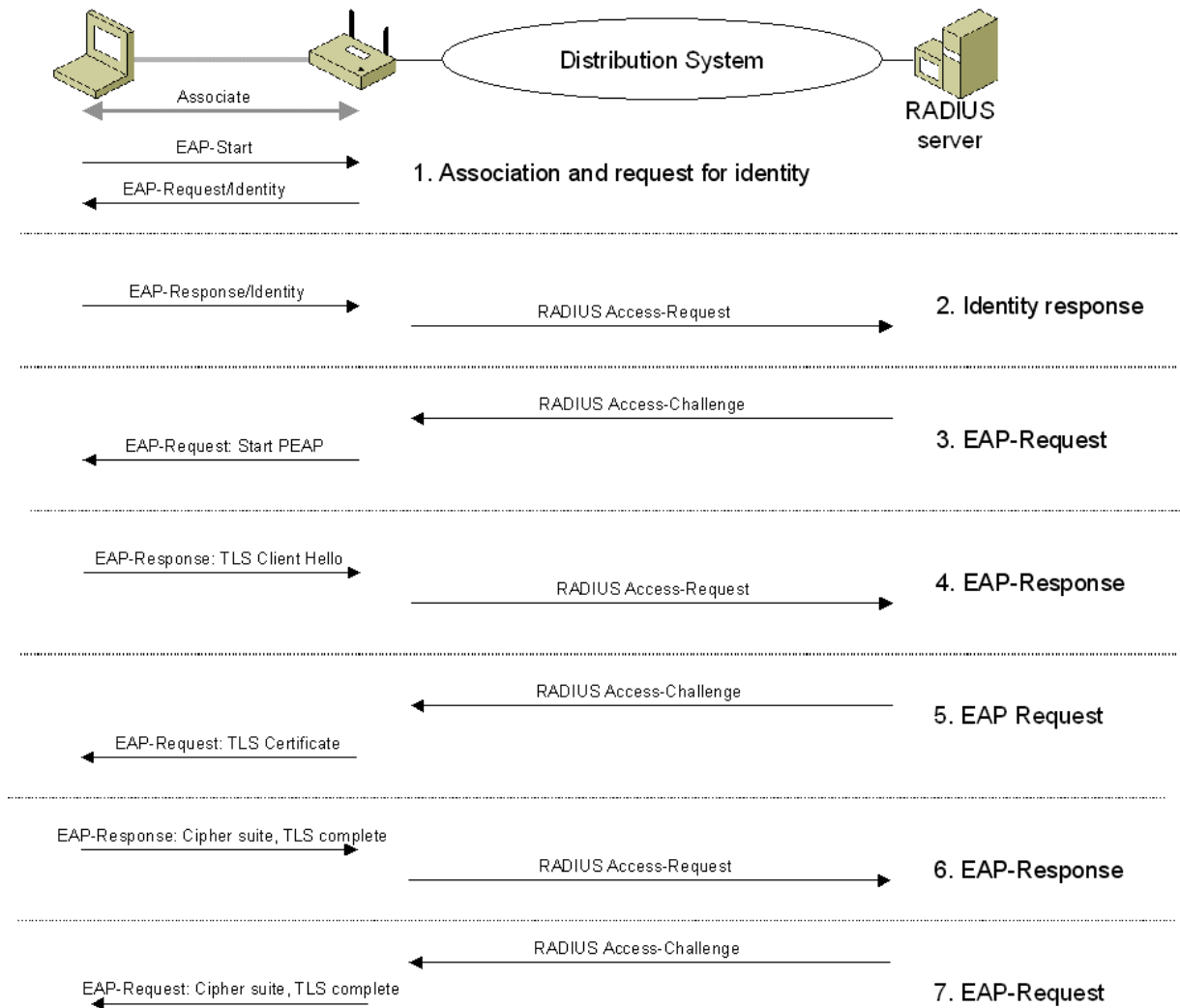


Figure 9 Authentication process for the PEAP channel

At the end of the PEAP negotiation, the RADIUS server has authenticated itself to the wireless client. Both nodes have determined mutual encryption and signing keys for the TLS channel, using public key cryptography, not passwords.

After the PEAP TLS channel is created, the following steps are used to authenticate the wireless client credentials with MS-CHAP v2:

- 1. EAP-Request/Identity from the RADIUS server**
The RADIUS server sends an EAP-Request message for the identity of the wireless client in the form of a RADIUS Access-Challenge message.
The wireless AP forwards the EAP message to the wireless client.
- 2. EAP-Response/Identity from the wireless client**
The wireless client transmits an EAP-Response/Identity message containing the computer or the user name.
The wireless AP forwards the EAP-Response/Identity message to the RADIUS server in the form of a RADIUS Access-Request message.
- 3. EAP-Request from the RADIUS server (MS-CHAP v2 challenge)**

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-MS-CHAP v2, containing the MS-CHAP v2 challenge for the wireless client.

The wireless AP forwards the EAP message to the wireless client.

4. EAP-Response from the wireless client (MS-CHAP v2 response and challenge)

The wireless client sends an EAP-Response message with a response to the RADIUS server's challenge and a challenge for the RADIUS server.

The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.

5. EAP Request from the RADIUS server (MS-CHAP v2 response and success)

The RADIUS server sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP-Type set to EAP-MS-CHAP v2, containing a response to the wireless client's challenge and an indication of the success of the wireless client's response to the RADIUS server's challenge.

The wireless AP forwards the EAP message to the wireless client.

6. EAP-Response from the wireless client (MS-CHAP v2 acknowledgement)

The wireless client sends an EAP-Response message with the EAP-Type set to EAP-MS-CHAP v2, containing the MS-CHAP v2 Acknowledgement message, indicating that the RADIUS server's response to the wireless client's challenge is correct.

The wireless AP forwards the EAP message to the RADIUS server in the form of a RADIUS Access-Request message.

7. EAP-Success from the RADIUS server

The RADIUS server derives the per-client unicast session key and the signing key from the keying material that is a result of the PEAP authentication process. Next, the RADIUS server sends a RADIUS Access-Accept message containing an EAP-Success message and the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes to the wireless AP.

The wireless AP uses the key encrypted in the MS-MPPE-Send-Key attribute as the per-client unicast session key for data transmissions to the wireless client (truncated to the appropriate WEP key length). The wireless AP uses the key encrypted in the MS-MPPE-Recv-Key attribute as a signing key for data transmissions to the wireless client that require signing (truncated to the appropriate WEP key length).

The wireless client derives the per-client unicast session key (the same value as the decrypted MS-MPPE-Send-Key attribute in the RADIUS message sent to the wireless AP) and the signing key (the same as value as the decrypted MS-MPPE-Recv-Key attribute in the RADIUS message sent to the wireless AP) from the keying material that is a result of the PEAP authentication process. Therefore, both the wireless AP and the wireless client are using the same keys for both the encryption and signing of unicast data.

The wireless AP forwards the EAP-Success message to the wireless client. The EAP-Success message does not contain the per-station unicast session or signing keys.

8. Multicast/global encryption key to the wireless client

The wireless AP derives the multicast/global encryption key by generating a random number or by selecting it from a previously set value. Next, the wireless AP sends an EAPOL-Key message to the wireless client containing the multicast/global key that is encrypted using the per-client unicast session key.

The Key field of the IEEE 802.1X EAPOL-Key message is RC4-encrypted using the per-client unicast session key and portions of the message are signed with HMAC-MD5 using the per-client unicast signing key.

Upon receiving the EAPOL-Key message, the wireless client uses the per-client unicast session key to verify the signed portions of the EAPOL-Key message and decrypt the multicast/global key. Next, the wireless LAN network adapter driver indicates the per-client unicast session key, the per-client unicast signing key, and the multicast/global key to the wireless LAN network adapter. After the keys have been indicated, the wireless client begins protocol configuration using the wireless adapter (such as using DHCP to obtain an IP address configuration).

When the wireless AP changes the multicast/global key, it generates and sends EAPOL-Key messages to its connected wireless clients. Each EAPOL-Key message contains the new multicast/global key encrypted with the particular wireless client's per-client unicast session key.

Figure 10 shows the MS-CHAP v2 authentication process that occurs within the encrypted PEAP channel.

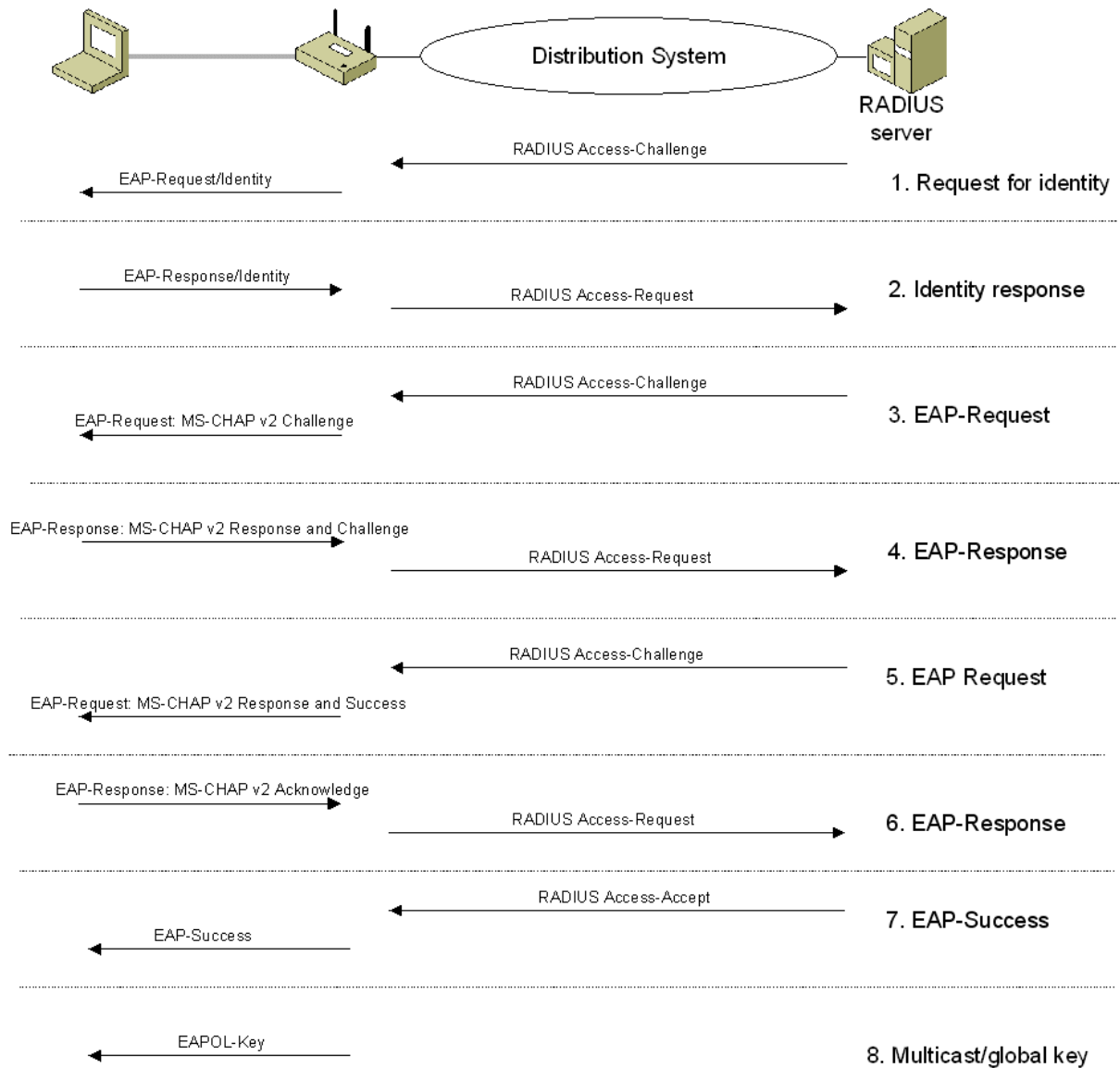


Figure 10 MS-CHAP v2 authentication process within the PEAP channel

At the end of this mutual authentication exchange, the wireless client has provided proof of knowledge of the correct password (the response to the RADIUS server challenge string), and the RADIUS server has provided proof of knowledge of the correct password (the response to the wireless client challenge string). The entire exchange is encrypted through the TLS channel created in the first part of the PEAP authentication.

If PEAP-TLS is used, a TLS authentication process occurs in the same way as EAP-TLS, except that the EAP messages are encrypted using the TLS channel.

PEAP Fast Reconnect

You can also use PEAP to quickly resume a TLS session. If PEAP Part 2 is successful, the RADIUS server can cache the TLS session created during PEAP Part 1. Because the cache entry was created through a successful PEAP Part 2 authentication process, the session can be resumed without having to go through a complete authentication again. In this case, an EAP-Success message is sent almost immediately for a reauthentication attempt. This is known as fast reconnect. Fast reconnect minimizes

the connection delay in wireless environments when a wireless client roams from one wireless AP to another.

Fast reconnect is an optional feature of PEAP. If you intend to use it, fast reconnect must be enabled on both the wireless client and the RADIUS server. Fast reconnect is supported for wireless clients running Windows XP with Service Pack 1 (SP1), Windows XP with Service Pack 2 (SP2), Windows Server® 2003, Windows Vista™ (now in beta testing), Windows Server Code Name "Longhorn" (now in beta testing), and Windows 2000 Service Pack 4 (SP4). IAS for Windows Server 2003 also supports fast reconnect. In all cases, fast reconnect is disabled by default. IAS for Windows 2000 Server SP4 does not support fast reconnect.

802.1X and 802.11 Security Issues

The current solutions provided by the use of 802.1X for the security issues that exist with 802.11 are the following:

- **Rogue wireless APs** The best solution for rogue wireless APs is to support a mutual authentication protocol such as EAP-TLS or PEAP-MS-CHAP v2. With EAP-TLS or PEAP-MS-CHAP v2, the wireless client ensures that the wireless AP is a trusted member of the secure wireless authentication infrastructure by validating the RADIUS server's certificate.
- **No per-user identification and authentication** The adaptation of IEEE 802.1X for wireless connections and its use of EAP enforce a user-level authentication before allowing wireless frames to be forwarded.
- **No mechanism for central authentication, authorization, and accounting** By using RADIUS in conjunction with IEEE 802.1X, RADIUS servers provide centralized authentication, authorization, and accounting services for wireless connections.
- **Some implementations derive WEP keys from passwords, resulting in weak WEP keys** By using IEEE 802.1X and EAP-TLS as the authentication method, public key certificates, not passwords, are used to perform authentication and derive encryption key material. By using IEEE 802.1X and PEAP-MS-CHAP v2, passwords are used to derive encryption keys; however, the password credential exchange is encrypted within a TLS channel.
- **No support for extended authentication methods (for example, token cards, certificates/smart cards, one-time passwords, biometrics; and so on)** IEEE 802.1X uses EAP as its authentication protocol. EAP was designed to be extensible for virtually any type of authentication method.
- **No support for key management (for example, rekeying global keys and dynamic per-session or per-session key management)** By using IEEE 802.1X and either the EAP-TLS or PEAP-MS-CHAP v2 authentication methods, random unicast session keys are derived for each authentication. Rekeying can be done either by the wireless client; by reauthenticating; or by the wireless AP, which changes encryption keys and sends the new keys to wireless clients using EAPOL messages.

Wi-Fi Protected Access (WPA)

Although 802.1X addresses many of the security issues of the original 802.11 standard, issues still exist with regard to weaknesses in the WEP encryption and data integrity methods. The solution to these problems is the IEEE 802.11i standard, a new standard that specifies improvements to wireless LAN networking security.

While the new IEEE 802.11i standard was being ratified, wireless vendors agreed on an interoperable interim standard known as Wi-Fi Protected Access (WPA™). The goals of WPA are the following:

- **To require secure wireless networking** WPA requires secure wireless networking by requiring 802.1X authentication, encryption, and unicast and global encryption key management.
- **To address the issues with WEP through a software upgrade** The implementation of the RC4 stream cipher within WEP is vulnerable to known plaintext attacks. Additionally, the data integrity provided with WEP is relatively weak. WPA solves all the remaining security issues with WEP, yet only requires firmware updates in wireless equipment and an update for wireless clients. Existing wireless equipment is not expected to require replacement.
- **To provide a secure wireless networking solution for SOHO wireless users** For the SOHO, there is no RADIUS server to provide 802.1X authentication with an EAP type. SOHO wireless clients must use either shared key authentication (highly discouraged) or open system authentication (recommended) with a single static WEP key for both unicast and multicast traffic. WPA provides a pre-shared key option intended for SOHO configurations. The pre-shared key is configured on the wireless AP and each wireless client. The unique initial unicast encryption key is derived from the authentication process, which verifies that both the wireless client and the wireless AP have the pre-shared key.
- **To be forward-compatible with the IEEE 802.11i standard** WPA is a subset of the security features in the IEEE 802.11i standard.
- **To be available today** WPA upgrades to wireless equipment and for wireless clients were available beginning in February of 2003.

WPA Security Features

WPA contains enhancements or replacements for the following security features:

- Authentication
- Encryption
- Data integrity

Authentication

With 802.11, 802.1X authentication is optional; with WPA, 802.1X authentication is required. Authentication with WPA is a combination of open system and 802.1X authentication, which uses the following phases:

- The first phase uses open system authentication to indicate to the wireless client that it can send frames to the wireless AP.
- The second phase uses 802.1X to perform a user-level authentication.

WPA supports two modes of operation. WPA Enterprise is for environments with a RADIUS infrastructure and uses an EAP authentication method. WPA Personal is for environments without a RADIUS infrastructure and uses a pre-shared key for authentication.

Encryption

With 802.1X, rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1X provide no mechanism to change the global encryption key that is used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. The Temporal Key Integrity Protocol (TKIP) changes the unicast encryption key for every frame, and each change is synchronized between the wireless client and the wireless AP. For the multicast/global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients.

WPA supports the following encryption methods:

- **TKIP** For 802.11, WEP encryption is optional. For WPA, encryption using TKIP is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, yet can be performed using the calculation facilities present on existing wireless hardware. TKIP also provides for:
 - The verification of the security configuration after the initial encryption keys are determined.
 - The synchronized changing of the unicast encryption key for each frame.
 - The determination of a unique starting unicast encryption key for each pre-shared key authentication.
- **AES** WPA defines the use of the Advanced Encryption Standard (AES) as an optional replacement for WEP encryption. Because adding AES support through a firmware update might not be possible for existing wireless equipment, support for AES on wireless network adapters and wireless APs is not required.

Data Integrity

With 802.11 and WEP, data integrity is provided by a 32-bit ICV that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, it is possible through cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a new method known as Michael specifies a new algorithm that calculates an 8-byte message integrity code (MIC) with the calculation facilities available on existing wireless hardware. The MIC is placed between the data portion of the 802.11 frame and the 4-byte ICV. The MIC field is encrypted along with the frame data and the ICV.

Michael also provides replay protection through the use of a new frame counter field in the 802.11 MAC header.

For additional details about the WPA encryption and data integrity process, see [Wi-Fi Protected Access Data Encryption and Integrity](#).

Required Software Changes for WPA Support

WPA requires software changes to the following:

- Wireless APs
- Wireless network adapters
- Wireless client software

Wireless Access Points

Wireless APs must have their firmware updated to support the following:

- New WPA information element
Information elements are included in the 802.11 beacon frames to advertise the wireless APs capabilities, such as supported bit rates and security options. To advertise their capability to perform WPA, wireless APs send beacon frames with a new 802.11 WPA information element that contains the wireless AP's WPA capabilities.
- WPA two-phase authentication: Open system followed by 802.1X (EAP with RADIUS or WPA pre-shared key)
- TKIP
- Michael
- AES (optional)

To upgrade your wireless APs to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless APs.

Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

- New WPA information element
Wireless clients must be able to process the WPA information element in beacon frames and respond with a specific security configuration.
- WPA two-phase authentication: Open system followed by 802.1X (EAP or WPA pre-shared key)
- TKIP
- Michael
- AES (optional)

To upgrade your wireless network adapters to support WPA, you might have to upload a WPA firmware update to your wireless network adapter.

For Windows-based wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP with SP1, Windows XP with SP2, or Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to Windows XP Wireless Auto Configuration, which is enabled by the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update within the updated wireless adapter driver. Because of this, updating your Windows wireless client consists of simply obtaining the new WPA-compatible driver and installing it. The firmware is automatically updated when the wireless network adapter driver is loaded into Windows.

Wireless Clients

Wireless client software must be updated to allow for the configuration of WPA authentication (including pre-shared key) and the new WPA encryption algorithms (TKIP and AES).

You must obtain and install a new WPA-compliant configuration tool from your wireless network adapter vendor for wireless clients running the following:

- Windows 2000
- Windows XP with SP1, Windows XP with SP2, or Windows Server 2003, and using a wireless network adapter that does not support Wireless Auto Configuration

Windows XP SP2, Windows Server 2003 SP1, Windows Vista, and Windows Server "Longhorn" include WPA support.

For wireless clients running Windows XP with SP1 or Windows Server 2003 with no service packs installed that are using a wireless network adapter that supports Wireless Auto Configuration, you must install the [Update for Microsoft Windows XP: KB826942](#)—a free download from Microsoft—which enhances the wireless network configuration dialog boxes to support new WPA options.

For additional information about how to configure WPA encryption and authentication options for a Windows wireless client, see [IEEE 802.11 Wireless Deployment Technology and Component Overview](#).

Supporting a Mixed Environment

To support the gradual transition of a WEP-based wireless network to WPA, it is possible for a wireless AP to support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients are using WEP and which are using WPA. The disadvantage of supporting a mixture of WEP and WPA clients is that the multicast/global encryption key is not dynamic. All other security enhancements for WPA clients are preserved.

Wi-Fi Protected Access 2

The IEEE 802.11i standard formally replaces WEP and the other security features of the original IEEE 802.11 standard. Wi-Fi Protected Access 2 (WPA2™) is a product certification available through the Wi-Fi Alliance that certifies wireless equipment as being compatible with the IEEE 802.11i standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA, such as AES encryption of wireless frames.

WPA2 is supported by the following versions of Windows:

- Windows XP with SP2 with the [Wi-Fi Protected Access 2 \(WPA2\)/Wireless Provisioning Services Information Element \(WPS IE\) Update for Windows XP with Service Pack 2](#), a free download from Microsoft
- Windows Vista
- Windows Server "Longhorn"

For more information about WPA2 security features, fast roaming, and hardware and software requirements for WPA2-based wireless connectivity, see [Wi-Fi Protected Access 2 \(WPA2\) Overview](#).

For information about the details of WPA2 data encryption and integrity, see [Wi-Fi Protected Access 2 Data Encryption and Integrity](#).

Recommended Security Configurations

The following are the recommended combinations of encryption and authentication for secure wireless networking in an organization, from the most to the least secure:

- WPA2/AES and EAP-TLS
- WPA2/AES and PEAP-MS-CHAP v2
- WPA/TKIP and EAP-TLS
- WPA/TKIP and PEAP-MS-CHAP v2

The following combinations of security technologies (in order of most to least secure) are discouraged from use except if used as a temporary configuration when transitioning to a WPA2 or WPA-based security configuration:

- WEP and EAP-TLS
- WEP and PEAP-MS-CHAP v2

For more information about deploying these security configurations for an organization intranet, see [Deployment of Secure 802.11 Networks Using Microsoft Windows](#).

For the SOHO wireless network without a RADIUS server, the following combinations of encryption and authentication are recommended, from the most to the least secure:

- WPA2/AES and WPA2 with pre-shared key authentication
- WPA/TKIP and WPA with pre-shared key authentication

The use of WEP with a static WEP key and open system authentication is not recommended.

For more information about deploying these security configurations for a small business or home, see [Step-by-Step Guide for Secure Wireless Deployment for Small Office/Home Office or Small Organization Networks](#) and [Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business](#).

Attacks on Wireless Networks

Wireless networks are vulnerable to various types of attacks. The following describes the different types of attacks and how to mitigate them:

- **Association attack** Occurs when an attacker attempts to use up all the available ports on a wireless AP. When all the ports are used up, the wireless AP denies association requests from legitimate wireless clients, which is a denial of service (DoS) attack on a wireless AP. Because the attacking wireless node must first authenticate, SOHO wireless networks with open system authentication are the most vulnerable to association attacks. The best defense against association attacks is to either deploy your wireless APs so that the coverage areas do not extend outside buildings, or configure your wireless APs to quickly abandon associations that have not been authenticated.
- **WEP key determination attack** Occurs when an attacker captures encrypted text or the shared key authentication exchange and uses cryptanalysis to determine the WEP encryption key. The best way to mitigate WEP key determination attacks is to use 802.1X and either EAP-TLS or PEAP-MS-CHAP v2 for per-authentication unicast encryption keys. Change the encryption key periodically from the client by reauthenticating, or (from the wireless AP side) by configuring the wireless AP to change the encryption key. Alternately, upgrade your wireless network components to use WPA or WPA2.
- **WEP bit flipping attack** Occurs when an attacker intercepts a wireless frame, changes bits in the frame, updates the encrypted ICV in the frame, and sends it as the original wireless node. This attack is possible with WEP encryption. To prevent WEP bit flipping attacks, upgrade your wireless network to use WPA or WPA2.

Summary

This article describes the requirements for security on wireless networks in terms of authentication, data confidentiality (encryption), and data integrity. The original 802.11 standard defined two types of authentication (open system and shared key) and WEP, which provides encryption and data integrity. The security methods used by the original 802.11 standard proved to be relatively weak and did not scale for large wireless networks. The 802.1X standard was adapted for 802.11 wireless networks to provide much stronger authentication and automated encryption key management. WPA, a software upgrade for wireless equipment, is an interim standard that uses TKIP for encryption and Michael for data integrity. WPA2, a product certification for the security features of the IEEE 802.11i standard, includes mandatory use of AES for encryption and data integrity. Using WPA or WPA2 can mitigate the most common attacks against wireless networks.

Related Links

See the following resources for further information:

- [Microsoft Wireless Networking Web site](http://www.microsoft.com/wifi) at <http://www.microsoft.com/wifi>
- [IEEE 802.11 Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.msp) at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.msp>
- [Deployment of Secure 802.11 Networks Using Microsoft Windows](http://www.microsoft.com/technet/prodtechnol/winxpro/deploy/ed80211.msp) at <http://www.microsoft.com/technet/prodtechnol/winxpro/deploy/ed80211.msp>
- [Step-by-Step Guide for Secure Wireless Deployment for Small Office/Home Office or Small Organization Networks](http://www.microsoft.com/downloads/details.aspx?familyid=269902e8-fc41-4eb1-9374-44612e64f0fb&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?familyid=269902e8-fc41-4eb1-9374-44612e64f0fb&displaylang=en>
- [Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wifisoho.msp) at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wifisoho.msp>

For the latest information about Windows Server System, see the [Windows Server System Web site](http://www.microsoft.com/windowsserversystem) at <http://www.microsoft.com/windowsserversystem>.



Windows Server System is comprehensive, integrated, and interoperable server infrastructure that simplifies the development, deployment, and management of flexible business solutions.
www.microsoft.com/windowsserversystem