

ProCurve Wireless LAN Security



Fundamentals Guide
Technical Training Version 8.21

ProCurve Wireless LAN Security Fundamentals

Introduction	1
Objectives	1
Discussion Topics.....	2
Authentication Options.....	3
802.11 Authentication.....	3
802.11 Association	4
Additional Requirements to Connect.....	4
Encryption Options.....	5
Shared Key.....	5
802.1X—Dynamic WEP and WPA/WPA2.....	6
Web-Auth	6
MAC-Auth.....	6
Discussion Topics.....	7
Local MAC-Auth.....	8
RADIUS MAC-Auth	9
Pros and Cons of MAC-Auth.....	10
Pros of MAC-Auth	10
Cons of MAC-Auth	11
Pros of RADIUS MAC-Auth.....	12
Discussion Topics.....	13
Static WEP—Using a WEP Key for Authentication.....	14
Encryption.....	14
Authentication.....	15
WEP Encryption	16
Keystream.....	16
XOR Operation.....	17
Vulnerabilities of WEP Encryption	18
WEP Integrity	20
Shared-Key WEP	21
Shared-Key Authentication Process	21
Roaming with Shared-Key WEP.....	22
Vulnerabilities of Shared-Key WEP	23
Open-Key WEP.....	25
Static WEP Pros and Cons	26
Pros of Static WEP	26
Cons of Static WEP	27
Shared-Key Versus Open-Key WEP	27
Discussion Topics.....	28

802.1X	29
802.1X Roles	30
Supplicant	30
Authenticator	31
Authentication Server	31
802.1X Ports	32
Controlled Port	32
Uncontrolled Port	32
Controlled Port States	33
EAP Process	34
Negotiating the EAP Method	36
EAP Methods: TLS	37
Benefits	37
EAP Methods: TTLS and PEAP	39
Step 1—Outer Method	39
Step 2—Inner Method	39
Benefits	40
EAP Methods: MD5 and GTC	41
EAP-MD5	41
EAP-GTC	42
Security Concerns	42
Summary of EAP Methods	43
Selecting an EAP Method	45
RADIUS Protocol	47
Complete 802.1X Process	49
802.1X Requirements	51
AP as an 802.1X Supplicant	53
802.1X Encryption Options	54
Dynamic WEP	55
Dynamic WEP Pros and Cons	57
Pros of Dynamic WEP	57
Cons of Dynamic WEP	57
WPA	59
WPA Requirements	59
TKIP	61
Securely Generated Master Keys	62
Key Rotation with Transient Keys	62
Key Mixing for Per-Frame Keys	62
TKIP Key Distribution: Four-way handshake for a pairwise key	63
Distributing Keys	63
Completing the Four-Way Handshake	64
TKIP Key Distribution: Two-way handshake for group key	65
TKIP Key Mixing	66
Phase 1	66
Phase 2	67
Michael	68

WPA2 (802.11i)	69
Strong Encryption	69
Encryption-Based Integrity	70
Authentication	70
CCMP/AES	71
CCMP/AES: Continued	72
AES Counter Mode Encryption	72
MIC for Data Integrity	73
WPA/WPA2 Uses and Requirements	74
Requirements for the Network	74
Requirements on the Station	74
Requirements on the AP	75
Using Multiple Encryption Standards	76
WPA/WPA2 Pros and Cons	77
Pros of WPA/WPA2	77
Cons of WPA/WPA2	77
Discussion Topics	79
WPA/WPA2-PSK	80
Failed WPA/WPA2-PSK Handshake	81
WPA/WPA2-PSK Pros and Cons	82
Pros of WPA/WPA2-PSK	82
Cons of WPA/WPA2-PSK	82
Discussion Topics	84
Web-Auth Uses	85
Web-Auth Pros and Cons	86
Pros of Web-Auth	86
Cons of Web-Auth	87
Discussion Topics	88
Comparing Security Options	89
Authentication	89
Encryption	89
Management	90
Requirements	90
Comparing Security Options: Continued	91
Authentication	91
Encryption	91
Management	92
Requirements	92
Comparing Security Options: Continued	93
Authentication	93
Encryption	93
Management	93
Requirements	94
Summary	95

ProCurve Wireless LAN Security Fundamentals

Introduction

Although wireless networks have become required equipment for most companies, they are not without their challenges. Perhaps the most critical issue is security. Because radio waves are shared media, anyone can eavesdrop on wireless transmissions or tamper with the data being transmitted.

To secure these transmissions, you cannot rely solely on authentication methods. In this guide, you will learn about the three interlocking aspects of wireless security:

- Authentication, which ensures that only authorized users access the network;
- Confidentiality, which hides data from other users of the shared wireless medium
- Integrity, which protects data from tampering

Objectives

After you have completed this guide, you should be able to:

- List the authentication options for wireless networks and identify their strengths and weaknesses
- Explain how MAC authentication (MAC-Auth) functions in a wireless network
- Explain how 802.1X functions in a wireless network, including describing common Extensible Authentication Protocol (EAP) methods
- Compare the encryption provided by Wired Equivalent Privacy (WEP) and by Wi-Fi Protected Access™ (WPA)
- Describe the advantages and disadvantages of using Web authentication (Web-Auth) to authenticate users in a wireless network

Discussion Topics

Discussion Topics



Overview

- Authentication methods
- Encryption options

MAC-Auth

WEP key as authentication (static WEP)

802.1X

WPA/WPA with preshared keys (WPA/WPA2-PSK)

Web-Auth

Comparing security options

Summary

This section outlines the authentication methods and encryption options available to protect wireless networks.

Authentication Options

Authentication Options



802.11 authentication	Open-system		Shared-key**
	MAC authentication*	None	WEP key
802.11 association			
Additional requirements to connect			
	None	Shared key (WEP or WPA)	Supplemental authentication
			802.1X Web-Auth*

Rev. 8.21

Pre-study Guide: 3

4

To connect to a wireless LAN (WLAN), a station must complete these steps:

1. 802.11 authentication
2. 802.11 association
3. Optional additional requirements to connect

The authentication options involved with each of these steps are listed below.

802.11 Authentication

802.11, the industry standard for wireless networks, defines two types of authentication:

- Open-system, which allows all users to associate to the AP
Typically, all users can associate, but there is one exception: MAC authentication (MAC-Auth) limits the WLAN to devices with allowed MAC addresses.
- Shared-key, which restricts access to users who know the correct WEP encryption key

Although shared-key authentication was designed to provide strong security, it failed to live up to this promise. WEP defines an encryption algorithm that is simply too easily cracked. In contemporary networks, open-system authentication is the preferred option, allowing all stations to pass to the next step.

802.11 Association

In this step, the station associates to the WLAN. If you were to use shared-key authentication, the station would be fully connected. However, most contemporary WLANs require stations and users to complete further authentication.

Additional Requirements to Connect

You have several options for enforcing more secure authentication on a WLAN. You can use a shared key, which functions like a password that users must input to connect to a WLAN. (The key can be either a WEP or a WPA key—as described in more detail later in this guide.) The shared key limits an open system in a practical sense: users cannot send or receive data without the correct key. For reasons explained later in this module, this option is more secure than shared-key WEP authentication. However, a shared key falls short of *true* authentication and is not suited for enterprise-level security in large networks.

These networks should enforce supplemental authentication to the network, specifically a RADIUS server. The most secure supplemental authentication is 802.1X. Web-Auth, another supplemental authentication, offers support for guests as well as not-up-to-standard stations.

Encryption Options

Encryption Options



Authentication Method	Encryption Option	Security Option	Recommendation
Shared key	WEP	Static WEP	WPA/WPA2-PSK for small companies
	TKIP or CCMP-AES	WPA/WPA2-PSK	
802.1X	WEP	Dynamic WEP	WPA/WPA2 with 802.1X preferred
	TKIP or CCMP-AES	WPA/WPA2 with 802.1X	
Web-Auth	None	Web-Auth	Typically used for guests; optional encryption secures wireless transmissions
	WEP	Web-Auth with static WEP	
	TKIP or CCMP-AES	Web-Auth with WPA/WPA2-PSK	
MAC-Auth	Does not provide encryption, but can be combined with other security options		Adds some security to methods such as WPA/WPA2-PSK

Not recommended Acceptable in some circumstances Most secure

Rev. 8.21

Pre-study Guide: 5

5

In an Ethernet network, requiring users to authenticate may be enough to secure the network. Wireless networks, however, typically require encryption as well. This guide covers the encryption offered by these protocols:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)—Encryption with Temporal Key Integrity Protocol (TKIP)
- WPA2—Encryption with Counter Mode CBC-MAC Protocol (CCMP) and Advanced Encryption Standard (AES)

Together the authentication method and the encryption option make up the security option.

Shared Key

Two security options use shared keys for authentication:

- Static WEP
- WPA/WPA2-PSK

Static WEP

Static WEP requires users to submit the correct shared key to connect to the WLAN. It uses the same shared key for encryption. Because the key can be cracked, this security option is not generally recommended.

WPA/WPA2-PSK

WPA/WPA2-preshared key (PSK) also requires users to submit the correct key before connecting to the WLAN. Unlike a WEP key, however, the WPA/WPA2 PSK is altered before it actually encrypts data, making this method far more secure. As a result, WPA/WPA2-PSK is preferred to static WEP, although the option is still best suited only for small companies.

802.1X—Dynamic WEP and WPA/WPA2

802.1X, the most secure authentication method, can be used with either WEP or WPA/WPA2 encryption. WEP with 802.1X is called dynamic WEP because the authentication server sends different keys to different users. WPA/WPA2, the far stronger encryption scheme, is preferred.

Web-Auth

By itself, Web-Auth does not require encryption to protect the wireless transmissions between the station and the AP or RP. However, the ProCurve Access Point (AP) 420, the AP 530, and the Wireless Module allow you to add either WEP or WPA/WPA2 encryption to Web-Auth. In this case, the user must input the encryption key as a shared key as with static WEP or WPA/WPA2-PSK.

MAC-Auth

MAC authentication (MAC-Auth) allows you to authenticate devices that do not support other security measures. For example, you may need to implement MAC-Auth for some wireless phones that do not support an 802.1X client. MAC-Auth can also be used in conjunction with other security measures to provide an additional check. However, MAC addresses can be easily spoofed, so this authentication method is ultimately not completely secure.

You can use MAC-auth in conjunction with other authentication methods. For example, you could implement MAC-Auth and WPA-PSK.

Discussion Topics

Discussion Topics



✓ *Overview*

MAC authentication (MAC-Auth)

- **Local MAC-Auth**
- **RADIUS MAC-Auth**
- **Pros and cons**

WEP key as authentication (static WEP)

802.1X

WPA/WPA with preshared keys (WPA/WPA2-PSK)

Web authentication (Web-Auth)

Comparing security options

Summary

Rev. 8.21

Pre-study Guide: 7

6

The next sections describe each of the security options for wireless networks in some detail, starting with MAC-Auth, one of the most basic security options available. MAC-Auth adds only minimal protection to 802.11's open-system authentication.

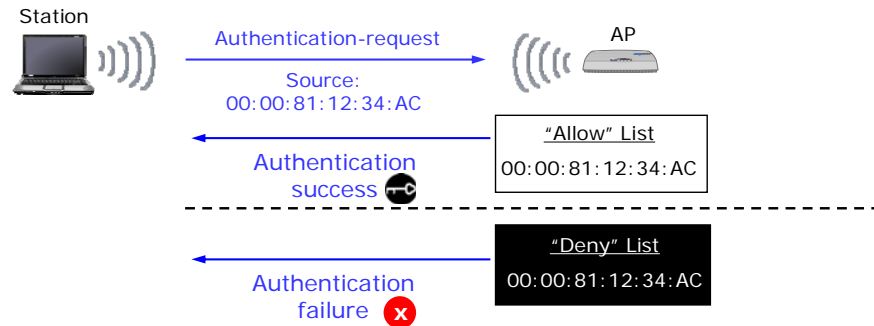
Local MAC-Auth

Local MAC-Auth



Provide control for stations with limited authentication capabilities.

1. All 802.11 authentication requests include the station's MAC address.
2. The AP checks this address against a MAC address list.
3. If the MAC address is allowed, the AP sends an authentication-success frame.



Rev. 8.21

Pre-study Guide: 8

7

Although the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification does not require MAC-Auth—and MAC-Auth is not as secure as other authentication options—many vendors support it because it is the only option for devices that do not have a user interface or support for 802.1X.

MAC-Auth fits within 802.11 open-system authentication. Typically, an AP accepts all authentication requests. With MAC-Auth, however, the AP filters requests according to the source MAC address in the request frame's header. Because all stations must include their MAC address in the request frame, all stations can be controlled through MAC authentication.

With local MAC-Auth, the AP maintains lists of MAC addresses and checks access requests against these lists. APs can store two types of lists:

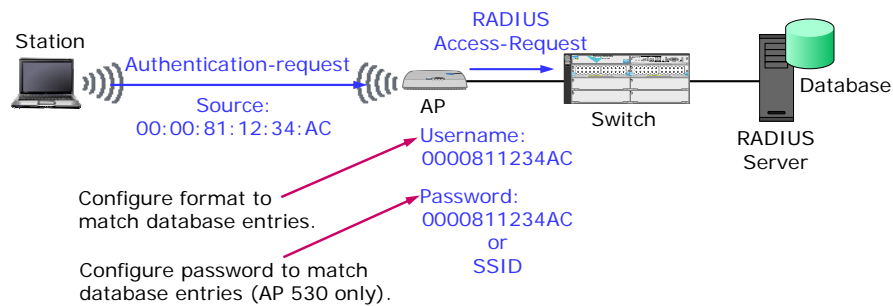
- Allow list—a list of addresses allowed to associate with the AP. This list might also be called a white list.
- Deny list—a list of addresses prohibited from associating with the AP. This list might also be called a block or black list.

RADIUS MAC-Auth

RADIUS MAC-Auth



- RADIUS MAC-Auth provides centralized control over stations with limited capabilities.
- APs relay stations' requests to a RADIUS server, translating them to RADIUS format.



Rev. 8.21

Pre-study Guide: 9

8

Instead of checking the MAC address itself, the AP can submit the station's request to a RADIUS server. In RADIUS terminology, the AP is a Network Access Server (NAS), and it must create a properly formatted NAS Access-Request packet:

1. The AP copies the source MAC address of the station's request into the packet's username field. The AP must use the format in which the address is stored on the RADIUS server. (For example, if the RADIUS server uses delimiters, the AP must use delimiters.)
2. The AP can place one of several values in the password field:
 - Typically, the AP copies the station's MAC address into this field using the same format that is used for the username.
 - Alternatively, the AP copies a different value, such as the Service Set Identifier (SSID) that the station is requesting to join. (Of the ProCurve wireless devices, you can configure this value only on the AP 530.)

The RADIUS server checks the username and password against its database. If the values match, the RADIUS server issues an Access-Accept, and the AP sends an authentication-success response to the station. Otherwise, the RADIUS server issues an Access-Reject, and the AP forwards an authentication-denied response to the station.

Pros and Cons of MAC-Auth

Pros and Cons of MAC-Auth



Method	Pros	Cons
MAC-Auth (local and RADIUS)	<ul style="list-style-type: none"> • Control over which devices connect • No user interface or special software necessary on the station • Easy to combine with another solution 	<ul style="list-style-type: none"> • Not scalable • Maintained manually • Easily spoofed MAC addresses • Hardware-based, rather than user-based • By itself, no encryption

Advantages of RADIUS MAC authentication:

- Centrally maintained list
- Dynamic settings

Rev. 8.21

Pre-study Guide: 10

9

Some advantages and disadvantages of MAC-Auth apply to both local and remote authentication, but others are specific to one type or the other.

Pros of MAC-Auth

The greatest advantage of MAC-Auth is how little it requires from stations. In fact, MAC-Auth is the only way you can authenticate stations that meet both of these conditions:

- They do not have user interfaces.
- They do not support 802.1X.

For example, MAC-Auth might be the only means of authenticating a Voice over IP (VoIP) phone.

Otherwise, you must either deny these stations entirely or not implement authentication at all (hardly feasible in today's vulnerable wireless world).

802.11-compliant stations already transmit their MAC addresses in authentication request frames, so all stations support MAC-Auth.

MAC-Auth allows you to control precisely which devices connect to your network—although hackers may be able to spoof MAC addresses that are allowed on your network.

You can also add another type of security to MAC-Auth. For example, in small networks, you can combine MAC-Auth with WPA/WPA2-PSK to bolster both security methods.

In summary, MAC-Auth is best suited for:

- Devices that do not have user interfaces or support 802.1X
- Small companies that use WPA/WPA2-PSK and want to strengthen security

Cons of MAC-Auth

Although MAC-Auth gives you precise control over which devices connect to the wireless network, the configuration is tedious. The larger the list of MAC addresses you must control, the more time it takes to manage the wireless network. MAC addresses are hardly stable—even if your company’s staff rarely changes, wireless NICs might.

In addition, MAC-Auth is not scalable. Every time your company purchases a new device, you must add its MAC address to the list of allowed devices. Guest access—an increasingly common service—is impossible to control with MAC-Auth unless you know the MAC addresses for guests’ stations in advance.

A network with multiple APs increases the work, particularly if you are not using a RADIUS server and must configure the MAC-Auth list on each AP separately.

Not only is MAC-Auth difficult to manage, but it also gives you little reward for all your work. It is not secure. 802.11 requires MAC addresses to be sent in plain text. As a result, an intruder can subvert the MAC-Auth process by spoofing a valid MAC address.

Spoofing a MAC address is disturbingly easy. A hacker simply needs:

- A protocol analyzer to detect one of the MAC addresses accepted in the WLAN
- An 802.11 NIC that allows the universally administered address (UAA) to be overwritten with a locally administered address (LAA)

MAC-Auth also provides access to hardware, not users. If you use MAC-Auth alone, you will find it difficult to grant users different levels of access.

Finally, by itself MAC-Auth does not provide any encryption—a potentially serious problem due to the shared medium of wireless communications. Some network administrators add MAC-Auth onto another authentication or encryption method for an extra layer of security. However, this solution is not scalable and not feasible in large networks, where MAC-Auth adds little but complexity and extra work to the supplemental authentication.

Pros of RADIUS MAC-Auth

RADIUS MAC-Auth provides some advantages that local MAC-Auth does not. For example, RADIUS MAC-Auth offers the advantage of a centrally managed database. Local MAC-Auth is even less scalable than RADIUS MAC-Auth because you must manage lists on an AP-by-AP basis. This management requirement can be a nightmare in a large enterprise environment: every time you make a change on one AP, you must make it on all APs. If you fail to do so, authorized users might lose their connections when they roam, or a recently de-authorized user might be able to associate with an AP that has an out-of-date MAC address list.

Another advantage of RADIUS MAC-Auth is that some wireless devices—such as ProCurve APs and Wireless Edge Services Modules—can receive dynamic settings stored for the station on the RADIUS server. Although these settings are not user-based (the settings remain the same no matter who is using the station), they still allow you to apply dynamic settings, giving you greater flexibility in managing wireless network access.

Discussion Topics

Discussion Topics



- ✓ *Overview*
- ✓ *MAC authentication (MAC-Auth)*

Static WEP

- **WEP key as authentication (static WEP)**
- **WEP encryption**
- **WEP integrity**
- **Shared-key authentication**
- **Open-key authentication**
- **Pros and cons**

802.1X

WPA/WPA with preshared keys (WPA/WPA2-PSK)

Web authentication (Web-Auth)

Comparing security options

Summary

Rev. 8.21

Pre-study Guide: 13

10

The next section describes static WEP, the first, but unsuccessful, attempt at securing wireless networks. It first describes WEP encryption and then outlines how it is used as a shared encryption key for authentication, either in a shared-key or open-key system.

Static WEP—Using a WEP Key for Authentication

Static WEP—Using a WEP Key for Authentication



- WEP uses symmetric keys to encrypt and decrypt data:
 - Transmitting device encrypts the payload.
 - Receiving device decrypts the payload.
- Key provides both encryption and authentication.
- Two types of static WEP are used:
 - Shared-key WEP
 - Open-key WEP



Rev. 8.21

Pre-study Guide: 14

11

WEP was designed to secure wireless networks. Its very name—Wired Equivalent Privacy—implied that it would provide the same privacy for the shared wireless medium that users enjoyed on a point-to-point wired connection.

How did WEP measure up? Basic wireless security has three requirements:

- Authentication
- Confidentiality
- Integrity

WEP attempted to meet both authentication and confidentiality needs with a secret key but, in the end, met neither adequately.

Encryption

With WEP, all stations, as well as the AP, must encrypt frames with the secret key before transmitting them. The key encrypts the 802.11 payload, not the header. The receiving station uses the same key to decrypt the frame. (That is, the key is symmetric.) If the AP receives a frame it cannot decrypt, it drops that frame.

Encryption occurs between the AP and wireless stations. The AP decrypts traffic before transmitting it into the wired network, where it travels in plain text.

Authentication

The WEP standard does not mandate how the shared key is established. Static WEP uses a single key shared between all stations and APs. As a result, the encryption key also authenticates users: users must know the key in advance for their stations to associate with the AP.

Two methods are commonly used for sharing the WEP key:

- Static WEP
- Dynamic WEP

Before learning more about these methods, it is important to understand how WEP encryption works. You will then begin to understand why static WEP does not provide adequate security for wireless networks.

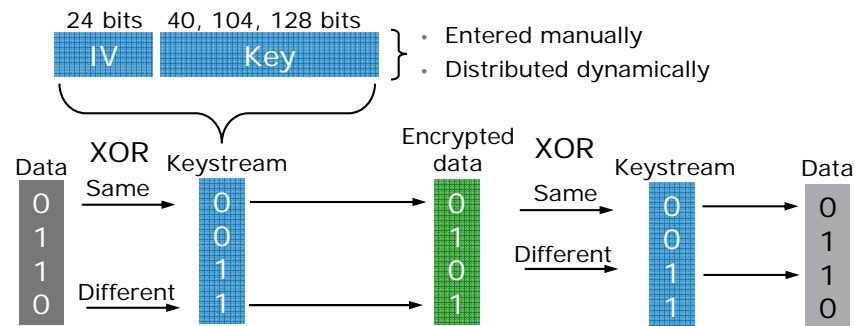
WEP Encryption

WEP Encryption



Uses Rivest Cipher 4 (RC4):

- Produces pseudo-random keystream from initialization vector (IV) plus key
- Performs reversible exclusive OR (XOR) operation on the data and keystream



Rev. 8.21

Pre-study Guide: 16

12

To preserve confidentiality, WEP uses the Rivest Cipher 4 (RC4) encryption algorithm with shared keys. RC4 is a stream cipher, which means that it transforms data bit-by-bit using a keystream.

Keystream

A keystream must be the same length as the data that it encrypts. RC4 expands a fixed length key into a pseudo-random keystream of the correct length using a key scheduling algorithm (KSM). Because the keystream is only pseudo-random, the same key always produces the same keystream for data of a certain length.

When the same keystream transforms more than one packet, it begins to leak information about the key. To decrease the number of packets using the same keystream, WEP adds a variable initialization vector (IV) to the key. Stations and the AP automatically change the IV so the keystream changes without network administrators having to change the key manually. (In practice, however, the IV does not enhance security as much as was hoped for reasons explained later in this section.)

The longer a key, the more secure it is. WEP encryption employs 64-bit, 128-bit, and 152-bit encryption as options; the IV is always 24 bits, so the shared secret itself is 40 bits, 104 bits, or 128 bits.

The 802.11 standard requires only the 64-bit key, but almost all vendors support both 64-bit and 128-bit WEP. Some vendors have implemented 152-bit encryption to enhance security.

For the types of attacks targeted at WEP, however, increasing the key length only increases the time required to crack a key *linearly*. In addition, cracking the key is usually the quickest part of the attack. Actually collecting enough packets generally takes longer. In other words, increasing the key length will provide just a few extra hours of security in the face of a determined attack.

Note

Some vendors refer to the shared secret length when citing WEP key length, and some refer to the shared secret plus the IV length. (This guide adopts the latter terminology.) This discrepancy can lead to confusion between 128-bit (104 plus 24-bit) and 152-bit (128 plus 24-bit) encryption.

XOR Operation

RC4 performs an exclusive OR (XOR) operation on the data and the keystream to produce the encrypted data. Two identical bits in the data and keystream produce a 0 in the encrypted data; two different bits produce a 1.

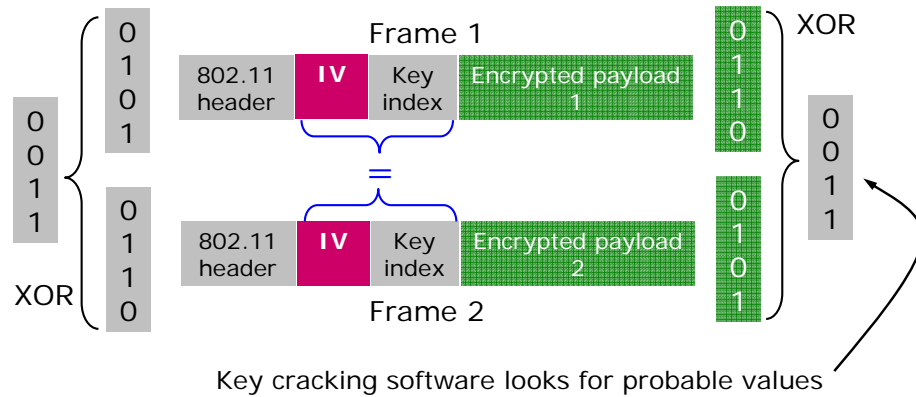
The XOR operation is fully reversible: XORing the encrypted data with the same keystream returns the original data.

Vulnerabilities of WEP Encryption

Vulnerabilities of WEP Encryption



- Hackers crack keys by collecting multiple frames encrypted with the same keystream, particularly frames encrypted with “weak keys.”
- IV (sent in plain text in WEP header) reveals these frames.
- The 3-byte IV space is not large enough to prevent reused keys.



Rev. 8.21

Pre-study Guide: 18

13

By collecting multiple frames encrypted with the same keystream, hackers can find information about the secret key. The mechanics of this process are beyond the scope of this guide but involve these basic principles:

- The XOR product of two plain text data streams equals the product of the encrypted data streams as long as the same keystream encrypted both data streams. In other words, hackers who collect multiple, identically encrypted, frames can *discover information* about the plain text data (although they cannot automatically *decipher* that data).
- This information helps hackers to perform dictionary attacks (match common words against the encrypted stream) and crack the key.

Note

The most famous attack on WEP, the Fluhrer-Mantin-Shamir (FMS) attack, exploits “weak keys.” These keys leak information about themselves. Because WEP simply adds the IV to the front of the secret portion of the key and then transmits the IV in plain text, hackers can easily identify weak keys by “weak IVs.” Hackers collect frames encrypted by the weak IVs and crack the key.

WEP's IV—intended to prevent the use of identical keys—offers fewer than 17 million different values in its 3-byte space. In a busy network, keys might start repeating IVs after as little as days or weeks, assuming that the AP actually uses all IVs. Some APs restart IVs at 1 every time a station disassociates, so hackers can probably start collecting useful frames within several minutes. In addition, hackers can sometimes stimulate the AP to generate more traffic, decreasing the time it takes to collect enough frames to crack WEP.

Worse, the WEP header shows the IV in plain text, pointing hackers straight to identically encrypted frames.

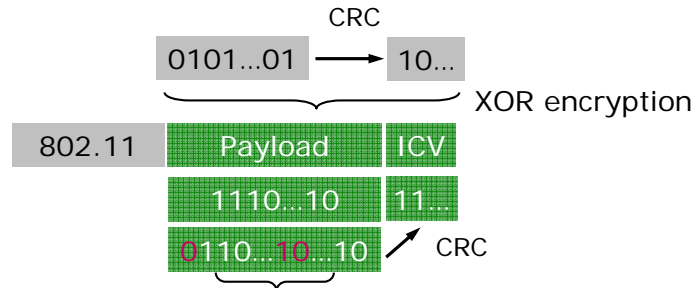
WEP Integrity

WEP Integrity



Integrity check value (ICV):

- Encrypted
- Based on CRC and too predictable for true security



Hackers add bits to conceal tampering.

With 802.11 and WEP, data integrity is provided by a 32-bit integrity check value (ICV) appended to the 802.11 payload and encrypted with WEP.

Encryption, however, does not compensate for the insecure cyclic redundancy check (CRC) on which the ICV is based. A discussion of the algorithm for calculating the CRC is beyond the scope of this guide. Suffice it to say, it is predictable enough that the CRC-based ICV check (although fine for eliminating accidentally garbled data) is woefully ill-equipped to foil someone attempting to trick it.

A hacker who tampers with a frame can use cryptanalysis to calculate which bits must be inserted to match the ICV of the tampered frame to the ICV of the original frame. Because the ICV checks out, the receiver does not detect the tampering.

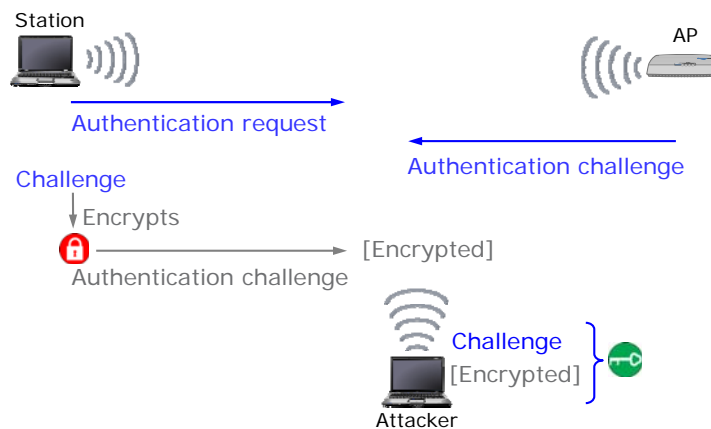
A hacker who has the ability to alter frames can exploit an AP to decrypt data for it in a replay attack. The hacker intercepts a frame and alters its destination to an IP address in the wired network. The hacker conceals the tampering as described above. The AP receives the frame, decrypts it, and transmits it unencrypted to the new address, where the hacker can collect it.

Shared-Key WEP

Shared-Key WEP



- An 802.11 authentication method based on the WEP encryption key
- Stations encrypt a challenge to prove they have the key.
- Not recommended because an attacker can combine plain text challenge and encrypted challenge to derive the key



Rev. 8.21

Pre-study Guide: 21

15

Shared-key authentication requires a station to formally prove that it has the correct secret key before it can associate to an AP. A station must support WEP encryption to use shared-key authentication.

Shared-Key Authentication Process

The station initiates the four-step shared-key authentication process:

1. The station transmits an authentication request specifying the shared-key authentication subtype.

The station and AP must agree on the authentication subtype. If a station transmits a shared-key authentication request and the AP supports only open authentication, the station cannot authenticate.

2. The AP generates an authentication challenge, which contains a random challenge string in plain text.
3. The station copies the challenge text into its response. The station then uses its shared key to encrypt the frame payload and transmits the encrypted response back to the AP.
4. The AP decrypts the encrypted frame. If the challenge text matches the challenge the AP sent, it knows the station is using the correct WEP key; the AP transmits an authentication-success response (status code 0). Otherwise, the AP replies with an authentication-failed message and prohibits the station from associating.

Roaming with Shared-Key WEP

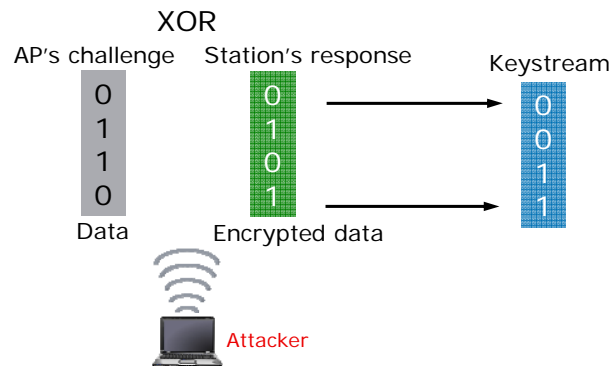
A station must always authenticate before it associates to an AP for the first time. Even though a roaming station may have already authenticated to one AP in a WLAN, it must reauthenticate to the new AP as well. Such reauthentication, however, takes place in the background: the user does not have to reenter the key. In addition, most APs store associations. If the station later roams back to the first AP, it may not need to reauthenticate.

Vulnerabilities of Shared-Key WEP

Vulnerabilities of Shared-Key WEP



- Exposes plain text challenge and the same challenge encrypted
- Allows attackers to calculate the keystream



Rev. 8.21

Pre-study Guide: 23

16

RC4 cipher's XOR function is perfectly acceptable for encryption. However, the shared-key authentication scheme is inappropriate for such a cipher. XOR RC4 operates on three bit streams:

- The original data stream
- The key stream
- The encrypted data stream

As long as hackers have any two of these streams, they can calculate the third. If hackers can match original data to a section of encrypted data, they can calculate the keystream.

Shared-key authentication docilely delivers hackers the necessary two streams:

- The AP sends a plain text challenge (the original stream).
- A station returns the encrypted challenge.

The hackers reverse the XOR operation and calculate the keystream.

Note

The encrypted frame returned by the station does include more data than the challenge text. However, this data—an authentication subtype and a sequence number—is entirely predictable from the shared-key WEP standard. Therefore, hackers can easily determine the correct original stream to combine with the encrypted stream.

Although the keystream is *not* the WEP key and does not allow hackers to encrypt their own data, it *does* allow hackers to correctly encrypt any data of the same length as the intercepted data—for example, the new challenge text the AP sends when hackers attempt to associate.

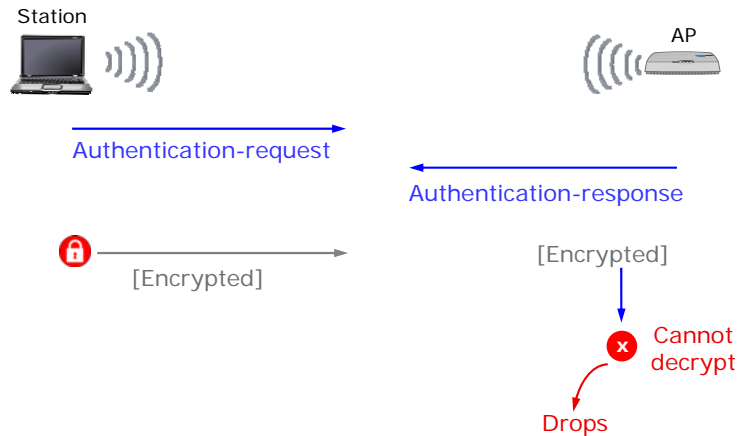
In this way, hackers can authenticate. They also have a head-start in cracking the key entirely. Once hackers have done that, they can send whatever data they want, as well as intercept and read other users' data.

Open-Key WEP

Open-Key WEP



- All stations can authenticate.
- AP drops frames encrypted with the wrong key, so only authorized stations can forward data.



Rev. 8.21

Pre-study Guide: 25

17

Open-key WEP uses 802.11 open-system authentication. In theory, any station can authenticate and associate to the AP; in practice, however, only stations with the correct key can connect to the network.

This is because stations must encrypt every frame with the shared WEP key before transmitting the frame to the AP. If the AP can decrypt the frame, the AP accepts it. Otherwise, the AP quietly drops it. Because the AP drops all incorrectly encrypted frames, only those stations with the correct key can send data into the network.

Even though, at first glance, open-key WEP seems less restrictive than shared-key, most network administrators consider open-key WEP more secure: at least it does not feed hackers information about the WEP key.

Static WEP Pros and Cons

Static WEP Pros and Cons



Method	Pros	Cons
Static WEP	<ul style="list-style-type: none"> • Encrypts data • Controls which users send and receive data (because these users must have the key) 	<ul style="list-style-type: none"> • Keys maintained manually and rarely changed • Keys maintained separately on each AP • Key can be cracked if enough frames are collected

Advantage of open-key WEP authentication:

- Does not leak information about the key

In whatever form, static WEP entails certain advantages and disadvantages. You should also consider the specific disadvantages of shared-key WEP.

Pros of Static WEP

As the first security method proposed for 802.11 networks, static WEP was widely adopted. Because its shortcomings have been widely publicized, however, most companies no longer use it. In rare cases, companies with older stations may have to use WEP if those stations do not support the more secure encryption methods used today.

As opposed to standalone MAC-Auth, WEP does at least encrypt data. You probably lock your doors, even though you know a burglar could still break a window, because you want to make it less attractive for the burglar to rob you. Although WEP may not deter the most determined attackers, it provides a similar, routine-level security.

Cons of Static WEP

The small IV space and manually configured key of static WEP render it entirely unfit for securing any reasonably busy network.

Hackers can compromise WEP encryption with readily available statistical mathematical analysis tools:

- NetStumbler exploits 802.11 behavior, sniffing the airwaves to discover wireless NICs, APs, and the networks in which they participate.
- AirSnort and WEPCrack capture traffic and implement the earlier described attacks to recover WEP keys.

Today, anyone armed with one of these shareware tools, a wireless NIC, an antenna, and a global positioning system (GPS) is capable of war driving.

Because you must configure the WEP keys manually on every AP, static WEP consumes a disproportionate amount of IT resources for the relatively little security it offers. Best practices dictate that you change the key not only every time an employee leaves the organization or a device is potentially compromised, but also periodically. In reality, many networks use the same key for months—if not longer.

Shared-Key Versus Open-Key WEP

As discussed earlier, open-key WEP ironically provides greater security than shared-key. Open-key WEP does not formally enforce authentication, but shared-key authentication is not only trivial for hackers to trick, it also reveals valuable information about the secret key. ProCurve Networking recommends that you always use open-key WEP when you choose WEP encryption.

Discussion Topics

Discussion Topics



- ✓ *Overview*
- ✓ *MAC authentication (MAC-Auth)*
- ✓ *Static WEP*

802.1X

- **Overview**
- **EAP methods**
- **Pros and cons**
- **Encryption options**
 - **Dynamic WEP**
 - **WPA/WPA2**

WPA/WPA with preshared keys (WPA/WPA2-PSK)

Web authentication (Web-Auth)

Comparing security options

Summary

Rev. 8.21

Pre-study Guide: 28

19

The next section describes 802.1X—an authentication standard that not only provides strong, user-based authentication through Extensible Authentication Protocol (EAP) but also enables secure key distribution.

You will also learn about the following encryption options for 802.1X:

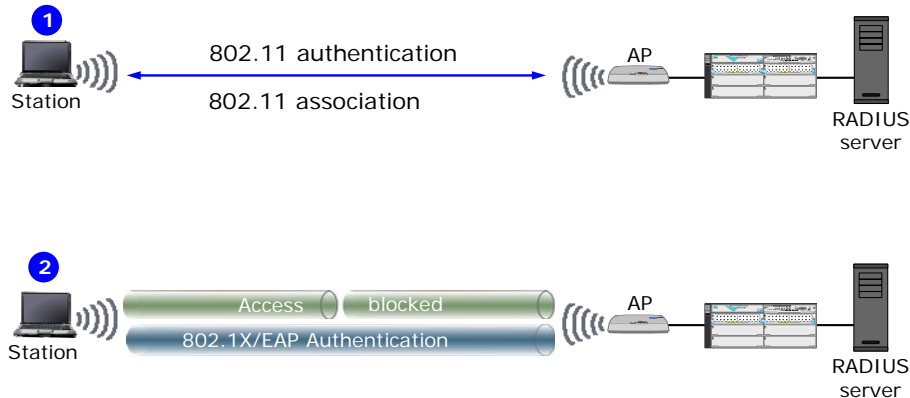
- Dynamic WEP
- WPA/WPA2

802.1X

802.1X



- Required for highest wireless security
- Forces a user to authenticate to a network RADIUS server as soon as the station associates with the AP



Rev. 8.21

Pre-study Guide: 29

20

You should now understand why network administrators rarely consider 802.11 authentication any authentication at all: even if the AP does not actually accept all requests, hackers can find and usurp necessary credentials relatively easily.

Secure wireless networks rely on supplemental authentication to a network RADIUS server after stations associate. The most powerful of the supplemental authentication methods is 802.1X.

802.1X forces a user to authenticate as soon as the connection's Data Link Layer is established. For a wireless connection, the Data Link Layer is established when the station associates with the AP (having first passed through 802.11 open-system authentication). 802.1X then manages the process by which the user authenticates and gains access to the network.

The basic sequence for initiating 802.1X involves two steps:

1. The station passes open-system 802.11 authentication and associates to the AP.
2. The AP blocks all traffic from the association and initiates the 802.1X authentication process.

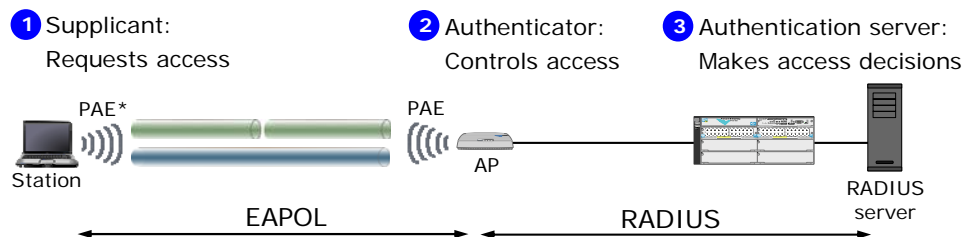
802.1X Roles

802.1X Roles



Three participants in the 802.1X authentication process:

- Supplicant
- Authenticator
- Authentication server



*PAE = Port access entity, a virtual entity that implements 802.1X on a port

Rev. 8.21

Pre-study Guide: 30

21

To understand 802.1X authentication, you must understand the role each device involved plays:

- What does the device expect from the process?
- What responsibilities does the device assume?
- What protocols does the device use to communicate?

Keep these questions in mind as you learn about the three participants in the 802.1X authentication process:

- Supplicant
- Authenticator
- Authentication server

Supplicant

On a wireless network, the station is the supplicant, or more precisely, the port access entity (PAE), which implements 802.1X on the station.

The supplicant requests access to the network and proves that it deserves this access by authenticating—typically in response to a challenge from the far end of the connection (for example, an AP).

In addition to responding to a challenge, the supplicant may also initiate the authentication process on its own behalf (by transmitting an EAP-Start packet). This mechanism protects supplicants that receive the challenge before the station has entirely booted, causing authentication to time out before the user can submit his or her credentials.

Authenticator

The authenticator is the PAE on the far end of the supplicant's connection. An AP has as many PAEs as it has associations with stations.

The authenticator controls the network access, forcing a supplicant to authenticate before it can send any non-EAP traffic over the connection.

The authenticator initiates the authentication process but then relays authentication messages between the supplicant and the authentication server.

After the authentication is completed, the authenticator decides how to control the connection. If the authentication server has accepted the user's request, the authenticator activates the virtual port created for the wireless association. In other words, the station is now completely connected to the wireless network. If the authentication server rejects the user's request, the authenticator enforces this denial and keeps the virtual port closed.

Note

The ProCurve AP 420 and AP 530 act as authenticators. With the ProCurve Wireless LAN System, however, the ProCurve Wireless Edge Services Module, rather than the ProCurve RP, is the authenticator.

Authentication Server

The authentication server makes decisions about whether or not users can access the network. These decisions are based on whether or not the user:

- Can prove his or her identity (the users' credentials are correct)
- Is connecting in the proper time and location

For example, a legitimate employee might be banned from wireless access after hours.

The server also submits its own credentials to the supplicant. In essence, the supplicant and the server authenticate each other, although the authenticator always acts as a proxy in this process.

The authentication server can be any Authentication, Authorization, and Accounting (AAA) server; however, it is almost always a RADIUS server and will be referred to as such in this guide.

The authenticator and authentication server communicate in RADIUS messages. The authenticator encapsulates the supplicant's EAP messages in this protocol.

802.1X Ports

802.1X Ports



Controlled port:

- Allows all traffic but can be disabled
- Used to control network access based on authentication state



Uncontrolled port:

- Always enabled but allows only EAP
- Used to transport authentication messages

*PAE = Port access entity, a virtual entity that implements 802.1X on a port

Rev. 8.21

Pre-study Guide: 32

22

To restrict an unauthenticated user so that the user's station can send only authentication messages, 802.1X divides the association between the AP and the station into two virtual ports.

Controlled Port

The controlled port allows all types of traffic, but it can be disabled and, by default, is. Both the authenticator port access entity (PAE) and the supplicant PAE control the port, based on the far end's authentication state. The controlled port allows the authenticator to block network access by unauthenticated users.

Uncontrolled Port

The uncontrolled port is always active. However, it can carry only the EAP packets used for authentication.

802.1X secures the network from the moment the supplicant connects by deactivating the controlled port. Without the uncontrolled port, this high level of security would shut out all traffic from users, preventing even authorized users from proving that they are authorized.

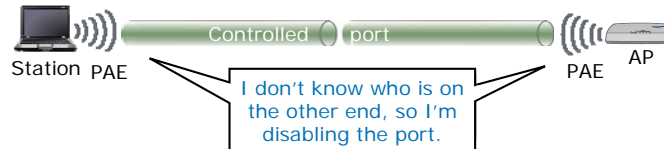
Controlled Port States

Controlled Port States



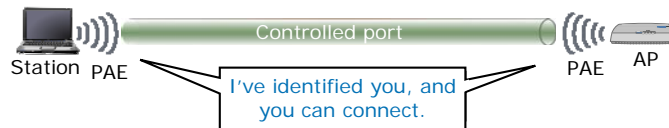
Disabled:

- Immediately when the connection is established (not authenticated)
- If the far end fails authentication



Enabled:

- If the far end authenticates successfully
- By the supplicant only, if EAP times out



Rev. 8.21

Pre-study Guide: 33

23

Because 802.1X considers all peers untrusted by default, the controlled port is disabled as soon as the connection is established. By the end of the authentication process, however, the authentication state of the supplicant, the authenticator server, or both may have changed—and the controlled port's status will reflect that change.

Both the authenticator and the supplicant PAEs leave the controlled port disabled if the far end's authentication fails. In other words, the authenticator PAE protects your network from unauthorized users. The supplicant PAE protects the user from man-in-the-middle attacks and rogue APs.

If the user authenticates successfully, the authenticator enables the controlled port and allows the user to access the network. Similarly, the supplicant enables the controlled port if the server authenticates successfully. (For example, the Windows Wireless Zero Configuration utility now lists the connection's status as Connected.)

Unlike the authenticator, the supplicant also enables the port if EAP times out; it assumes the network does not require 802.1X.

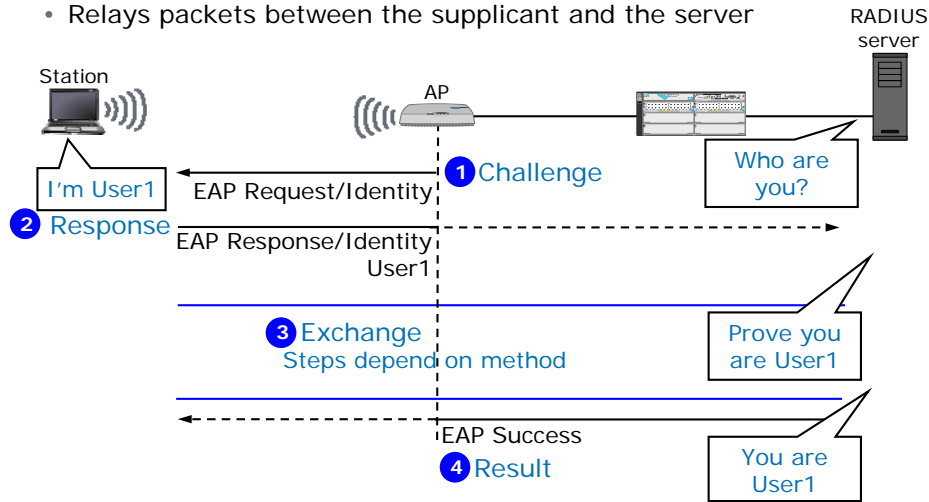
EAP Process



EAP Process

AP or Wireless Edge Services Module:

- Initiates the process
- Relays packets between the supplicant and the server



Rev. 8.21

Pre-study Guide: 34

24

The next slides describe the authentication process for 802.1X in more detail.

EAP, the protocol 802.1X uses for authentication, defines a flexible framework into which you can fit authentication methods that meet your company's environment and security policies.

The illustration above shows this general framework. As you follow the process, remember that the authenticator relays all messages from the station to the RADIUS server, translating them as necessary. The vertical dashed line underneath the AP shows the point at which the authenticator translates frames. Horizontal dashed lines show frames after they have been translated to the new format.

1. The station associates with the AP.

The AP shuts down the controlled port, blocking all traffic except EAP, and issues a challenge. The challenge is an EAP Request/Identity packet. Basically, this frame initiates the authentication process and asks the station to identify itself but not to send any other information.

2. The station responds with an EAP Response/Identity packet, which typically includes a username.

The authenticator includes the user's identity in all future frames so that the server can keep track of which EAP messages belong to which user. The user's identity also marks any accounting frames for the connection—which are important for wireless hotspots and other networks that require devices to track billing information.

3. Depending on the EAP method, the station and RADIUS server exchange a particular series of messages, which might contain one of many types of authentication credentials.

Because EAP is so flexible, it supports a variety of different EAP methods. This section of the guide describes some of the more common EAP methods used on wireless networks.

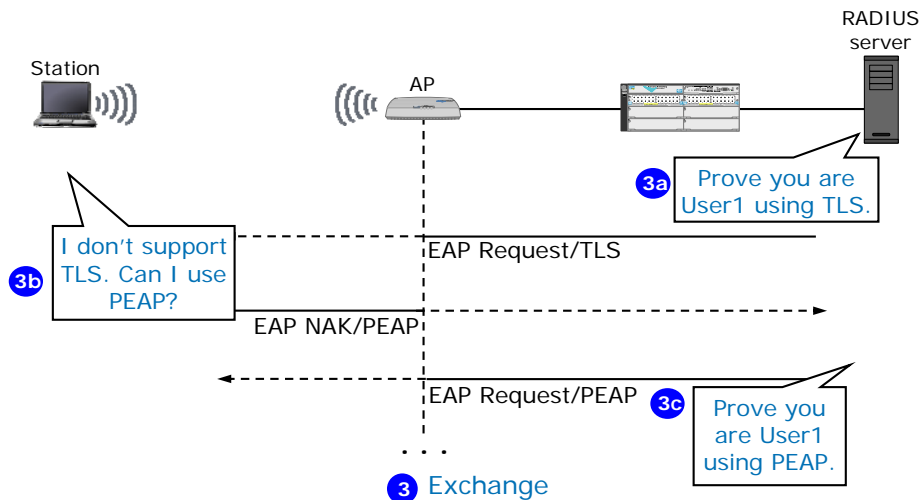
4. Based on information received in step 3, the authentication server determines whether or not the station has authenticated successfully. The AP then either activates the connection and transmits an EAP-Success or leaves the connection deactivated and transmits an EAP-Failure.

Negotiating the EAP Method

Negotiating the EAP Method



The station and the RADIUS server must support the same EAP method.



Rev. 8.21

Pre-study Guide: 36

25

The EAP method determines how the user proves his or her identity. Different methods dictate different steps, so the station and the RADIUS server *must* agree upon the method.

The first step in the exchange—the server’s EAP Request/METHOD packet—both starts the process and indicates the method that the server requires. (Depending on your RADIUS server, you can program it to select methods according to conditions such as user identity and location.)

If the station supports the requested method, it continues the exchange. Otherwise, the station sends an EAP NAK packet, which can suggest a different method. The server, if it supports the alternative method, may then initiate the exchange with the new method.

EAP Methods: TLS

EAP Methods: TLS

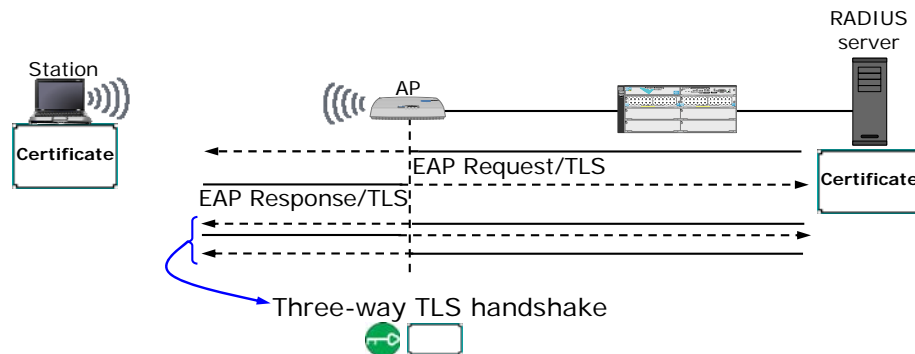


Three-way TLS handshake exchange:

- Server certificate
- User certificate
- Encryption key material

Benefits:

- Extremely secure digital certificates (which can be maintained on a smart card)
- Credentials managed by network administrators
- Key distribution
- Mutual authentication



Rev. 8.21

Pre-study Guide: 37

26

Considered one of the most secure EAP methods, EAP-TLS uses a three-way TLS handshake to exchange digital certificates and to generate encryption keys. By the end of the process, not only are the connection endpoints authenticated, but the connection itself is secured with encryption.

The EAP Request/TLS and EAP Response/TLS packets include information such as:

- Digital certificates and certificate verifications
- Supported encryption suites
- Values for generating encryption keys (not the keys themselves)

Benefits

EAP-TLS is one of the most secure EAP methods because it provides mutual authentication with Public Key Infrastructure (PKI) digital certificates. (Digital certificates rely on extremely strong asymmetric keys and trusted certificate authorities [CAs].) In addition, the process has key distribution built into it, making it ideal for wireless networks.

Because authentication is based on a digital certificate—something you have—rather than a shared secret—something you know—you, as a network administrator, have more control over users' credentials. Someone who steals a laptop can gain access to certificates installed on that laptop. Smart cards, which contain digital certificates and which users must insert themselves, protect against this vulnerability.

EAP-TLS is impervious to the attacks that affect less secure EAP methods such as EAP-MD5, but security comes at the cost of purchasing and managing the digital certificates—substantially more expensive than managing passwords. Maintaining a large number of certificates requires specialized software and trained IT staff. Another barrier to adopting EAP-TLS is the requirement for digital certificates on all stations—an impossibility in some environments.

EAP Methods: TTLS and PEAP

EAP Methods: TTLS and PEAP

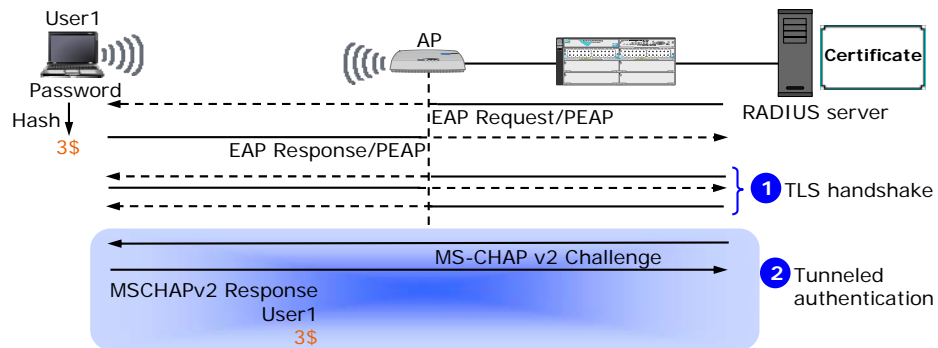


Tunnel secures weaker methods:

- Outer method—TTLS or PEAP
- Inner method—other EAP or MSCHAPv2
- Credentials—usually, username and password

Benefits:

- Stations do not require certificate
- Username and password transmitted in secure tunnel
- Key distribution
- Mutual authentication



Rev. 8.21

Pre-study Guide: 39

27

Tunneled Transport Layer Security (TTLS) and Protected EAP (PEAP) were developed to provide much of the security of EAP-TLS without forcing stations to use digital certificates—drastically reducing implementation costs. For this reason, these are among the most common EAP methods. (TTLS was developed by Funk Software and Certicom; PEAP was developed by Microsoft, Cisco Systems, and RSA Security.)

TTLS and PEAP function in very similar ways. Both methods involve a two-step authentication process; in the first step, the outer method creates a secure tunnel in which the second step takes place.

Step 1—Outer Method

Like EAP-TLS, TTLS and PEAP use a three-way TLS handshake to generate encryption keys and negotiate a tunnel secured by those keys. However, only the server authenticates itself with a digital certificate during this exchange. (Encryption keys for the tunnel are derived from the public key in this certificate.)

Step 2—Inner Method

The station authenticates itself in the second step; it uses a weaker—and so more easily implemented—authentication method, protected by the secure tunnel in which it takes place.

For the inner authentication method, TTLS can use a weaker EAP method, such as EAP-GTC, or a legacy RADIUS method, such as CHAP, PAP, or Microsoft CHAP variants (MS-CHAP v1 or MS-CHAP v2). PEAP supports methods such as MS-CHAP v2, EAP-GTC, and TLS. Because Windows wireless clients support PEAP with MS-CHAP v2, this is by far the most prevalent EAP method; all ProCurve products support it.

The tunnel is closed after the station authenticates. However, the final RADIUS Access-Accept packet distributes new keying information for the wireless association.

Benefits

Like EAP-TLS, EAP-TTLS and PEAP provide strong, mutual authentication and dynamic key distribution. Because TTLS and PEAP use encrypted tunnels to secure usernames and passwords (rather than requiring digital certificates on stations), you can implement these methods more easily than you can TLS.

TTLS has one unique benefit: it always protects the username. Depending on how PEAP is implemented, the username might be transmitted in plain text, allowing a hacker to detect the user's identity and possibly lock the user out of his or her account.

EAP Methods: MD5 and GTC

EAP Methods: MD5 and GTC

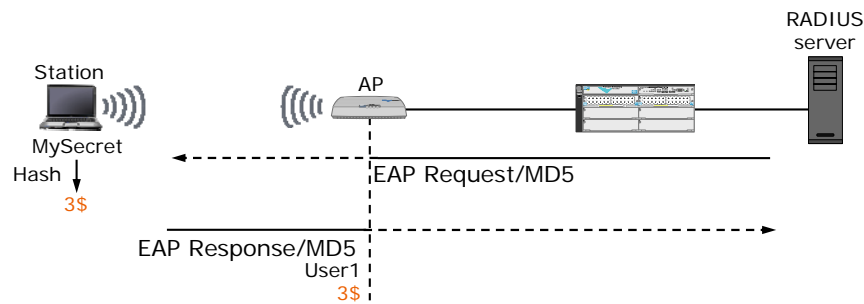


Simply transport credentials;
not appropriate for wireless:

- MD5—Username and hashed password
- GTC—Username and value from token card (or password)

Security concerns:

- No key distribution
- No mutual authentication
- Username in clear text



Rev. 8.21

Pre-study Guide: 41

28

The least secure EAP methods transport the authentication credentials in a simple two-way exchange without special provisions to prevent hackers from intercepting them. Although EAP-Message Digest 5 (MD5) and EAP-Generic Token Card (GTC) are more or less obsolete, understanding these methods does provide you with two benefits:

- The simple sequence helps you to understand some basic goals of EAP, which still apply to more complicated methods.
- EAP-GTC can be used as an inner method for TTLS or PEAP.

EAP-MD5

Similar to RADIUS-CHAP, EAP-MD5 sends:

- A username
- A one-way hash of a random challenge string and a password

MD5 inherits CHAP's strength—its simplicity and straightforward implementation.

Unfortunately, MD5 also inherits CHAP's susceptibility to dictionary and man-in-the-middle attacks.

EAP-GTC

Like EAP-MD5, EAP-GTC is a base-level method defined in the first proposal for EAP and features a similar two-step exchange. Traditionally, authentication credentials were values read from a token card. However, EAP-GTC can carry simple passwords as well.

Security Concerns

Although EAP-MD5 and EAP-GTC meet the basic requirements of EAP, they do not meet the goal of secure authentication in the unsafe, public environments of the wireless world.

Like CHAP, MD5 is vulnerable to:

- **Dictionary attacks**—Hackers who obtain the random challenge can use an automated dictionary tool to crack the user's password. (The tool couples common words with the random challenge, looking for the word that creates the correct hash.) This attack is most successful against poorly chosen passwords—always a risk when users select their own passwords.
- **Spoofing and man-in-the-middle attacks**—MD5 does not support mutual authentication, which forces both the station and the server to prove its identity. An attacker may, therefore, pose as an authentication server and intercept the session with the unaware user.

Without mutual authentication, GTC is also vulnerable to man-in-the-middle attacks. When GTC actually transports changing values read from a token card, it is less susceptible to dictionary attacks.

Neither method conceals the wireless user's identity.

Most importantly, wireless networks require encryption, but neither method supports dynamic key distribution. For this reason, you should *not* use these methods in your wireless network. In addition, some 802.1X supplicants (including the Windows client utility) do not support these EAP methods.

Summary of EAP Methods

Summary of EAP Methods



EAP Method	Authentication Credentials		Key Material	Mutual Auth	Conceals User Identity	Open	RFC
	Supplicant	Server					
MD5	Username Password	None				✓	1321
TLS	Certificate	Certificate	✓	✓		✓	2716
TTLS	Username Password	Certificate	✓	✓	Required	✓	
PEAP	Username Password	Certificate	✓	✓	Optional	✓	
SIM	SIM card	GSM triplets	✓	✓	Optional	✓ (GSM)	4186
AKA	USIM	3 rd generation AKA	✓	✓	Optional	✓ (UGSM)	4187
LEAP	Username Password	Password	✓	✓			
SRP	Username Password	Password	✓	✓	Optional	✓	

Rev. 8.21

Pre-study Guide: 43

29

This table compares various EAP methods. Important considerations include:

- Type of credentials**—Digital certificates, Subscriber Identity Module (SIM) cards, and Universal Mobile Telecommunications System (UMTS) SIM cards are more secure than usernames and passwords. EAP-SIM and EAP for UMTS Authentication and Key Agreement (EAP-AKA) authenticate the server by assuming that only an authorized server has access to the material used to generate valid encryption keys (GSM triplets). EAP-AKA's method, developed in conjunction with the 3rd Generation Partnership (3GP), is based on stronger encryption.

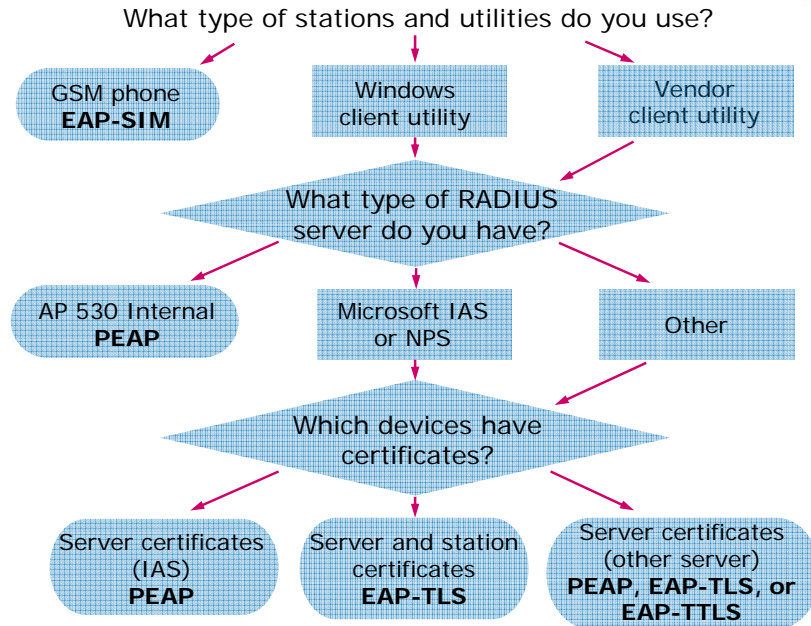
A method that relies on a password should take steps to secure that password, as do EAP-TTLS, PEAP, and EAP-Secure Remote Password (SRP), a less commonly deployed EAP method.

- Support for mutual authentication**—Any EAP methods used for authenticating wireless users should provide mutual authentication. (Mutual authentication is optional for EAP-Secure Remote Password [SRP].)

- **Ability to conceal the user's identity**—Security measures often focus on protecting a user's password. However, guarding a user's identity can also be important. First, this security measure guarantees your users' privacy. Second, it prevents a denial of service (DoS) attack in which a hacker attempts to log in as a user. After failing three times, the account is locked.
Most EAP methods provide at least optional identity protection. However, a supplicant's particular implementation may not take advantage of this capability.
- **Open or proprietary standard**—Open standards usually have wider support.

Selecting an EAP Method

Selecting an EAP Method



Rev. 8.21

Pre-study Guide: 45

30

Understanding the benefits and drawbacks that are associated with various EAP methods should give you some idea of which EAP method is right for your network. Common EAP methods, from the most to the least secure, are:

- EAP-SIM and EAP-TLS
- EAP-TTLS
- PEAP MS-CHAP v2 or PEAP GTC

Of course, you want the tightest security. However, security often comes at a cost, and in some environments TTLS or PEAP provide adequate security. The decision tree above lists some of the issues you should consider when selecting an EAP method. Find the combination of features that matches your circumstances. For example, if your network includes certificates on servers, a Microsoft Internet Authentication Service (IAS) or NAP Policy Server (NPS), and stations that use the Windows client utility, select PEAP MSCHAPv2. (A RADIUS server, NPS is part of the Network Access Protection [NAP] platform that is included with Microsoft Windows Server 2008.)

First, consider whether your network has an operational PKI and, if not, whether the security that such a system provides is worth the cost—in both money and time—of implementing it.

If your network has a complete PKI, you should probably use EAP-TLS. A directory service such as Windows Active Directory (AD) helps you manage the certificates required for this EAP method.

Select EAP-SIM for a network that includes GSM phones.

If your network does not have a complete PKI, you must select a less secure method. By installing certificates only on your network's RADIUS servers, you can use PEAP or EAP-TTLS to gain much of the security of TLS at a fraction of the cost.

Because PEAP and TTLS provide nearly the same features, your choice between them will depend largely on the method your RADIUS server supports. For example, IAS supports PEAP MS-CHAP v2. A small-to-medium business that does not have a RADIUS server can use either PEAP method with the AP 530's internal RADIUS server.

You should also consider the features on your wireless stations. The table on the previous page points out the EAP methods supported when you use the Windows client utility. Other vendors' utilities might support additional methods.

Note that all the methods shown in the table on the previous page enable the secure generation of encryption keys. You should not use EAP-MD5 and EAP-GTC in a wireless network because they cannot generate keys and so do not support dynamic WEP and WPA—the encryption methods supported with 802.1X.

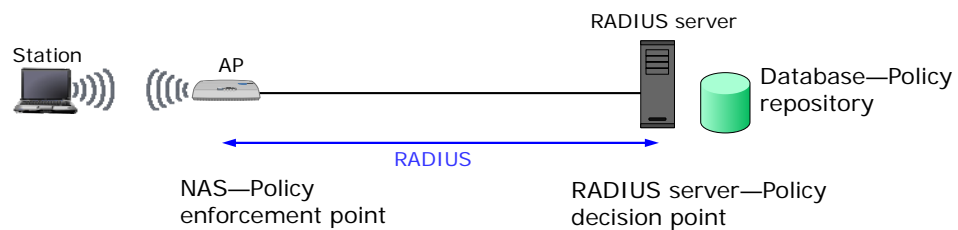
RADIUS Protocol

RADIUS Protocol



Used to communicate between:

- A device that grants users access (network access server, or NAS)
- A device that authenticates users (RADIUS server)



Rev. 8.21

Pre-study Guide: 47

31

The overview of EAP methods focused on the fundamental exchange between the supplicant and the authentication server. In reality, the supplicant and the server do not communicate directly. Instead, the authenticator (the AP or Wireless Edge Services Module) acts as a proxy to the RADIUS server.

As mentioned earlier, an 802.1X authenticator can use any AAA protocol to communicate with the authentication server. RADIUS is an industry-standard protocol for communications between a device that grants users network access and a device that authenticates, authorizes, and tracks the users. As such, it is ideal for 802.1X.

The RADIUS standard sends calls to the entity that 802.1X refers to as the authenticator, which is also called a network access server (NAS). The NAS enforces the RADIUS server's policy decisions. For example, acting as a NAS, an AP receives a RADIUS message that a user is allowed to connect. The AP's 802.1X PAE activates the association. The NAS also enforces access controls. For example, the AP 420 can place a user in a particular VLAN, and the AP 530 or the Wireless Module can apply VLANs, ACLs, and rate limits to the user.

The RADIUS server acts as the policy decision point. It determines whether a user is who he or she claims to be and decides which policies apply to the user. The server draws on information stored in a database (either its own database or a directory service database) to make these decisions.

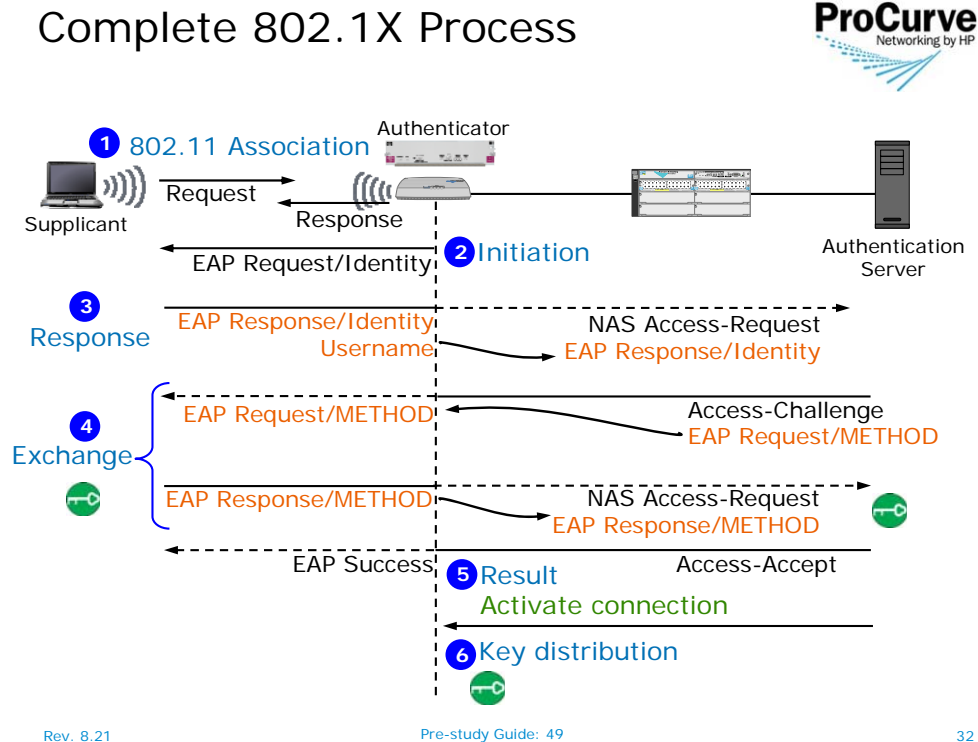
The NAS and the RADIUS server exchange these packets:

- NAS Access-Request
- Access-Challenge
- Access-Accept
- Access-Reject

When used with 802.1X, the NAS acts as a go-between for a station and a RADIUS server, encapsulating the station's EAP messages into RADIUS format. The server must support EAP over LAN (EAPOL), so that it can read these messages.

EAPOL is the form of EAP designed for Ethernet networks, but it is also used in 802.11 wireless networks. 802.11 defines the association between the station and the AP as the point-to-point link required by EAPOL.

Complete 802.1X Process



This illustration outlines the entire 802.1X process. The authenticator initiates the process when the station is associated with the AP. The authenticator then relays EAP messages between the station and the RADIUS server, encapsulating the messages in RADIUS format for the server. (This illustration and the steps below use an AP as the authenticator, but the authenticator could also be a Wireless Edge Services Module.)

More precisely, the steps are as follows:

1. The station associates to the AP. 802.1X requires 802.11 open-system authentication, so all stations can authenticate and associate. An AP that implements 802.1X blocks network access as soon as the 802.11 association is established.
2. Either the AP or the station can initiate EAP: the AP sends an EAP Request/Identity packet to initiate the process; the station sends an EAPOL Start packet.
3. After the AP issues an EAP Request/Identity packet, the station responds with its identity (either its MAC address or a username).

The AP relays the EAP Response/Identity to the RADIUS server to initiate the authentication services. The AP copies this message into the EAP field of a RADIUS NAS Access-Request and also adds information such as its own MAC address and the station's WLAN.

4. The RADIUS server selects a particular EAP method based on the user's identity and other criteria. The server initiates this EAP method, requesting credentials from the station. The AP relays the EAP message to the station, decapsulating it from the RADIUS packet.

The station sends a reply, and the exchange proceeds as dictated by the particular EAP method.

EAP methods appropriate for wireless networks include the exchange of key material. By the time the authentication is completed, the station should have all the material necessary for generating a shared encryption key.

5. If the station authenticates successfully, the RADIUS server transmits an Access-Accept packet, including an encapsulated EAP-Success packet.

When the AP receives the Access-Accept packet, it enables the controlled port and relays the EAP-Success packet to the station. The station now has network access (although the users' rights might be limited by access control lists, or ACLs).

6. The RADIUS server transmits an EAPOL Key packet to the AP so that it can generate the same key that the station has generated. You will learn more about these keys in the next section, which describes the encryption options for wireless networks that use 802.1X. For now, you should simply remember that 802.1X authentication has become an integral part of the *secure* generation of encryption keys.

802.1X Requirements

802.1X Requirements



- AP must support 802.1X.
 - AP 420, AP 530, and Wireless Module all support 802.1X.
- Network must include an EAPOL-compliant RADIUS server.
 - Wireless Module and AP 530 have internal RADIUS servers.
- Station's wireless NIC and client utility must support 802.1X with EAPOL.
 - Native support in Windows 2000 SP1 and above
 - Vendor supplicant

Rev. 8.21

Pre-study Guide: 51

33

802.1X delivers more than 802.11 authentication, but it also demands more.

The AP 420, AP 530, and the Wireless Edge Services Modules all support 802.1X. Assuming you are using one of these products, your network also requires:

- A RADIUS server (or other AAA server) that supports EAPOL

The AP (or Wireless Module) encapsulates EAPOL messages and forwards them to the RADIUS server; the server must be able to understand these messages. (If the server does not, it automatically rejects all authentication requests from the wireless stations.)

Note

The stations and the RADIUS server must also use compatible EAP methods.

You can continue to use a legacy authentication server such as a domain, Lightweight Directory Access Protocol (LDAP), or non-EAPOL-compliant RADIUS server; however, you must add the EAPOL-compliant RADIUS server as a “translator” between the APs and the legacy server. The translator server manages the exchange of EAP messages and queries the legacy server with the users’ credentials as it receives them.

The Wireless Module and the AP 530 do not require an external RADIUS server for 802.1X; they can use their internal RADIUS server instead. Alternately, they can use an external RADIUS server.

- Stations that support 802.1X with EAPOL

Some older wireless NICs do not support 802.1X. If a station has one of these older NICs, it can still authenticate as long as it includes a separate client utility that supports EAPOL. In other words, the station must include one of the following:

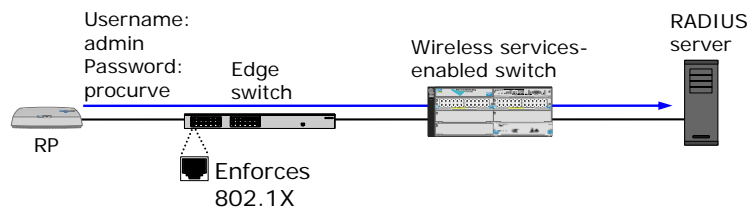
- A wireless NIC that supports 802.1X with EAPOL
- A client utility that supports EAPOL

AP as an 802.1X Supplicant

AP as an 802.1X Supplicant



- 802.1X can also control which infrastructure devices join your wired network.
- APs or RPs can act as 802.1X supplicants, authenticating to:
 - An edge switch
 - A RADIUS server



Rev. 8.21

Pre-study Guide: 53

34

In addition to authenticating users, 802.1X can control which devices connect to your wired network. Implementing 802.1X on switch ports ensures that only authorized devices join your company's network. You can use 802.1X to prevent hackers or well-meaning employees from connecting unauthorized, or rogue, APs to your switch. A rogue AP can bypass your security solutions, leaving your network open to attack.

Your APs and your switches must support the 802.1X standard. This means that the AP must include a supplicant, allowing it to function as a supplicant. The AP can then submit its login credentials to the edge switch, which can either check the devices' credentials itself or pass the credentials on to a RADIUS server.

If a switch checks the credentials itself, it matches them to its operator username and password.

If you configure the switch to use a RADIUS server, make sure that this server has a policy that allows the correct method. You might create a policy only for authenticating APs or RPs because it is not always a good idea to open these relatively insecure methods to general use. You must also configure an account for the AP or RP on your company's RADIUS server (or directory server) and then configure a matching username and password on the device.

Configuring an AP or RP to act as an 802.1X supplicant is completely unrelated to the security that you implement on its WLANs.

802.1X Encryption Options

802.1X Encryption Options



- Dynamic WEP
- WPA
- WPA2 (802.11i standard)

Rev. 8.21

Pre-study Guide: 54

35

802.1X satisfies the authentication requirement for security in an 802.11 network. Because most EAP methods allow for securely negotiating encryption keys, 802.1X is also entwined with standards that meet the confidentiality and integrity requirements for wireless network:

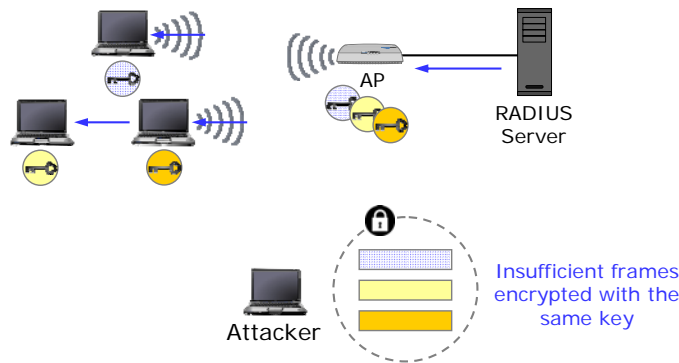
- Dynamic WEP
- Wi-Fi Protected Access (WPA)
- WPA2 (which complies with the complete 802.11i standard)

Dynamic WEP

Dynamic WEP



- Uses WEP encryption
- Generates keys as part of the 802.1X authentication process
- Narrows the window for an attack with per-session and rotating keys



Rev. 8.21

Pre-study Guide: 55

36

As mentioned earlier, WEP defines a process for encrypting data with a symmetric key. It does not dictate how wireless stations receive this key. Static WEP encryption is weak because it uses the same key again and again.

Two closely related barriers stand in the way of changing WEP keys often enough for any level of security:

- The administrative overhead of changing the key on every AP
- The administrative overhead of informing every user about the new key so he or she can authenticate

Dynamic WEP overcomes both of these barriers with 802.1X. First, 802.1X authentication frees the encryption key from its double-duty of providing both confidentiality and authentication. Second, the 802.1X process is co-opted for generating a unique, per-session key at the beginning of each association.

WEP, with all its vulnerabilities, still provides encryption. However, attacks on WEP rely on collecting millions of packets encrypted by the same key. This is easy enough to do in a busy network that uses the same key for weeks and months on end but much harder when a key lasts only as long as a single station's session.

In addition, APs can periodically refresh keys through key rotation and re-authentication.

Note

Because multiple stations receive the same broadcasts and multicasts, they must share a key for this traffic: the global key. Because it is shared, the global key is vulnerable to attacks and should be periodically rotated.

Dynamic WEP Pros and Cons

Dynamic WEP Pros and Cons



Method	Pros	Cons
Dynamic WEP	<ul style="list-style-type: none"> • Generation and distribution of per-session keys • Secure, centralized distribution of global keys • Key rotation • User-based authentication • Widely supported 	<ul style="list-style-type: none"> • Per-session keys (the default) can be cracked. • Frequent rotation for per-packet keys adds overhead. • A RADIUS server is required.* • Stations must support 802.1X.

*The Wireless Module and AP 530 provide standalone support for dynamic WEP.

Rev. 8.21

Pre-study Guide: 57

37

Pros of Dynamic WEP

Per-session unicast keys and securely distributed global keys greatly increase security. Periodic key rotation helps to prevent hackers from collecting enough packets that are encrypted by the same key to crack the key.

802.1X centralizes key distribution, making dynamic WEP not only more secure but also easier to manage.

802.1X is a more flexible and secure authentication scheme, which allows user-based VLANs on the AP 420 as well as other access controls on the AP 530 and the Wireless Edge Services Module.

Finally, wide support for dynamic WEP (for example, Windows 2000 SP 1 provides native support) means that you can implement this security even in environments with older equipment.

Cons of Dynamic WEP

Dynamic WEP is prey to all the attacks that have plagued WEP (although the windows of vulnerability are much narrower). Per-session keys can be cracked. Per-packet keys, a more secure option, add a prohibitive amount of overhead. Periodically rotating both session and global keys is usually a better solution for dynamic WEP than per-packet keys, and this is how the ProCurve AP 420, AP 530, and the Wireless Module implement dynamic WEP.

Dynamic WEP requires a RADIUS server on the network and 802.1X support on stations. Although not exactly disadvantages, these requirements are costs that you should consider.

Note

The Wireless Module and AP 530 can support dynamic WEP using their internal RADIUS server. (Stations must support 802.1X with PEAP.)

WPA

WPA



- Provided an interim solution until 802.11i was ratified
- Designed to meet all requirements on WEP-capable software

Requirement	Solution
Rotation of unicast (pairwise) and global (group) keys	Temporal Key Integrity Protocol (TKIP)
Encryption-based integrity checks	Michael
True user authentication	802.1X*

*Preshared keys provide a less secure option for smaller networks

Almost as soon as WEP was released as part of the IEEE 802.11 standard in 1999, it was cracked. The IEEE 802.11i taskforce set to work on a new standard, which was completed in 2004. In the meantime, however, companies could not wait years for increased security—hackers certainly were not waiting years to attack. The Wi-Fi Alliance designed WPA as an interim solution until the ratification of 802.11i.

WPA and WPA2 were developed to the 802.11i standard: WPA meets only the first part of the standard, which provides for backward compatibility with WEP equipment, while WPA2 meets the complete standard.

WPA Requirements

WPA consists of a series of compromises between two overarching goals. On the one hand, WPA must remedy WEP's vulnerabilities, providing:

- Rotation of both unicast and global encryption keys
- Encryption-based integrity checks
- True user authentication

On the other hand, WPA must be backward compatible with WEP hardware, eliminating the need for expensive upgrades to equipment.

Temporal Key Integrity Protocol (TKIP)

TKIP replaces WEP as a far stronger encryption algorithm, but one that uses the calculation facilities present on older wireless devices. TKIP meets the WPA's requirement for rekeying by:

- Synchronizing the refreshing of unicast and global keys on APs and stations via various handshakes
- Using key mixing to create per-frame keys

Note

WPA supports Advanced Encryption Standard (AES) as an additional replacement for WEP encryption. However, WPA does not require AES because a software upgrade may not be enough to support this algorithm. Implementation depends on the vendors building devices that support it.

Michael

As mentioned earlier, hackers can predict how to alter WEP's ICV to conceal tampering.

To meet the requirement for true data integrity, WPA designers introduced Michael. When transmitting a frame, Michael hashes the frame payload with a MIC key to produce a cryptographically secure 8-byte message integrity check (MIC), which is then appended to the payload. When receiving a frame, Michael checks the MIC, implementing countermeasures if it detects an error.

802.1X

802.1X meets WPA's requirement for user authentication. In addition, 802.1X authentication lays the foundation on which TKIP builds secure, per-frame keys.

Note

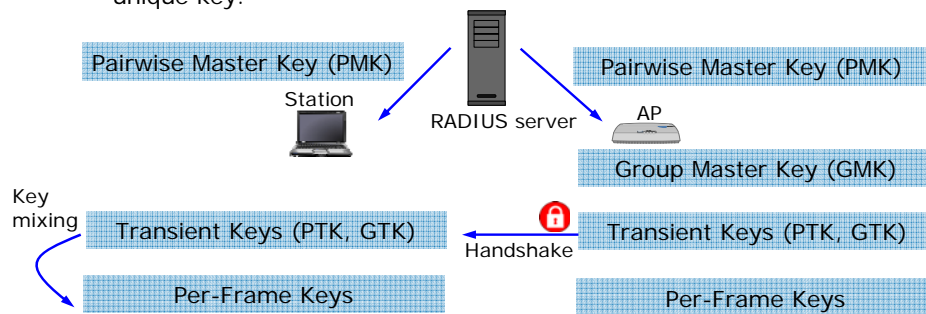
To accommodate home and small-office networks, which may not include an AAA server, WPA defines a Personal mode that uses preshared keys for authentication. This mode will be discussed later in this guide.

TKIP

TKIP



- Generates master keys during 802.1X authentication
 - Advantage—Master keys, based on pseudorandom values, cannot be leaked or guessed.
- Distributes transient keys through handshakes
 - Advantage—Keys are frequently rotated; handshakes use encryption to prevent intercepted keys.
- Creates per-frame keys with key mixing
 - Advantage—Expanded IV ensures each frame is encrypted with a unique key.



Rev. 8.21

Pre-study Guide: 61

39

TKIP uses WEP-capable hardware to generate and distribute an impressive array of keys both for encrypting and authenticating data.

Like WEP, TKIP uses RC4 encryption with 128-bit keys. One of the main problems with WEP is that frequently reused secret keys cease to remain secret. A priority for TKIP, then, is to encrypt each frame with a new key.

Pairwise keys, used for unicast traffic, are completely unique. Group keys, used for beacons, broadcasts, and multicasts, must, of course, be available to all stations in a WLAN. However, key mixing still produces per-frame keys for broadcast traffic.

To derive per-frame keys, TKIP:

1. Receives pairwise master keys (PMKs) from a RADIUS server as part of 802.1X authentication
2. Distributes refreshed pairwise and global keys, called transient keys, through periodic handshakes
3. Creates per-frame keys using key mixing

Securely Generated Master Keys

TKIP's master keys do not actually encrypt any traffic. They provide a common, shared base from which stations and APs can eventually derive identical per-frame keys:

- The AP shares a unique PMK with each station. The station and RADIUS server generate this key securely by exchanging random values during 802.1X authentication.
- The AP maintains a group master key (GMK) for all stations. It generates the key randomly.

Because keys are generated randomly and never transmitted unsecured over the network, they are not vulnerable to leaks and dictionary attacks in the way WEP keys are.

Note

The illustration on the previous page shows the source of keys on the AP and on the station. The illustration is not meant to show actual physical connections.

Key Rotation with Transient Keys

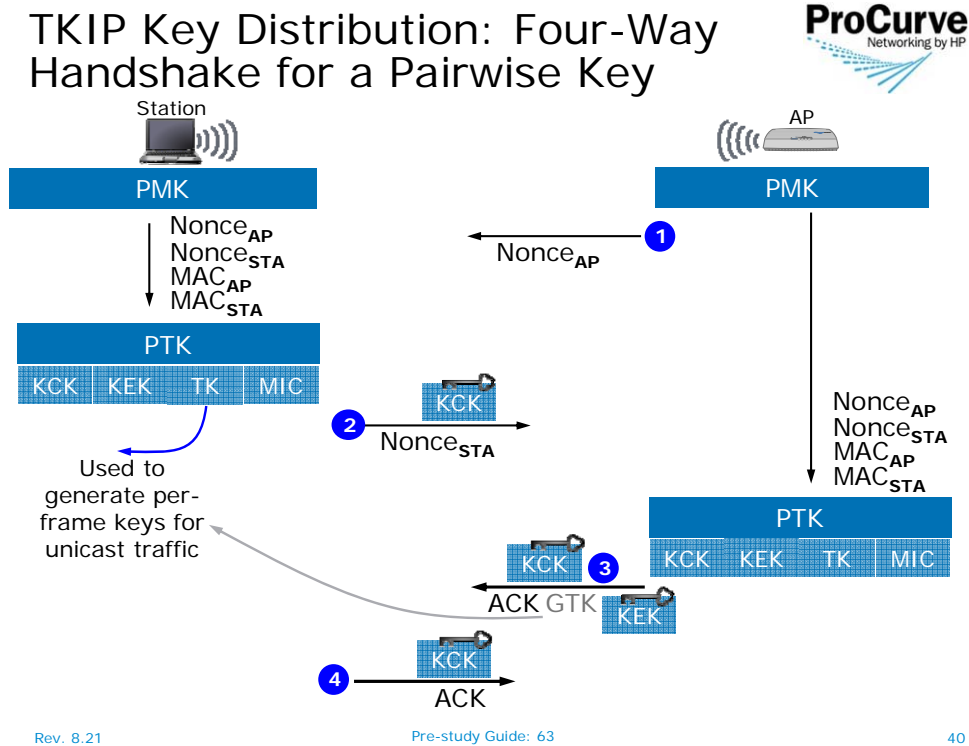
The AP periodically completes a handshake with each station to create a new pairwise transient key (PTK). The AP also periodically sends a new group transient key (GTK) to every station. The periodic refreshing ensures that the same key is never reused.

Key Mixing for Per-Frame Keys

TKIP's key mixing was designed with the same basic goal as WEP's IV—the creation of per-frame keys—but has been far more successful at meeting this goal. TKIP:

- Expands the IV to allow nearly 300 billion (2^{48}) unique values
- Performs bit-swaps and other easily processed operations on the IV and temporal key rather than simply adding the IV to the beginning of the key

TKIP Key Distribution: Four-way handshake for a pairwise key



Distributing Keys

TKIP's dynamic distribution system significantly enhances the security of the network by:

- Periodically refreshing keys so that no key is ever re-used
- The station and the AP complete handshakes to agree on new transient keys. Although based on the master keys, each new transient key is unpredictable and unique.

- Encrypting packets involved in key distribution

The AP initiates a four-way handshake and refreshes PTKs at these times:

- After 802.1X authentication or reauthentication (the reauthentication period is configurable on the ProCurve AP 420 and ProCurve Wireless Edge Services Module)
- After a certain amount of time (configurable on the AP 420 and Wireless Module)

Note

The following section describes the handshake between an AP and a station. A Wireless Edge Services Module can also manage this handshake between an RP and a station.

Completing the Four-Way Handshake

The four-way handshake proceeds with the following EAPOL-Key messages:

1. The AP transmits a random value, or nonce, to the station. (A *nonce* is a random value used to create unique temporal keys from a master key.)

The station then has all the information it needs to generate a new 512-bit PTK from its PMK:

- Its own and the AP's nonce—The randomly generated nonces, which are different for each new handshake, make transient keys unique.
- Its own and the AP's MAC address

The station splits the PTK into four 128-bit keys:

- Key confirmation key (KCK)
- Key encryption key (KEK)
- Temporal key (TK)
- Message integrity check (MIC) key

The first two keys serve only to secure the exchange of keys.

The station transmits the TK to TKIP for generating per-frame keys. Michael uses the MIC key to preserve data integrity.

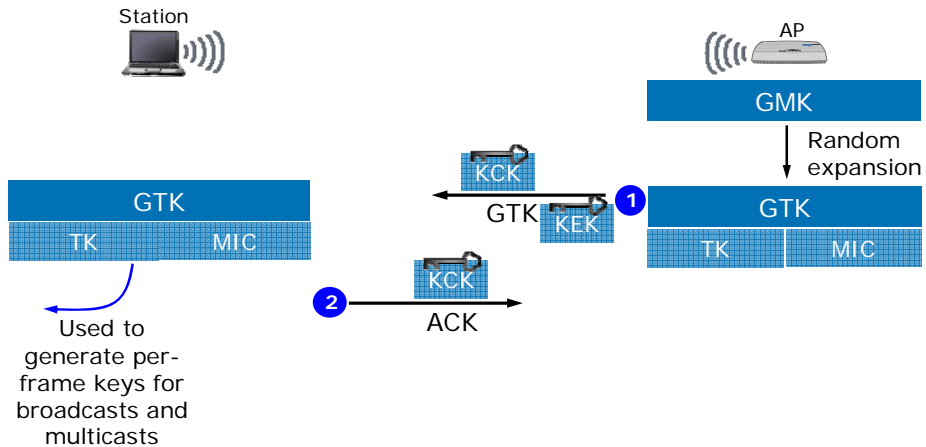
2. The station transmits its nonce to the AP, so the AP can follow the same process to generate identical keys. The station also creates a MIC with the KCK and appends it to the packet. After the AP generates the KCK itself, it verifies the packet. An incorrect MIC indicates a man-in-the-middle attack, so the AP terminates the handshake.
3. The AP acknowledges that it has installed the new keys. The packet the AP sends can optionally include a GTK encrypted with the KEK to refresh the global key.
4. The station acknowledges the last message, completing the handshake.

TKIP Key Distribution: Two-way handshake for group key

TKIP Key Distribution: Two-Way Handshake for Group Key



Relies on KCK and KEK established in previous four-way handshake



Rev. 8.21

Pre-study Guide: 65

41

By itself, 802.1X provides no mechanism for refreshing *global* encryption keys. Instead of, or in addition to, transmitting the GTK as part of the four-way handshake, the AP can complete a two-way handshake to refresh this key.

The AP initiates the handshake to distribute an *existing* GTK whenever a station authenticates and completes the four-way handshake.

The AP creates a *new* GTK and initiates the two-way handshake to distribute it after:

- A certain amount of time (configurable on the AP 420 and Wireless Edge Services Module)
- 10,000 frames (the AP 530)

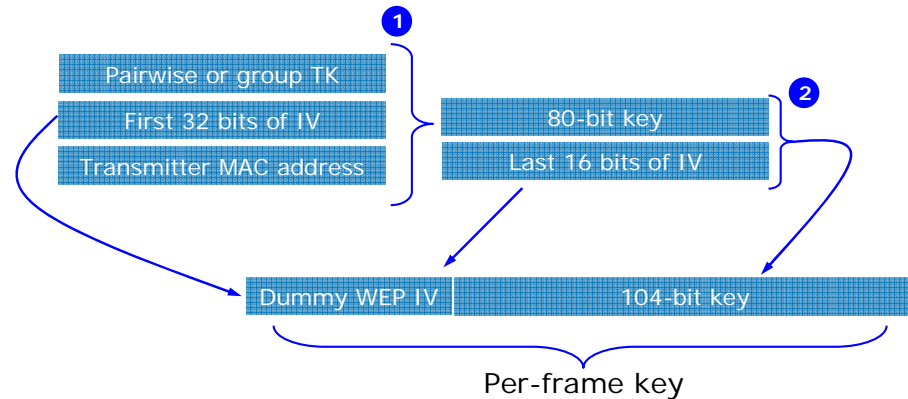
Distributing the GTK requires only two steps because the AP and station do not have to exchange nonces. The AP simply secures the exchange using the previously established KEK and KCK. The station acknowledges the key.

TKIP Key Mixing

TKIP Key Mixing



Per-frame key constructed from a temporal key in two phases



Rev. 8.21

Pre-study Guide: 66

42

Key mixing produces a unique, non-predictable key for each new frame. This key is based on the temporal key and various other inputs.

Key mixing takes place in two phases, the first of which occurs once every 65,536 frames to limit the drain on processing power.

Phase 1

TKIP mixes three values to produce an 80-bit key. Instead of simply concatenating the values as WEP does with the IV and shared key, TKIP performs bit-swaps and other calculations to hash the three values together.

Pairwise or Group TK

You should now understand how TKIP generates changing temporal keys for both unicast traffic (the pairwise TK) and broadcast and multicast traffic (the group TK).

IV

Static WEP attempted to create different keys by concatenating the secret key with different IVs. However, the limited size and clear-text transmission of the IV undermined any added security.

TKIP's IV acts as a sequence counter, incrementing by one for every frame and helping to guard against tampering and replay attacks. The greater length of TKIP's IV (expanded from WEP's 3 bytes to 6 bytes) ensures no IV will be repeated in the limited lifetime of transient keys.

In the first phase, TKIP factors only the first 32 bits of the IV into the hash. Because these bits only change every 65,356 frames, the AP or station calculates the phase 1 key relatively infrequently, saving processing power.

MAC Source Address

TKIP also mixes portions of the 802.11 header such as the transmitter address into the key. (For frames sent by stations, the transmitter address is the station. For frames forwarded by the AP, this address is the AP's, even though the *source* address might be that of a device in the wired network.) Mixing in this MAC address further expands the number of different keys on different stations.

Phase 2

TKIP now mixes the last 16 bits of the IV with the 80-bit key produced in phase 1. Because these bits change every frame, so does the key.

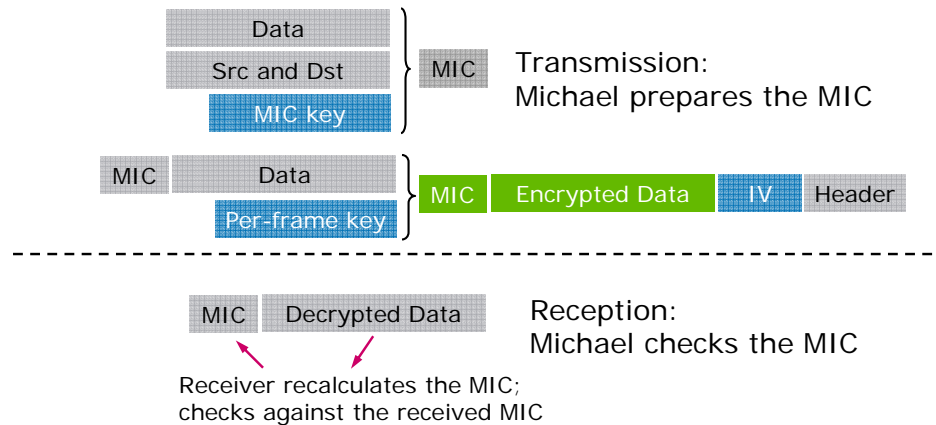
TKIP places a dummy WEP IV at the front of the key.

Michael

Michael



- Michael creates unpredictable MICs using the MIC key.
- TKIP encrypts MIC with the frame.
- If Michael detects errors in the MIC check, it implements countermeasures.



Rev. 8.21

Pre-study Guide: 68

43

Using simple bit-shifts and swaps supported by calculation facilities on WEP-capable devices, Michael operates on 32-bit blocks of data with the MIC key to calculate an 8-byte MIC for each frame that appears unique and random. Because Michael factors the source and destination addresses into the MIC, the frame header is also protected from tampering, preventing attacks in which hackers use the AP to decrypt packets for them.

Michael places the MIC between the data portion of the IEEE 802.11 frame and the 4-byte ICV, where it is encrypted along with the data.

After the receiver decrypts the packet, Michael checks the decrypted MIC by recalculating the MIC on the received data. If the two MICs match, the receiver can be reasonably sure that the data has not been altered.

WPA's designers were well aware that Michael is less a perfect solution than it is the best available solution for hardware designed for WEP. Certain brute force attacks can crack the MIC key. If Michael detects a MIC error, which might indicate the initial phases of such an attack, it takes counter-measures such as deactivating the implicated association for 60 seconds and refreshing master keys. (A MIC error signals a serious security breach because earlier CRC and ICV checks would screen out integrity losses from innocently garbled data.)

WPA2 (802.11i)

WPA2 (802.11i)



- Highly secure system that meets 802.11i standard
- Encryption—Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP) and Advanced Encryption Standard (AES)
- Integrity—CBC-MAC
- Authentication—same modes as WPA

Rev. 8.21

Pre-study Guide: 69

44

WPA supported the subset of 802.11i designed for backward compatibility with WEP equipment. WPA2, on the other hand, is fully compatible with 802.11i.

In concept, WPA2 functions much as WPA does. It provides:

- Per-frame pairwise (unicast) keys
- Per-frame group (global) keys
- Encryption-based integrity checks
- 802.1X authentication

However, WPA2 is based on the Advanced Encryption Standard (AES) block cipher, which raises security to a higher level.

Strong Encryption

AES operates under the Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP). CCMP also distributes and refreshes the keys necessary for AES using handshakes similar to TKIP's.

The bulk of WPA2's added security originates in the strength of the AES block cipher. For WPA2, AES operates in counter mode, a mode that:

- Allows each 128-bit block of data to be encrypted with a unique key stream
- Minimizes the effects of data corrupted in transmission

In addition to CCMP/AES, WPA2 supports TKIP for backward compatibility with older stations that cannot support AES.

Encryption-Based Integrity

CCMP/AES creates a cryptographically secure, 8-byte hash, or MIC, to attest to a frame's authenticity. The protocol calculates the MIC by operating on the frame payload, as well as information from the frame's header, with the *same* temporal key used to encrypt the payload. However, this operation uses Cipher Block Chaining (CBC) rather than AES counter mode.

It is important to understand that:

- CBC-MAC is a secure protocol that creates hashes unpredictable to anyone without the correct key.
- The information added from the frame's header protects against replay attacks.

Authentication

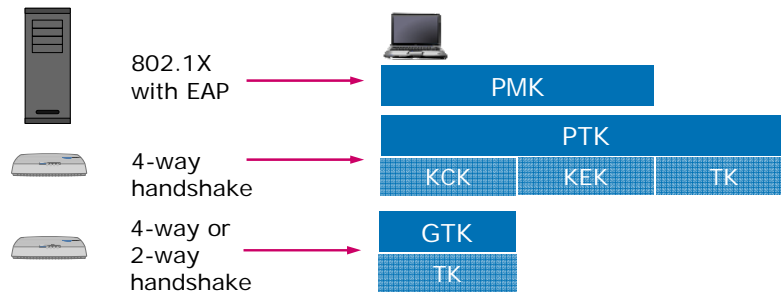
Because 802.1X currently provides industry-standard secure authentication, WPA2 relies on the same authentication as WPA. In addition to 802.1X, WPA2 can use preshared keys, an option described later in this guide.

CCMP/AES

CCMP/AES



- Similar key hierarchy to TKIP but based on stronger AES encryption
- Periodically refreshed PTKs and GTKs



Rev. 8.21

Pre-study Guide: 71

45

The main difference between CCMP/AES and TKIP is the greater security of the encryption method. The key hierarchy and distribution process, however, are quite similar:

- Each station generates its PMK, preferably as part of the 802.1X authentication to a RADIUS server. The AP also knows the PMK.
- The AP periodically expands each PMK into a new PTK, which it distributes to the station via a four-way handshake. Either the four-way handshake or a two-way handshake distributes refreshed GTKs to all stations.

Unlike TKIP, CCMP uses the same key to secure data and the MIC. As a result, CCMP requires only 128 bits for the GTK and 384 bits for the PTK. The entire GTK is used to create the per-frame keys for global traffic while the PTK first divides into three 128-bit keys:

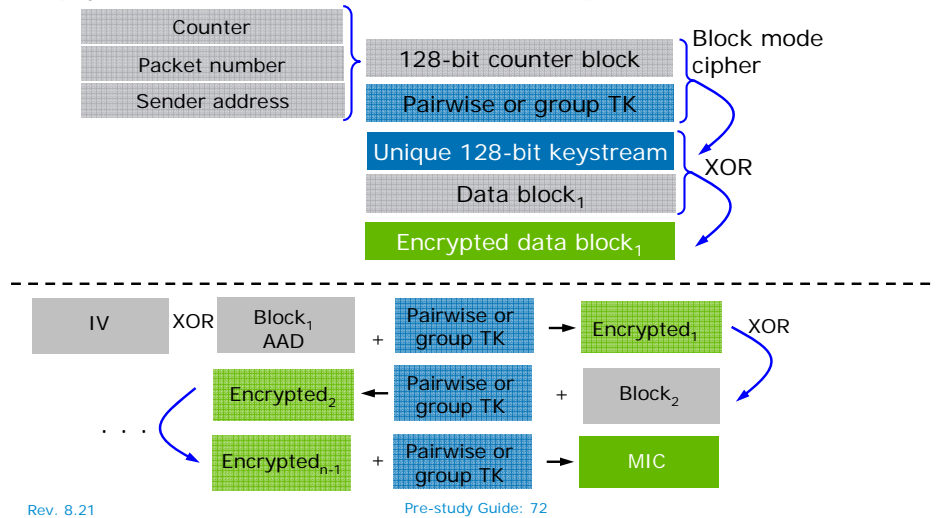
- The KCK and the KEK for securing the key distribution handshakes
- The TK for deriving per-frame keys for unicast traffic

CCMP/AES: Continued

CCMP/AES: Continued



- AES counter mode encryption—A unique keystream, generated using the block cipher and TK, encrypts each 128-bit block of data.
- MIC for integrity—CBC-MAC calculates the MIC using the TK and the frame payload. Additional authentication data (AAD) protects the frame header.



Rev. 8.21

Pre-study Guide: 72

46

An entire book could be devoted to the intricacies of WPA2 and CCMP/AES. This guide focuses on explaining WPA2’s improvements at a relatively high-level:

- Operating in counter mode, AES generates unique key streams and encrypts data. AES is the most important security enhancement of WPA2 over WPA. This algorithm is simply stronger than WEP-based encryption, despite all of TKIP’s fixes.
- CCMP’s method of calculating the MIC relies on encryption and is tamper-resistant.

AES Counter Mode Encryption

A block cipher such as AES performs a fixed series of operations on equal-sized blocks of text. AES uses the Rijndael key schedule and a 128-bit key to transform a 128-bit input block into an encrypted block.

WPA2 specifies that AES functions in counter mode, which means that, rather than actually encrypting data, the block cipher creates a series of 128-bit key streams. In other words, instead of using the block cipher and TK to encrypt the data itself, counter mode AES applies the block cipher and TK to a “counter” block.

A “counter” block includes information such as:

- **Counter**—The counter increments for each iteration of the block cipher.
- **Packet number and sender address**—Including the sender address allows different stations to use the same packet numbers but always creates different key streams.

The output is a 128-bit keystream, which then encrypts plain-text data in much the same way as a stream cipher, using a simple XOR operation. The next 128-bit block of data will be XORed with a different key stream, the one created by encrypting the second “counter” block with the block cipher and TK. Because each block of data is encrypted with a unique, securely generated key stream, the same block of plain text never produces the same block of cipher text, and encrypted data remains quite secure (vastly more secure than WEP-encrypted data).

Using a block cipher that mimics a stream cipher makes CCMP more resistant to errors—an important advantage in the wireless medium. A bit corrupted during transmission only affects one decrypted bit instead of an entire block of data.

MIC for Data Integrity

CCMP calculates the MIC using the CBC-MAC method. This AES mode encrypts data using the block cipher and a TK. It then XORs the encrypted block with the next block of plain text before encrypting that new block. The final encrypted block is the MIC. All previous blocks are forgotten: as with most integrity checks, validating the final result is important, but preserving the actual data used to encrypt is not.

With CBC-MAC, changing even one bit in the message produces a totally different result, a result that cannot be predicted without the temporal key used to perform the CBC encryption. Consequently, hackers cannot tamper with data without invalidating the MIC, unlike WEP’s easily circumvented ICV.

As you can see in the illustration on the previous page, the first block (or blocks) of data to be authenticated are called additional authentication data (AAD). These are bits taken from the 802.11 header. If a hacker tampers with the header (which must, of course, be transmitted in plain text), the MIC check fails. Securing the 802.11 header protects you from replay attacks in which a hacker hijacks the AP to decrypt intercepted and re-addressed frames.

WPA/WPA2 Uses and Requirements



WPA/WPA2 Uses and Requirements

- You should choose WPA or WPA2 for enterprise networks:
 - WPA for wider support
 - WPA2 for higher security
 - Both for backward compatibility

Network Requirements
 EAPOL-compliant RADIUS server

Station Requirements
 802.1X capability, either:

- Native support on Windows 2000 SP1 and above
- Supplicant software for 802.1X

For WPA, either:

- WPA Client for Windows
- Software for TKIP and Michael

For WPA2, either:

- WPA2 Client for Windows
- Software for AES

AP Requirements
All ProCurve APs

WPA two-phase authentication:

- 802.11 open-system
- 802.1X

For WPA:

- TKIP and Michael
- WPA informational element

For WPA2:

- Software and hardware for AES
- Backward compatibility with TKIP
- WPA2 informational element

Rev. 8.21

Pre-study Guide: 74

47

An enterprise network requires the security of WPA or WPA2. Choosing between the two standards is largely a matter of balancing wider support with higher security. (You can also use both standards in the same WLAN, as described later in this guide.)

Before you select WPA or WPA2, you should verify that your company’s network meets all the requirements. Although WPA was designed to upgrade WEP-ready hardware as painlessly as possible, it does require certain software enhancements on legacy equipment, and WPA2 requires further enhancements still. However, the ProCurve AP 420, AP 530, and Wireless Edge Services Module meet all requirements for WPA and WPA2.

Requirements for the Network

For 802.1X authentication, the network requires an EAPOL-compliant RADIUS server. You can continue to use an existing authentication server that does not support RADIUS with EAPOL. However, you must add an EAPOL-compliant server between the AP and the existing server.

Requirements on the Station

The station must support 802.1X authentication with EAPOL. Either the wireless NIC or other software installed on the station must support the WPA encryption algorithms. TKIP is mandatory, but AES is mandatory only for WPA2. Today most wireless NICs support AES, but some still support only TKIP. Therefore, backward compatibility with TKIP remains important in many networks.

Stations might also require updates to their wireless client utilities. The table at the end of this section summarizes these requirements, listing the Windows version and support for Wireless Zero Configuration—hereafter referred to as the Windows client utility.

Initially, the Windows client utility did not support WPA; instead, wireless NIC vendors provided WPA support with their own client utilities. Now the Windows WPA Client enables the WPA options in the Windows client utility dialog boxes. You can download this client for free, using the link shown in the table below.

If you have a legacy operating system that does not support the Windows client utility, you must obtain a WPA-compliant configuration tool from your wireless NIC vendor.

The Windows WPA2 Client is only supported on stations running Windows XP with SP2, but vendor utilities can provide support for WPA2.

Windows Version	Wireless Zero Configuration	Requirement for WPA	Requirement for WPA2
Windows XP with SP2 or Windows Vista	Yes	None (Windows WPA Client automatically included)	WPA2 Client http://support.microsoft.com/?id=893357
Windows XP with SP1 or Windows Server 2003	Yes	Windows WPA Client (Search Microsoft for the Windows XP Support Patch for Wi-Fi Protected Access.)	WPA2-compliant configuration tool for wireless NIC
Windows Server 2003	No	WPA-compliant utility for NIC	WPA2-compliant utility for wireless NIC
Windows 2000	Not applicable	WPA-compliant utility for NIC	WPA2-compliant utility for wireless NIC

Requirements on the AP

The AP must be configured to beacon the WPA or WPA2 informational element, thereby indicating its support of this security option.

WPA/WPA2 also requires two-phase authentication:

1. Open-system authentication before association to satisfy the 802.11 requirement
2. 802.1X authentication after the 802.11 association is established

The AP requires special software to implement TKIP and Michael for WPA and CCMP with AES for WPA2.

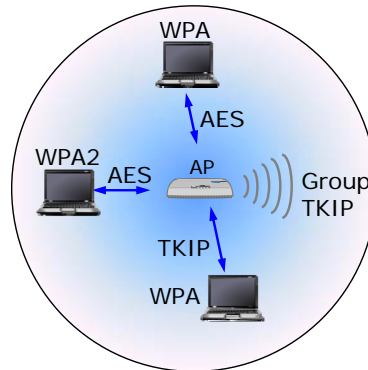
The ProCurve AP 420, AP 530, and Wireless Edge Services Module meet these requirements. Remember, however, that AES encryption adds overhead, a potential concern if your network includes small wireless devices such as phones or personal digital assistants (PDAs).

Using Multiple Encryption Standards

Using Multiple Encryption Standards



- WPA and WPA2 stations can join the same WLAN but must use the required encryption.
- 802.11i Mixed Mode allows both types of encryption:
 - A station can use either a TKIP or AES pairwise key.
 - The AP distributes a TKIP group key.



802.11i Mixed Mode

Rev. 8.21

Pre-study Guide: 76

48

The two WPA versions correspond loosely to encryption protocols. WPA stations always support TKIP, and WPA2 stations always support CCMP/AES. However, WPA stations, with the proper software and hardware, *can* use AES, and WPA2 stations support backward compatibility with TKIP.

Because WPA and WPA2 overlap in many ways, stations of both types can join the same WLAN. However, all stations in the WLAN must use the required encryption standard. For example, if the WLAN requires AES encryption, WPA stations can join only if they support such encryption, even though AES is optional under WPA.

802.11i Mixed Mode allows simultaneous support for multiple encryption standards so that companies can migrate their network from TKIP with WPA to CCMP/AES with WPA2. Mixed Mode allows stations to choose either a TKIP or AES key for unicast traffic.

The Mixed Mode global key is always a TKIP key. Because both WPA and WPA2 stations must support this standard, all stations can encrypt and decrypt broadcasts and multicasts.

WPA/WPA2 Pros and Cons

WPA/WPA2 Pros and Cons



Method	Pros	Cons
WPA/WPA2	<ul style="list-style-type: none"> • Per-frame keys • Secure key distribution and rotation with TKIP or CCMP • Centralized user authentication • Optional AES 	<ul style="list-style-type: none"> • Increased AP workload, potentially decreasing performance • RADIUS server and station support for 802.1X • Either software upgrades or special hardware and software on legacy APs and stations

WPA versus WPA2:

CCMP/AES offers higher security, but not all stations support it.

Rev. 8.21

Pre-study Guide: 77

49

Pros of WPA/WPA2

Both WPA and WPA2 provide many benefits:

- Unique, per-frame keys with minimal added overhead
- TKIP or CCMP for distributing and rotating transient keys
- Centralized user authentication through 802.1X

In addition, WPA/WPA2 can support the highly secure AES.

Currently, WPA and WPA2 are the only solutions for true Layer 2 security in wireless networks.

Cons of WPA/WPA2

WPA and WPA2 increase the APs' workload—they must encrypt and decrypt frames from multiple stations, performing relatively sophisticated calculations. When enforcing these encryption methods, an AP may not support as high throughput for as many stations as an AP implementing less grueling encryption. If you must purchase more APs to meet bandwidth requirements, remember to include that cost in your analyses.

Like dynamic WEP, WPA/WPA2 in standard (or Enterprise) mode requires an EAPOL-compatible RADIUS server and 802.1X support on stations.

For legacy APs and stations, WPA may require a software upgrade; new wireless devices support WPA.

Discussion Topics

Discussion Topics



- ✓ *Overview*
- ✓ *MAC authentication (MAC-Auth)*
- ✓ *Static WEP*
- ✓ *802.1X*

WPA/WPA with preshared keys (WPA/WPA2-PSK)

- **Overview**
- **Failed WPA/WPA2-PSK handshake**
- **Pros and cons**

Web authentication (Web-Auth)

Comparing security options

Summary

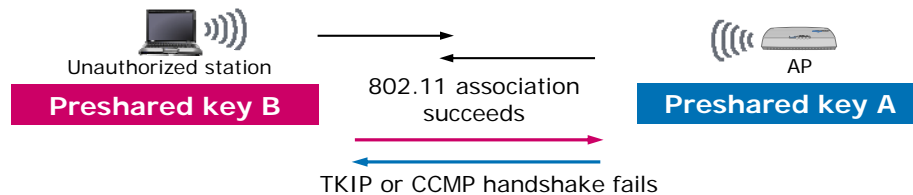
The next section describes a less secure authentication method, which uses WPA/WPA2 with preshared keys.

WPA/WPA2-PSK

WPA/WPA2-PSK



- Preshared key authentication instead of 802.1X (Personal mode)
- Less secure option for:
 - Networks without a RADIUS server
 - Stations without 802.1X
- Preshared key:
 - Provides authentication
 - Provides master keys for TKIP or CCMP/AES encryption
 - Is secure against cracks
 - Is susceptible to leaks



Rev. 8.21

Pre-study Guide: 80

51

Both WPA/WPA2 and the 802.11i standard on which it is based specify an exception for the 802.1X requirement. Instead of authenticating through 802.1X, all users can authenticate by entering the same preshared key. The Wi-Fi Alliance also calls this option Personal mode.

WPA/WPA2-PSK allows small businesses without an EAPOL-compatible RADIUS server to take advantage of the stronger encryption offered by TKIP or CCMP/AES. You might also select this variant of WPA/WPA2 to configure a WLAN for guests who have stations that might not support 802.1X—although many companies select Web-Auth for such guest WLANs.

802.1X typically helps APs and stations derive unique PMKs for unicast traffic. For WPA/WPA2-PSK, the master key is the preshared key instead, so all stations share the master key. However, the stations still compute different transient keys because TKIP and CCMP also factor nonces and MAC addresses into these keys.

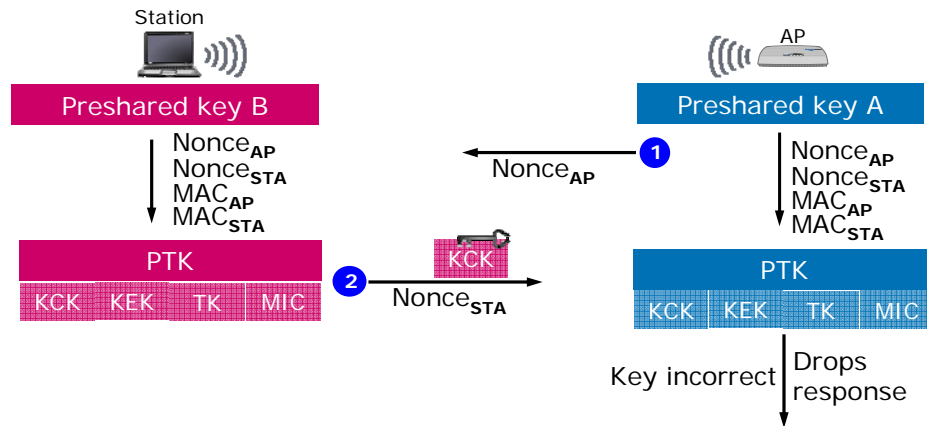
Like open-system WEP, WPA/WPA2-PSK institutes a de facto, rather than formal, authentication. A user who enters the incorrect preshared key completes the 802.11 association, but the TKIP or CCMP handshake fails, and the station cannot forward data.

Failed WPA/WPA2-PSK Handshake

Failed WPA/WPA2-PSK Handshake



- When a station enters the wrong preshared key, it derives the wrong KCK.
- The handshake fails.



Rev. 8.21

Pre-study Guide: 81

52

Now that you understand TKIP (or CCMP) handshakes, you should understand how a WPA preshared key enforces de facto authentication. The preshared key acts as the PMK for WPA-PSK.

If a station and an AP have different preshared keys, or PMKs, they derive different PTKs. From the PTKs, they in turn derive different KCKs. When the AP uses its KCK to check the station's response in the four-way handshake, the check fails. The AP drops the response, and the station, although formally associated with the AP, can never complete the handshake. Typically, the station then disassociates itself.

WPA/WPA2-PSK Pros and Cons

WPA/WPA2-PSK Pros and Cons



Method	Pros	Cons
WPA/WPA2-PSK	<ul style="list-style-type: none"> • No need for RADIUS server and 802.1X • Per-frame keys • Secure key distribution and rotation with TKIP or CCMP • Optional AES 	<ul style="list-style-type: none"> • Weaker authentication • Either software upgrades or special hardware and software on APs and stations • Increased AP workload, potentially decreasing performance

Rev. 8.21

Pre-study Guide: 82

53

Pros of WPA/WPA2-PSK

WPA/WPA2-PSK provides networks that do not include RADIUS servers and 802.1X support with many of the same advantages as standard WPA/WPA2:

- Per-frame keys
- Secure key distribution and rotation with TKIP or CCMP
- Optional AES, an extremely secure encryption algorithm

For this reason, small companies often choose WPA/WPA2-PSK. Of course, the Wireless Module and the AP 530 both have internal RADIUS servers, providing support for WPA/WPA2 with 802.1X to such companies.

Cons of WPA/WPA2-PSK

The simplified authentication scheme of WPA-PSK does, however, manifest as weaker authentication and potentially less control over who connects to your network. Although all stations use the same master key, WPA's other enhancements, such as key mixing, the extended IV space, and secure key rotation, compensate for this shortcoming. (That is, using the same master key hardly entails all the problems of using the same WEP key.)

The greater security concern is that, because all users have the same password, chances that one user will leak the password rise dramatically. WPA does bolster one weakness of shared passwords: expanding master keys into transient keys exhausts enough time and processing power to deter many dictionary attacks. Still, you should avoid choosing a short password or one that is easily guessed. Instead, pick a password with at least eight characters and some special characters.

As with all types of WPA/WPA2, the stronger encryption comes at the cost of potentially decreased performance. If you have legacy equipment, it also requires software or hardware upgrades.

Discussion Topics

Discussion Topics



- ✓ *Overview*
- ✓ *MAC authentication (MAC-Auth)*
- ✓ *WEP key as authentication (static WEP)*
- ✓ *802.1X*
- ✓ *WPA/WPA with preshared keys (WPA/WPA2-PSK)*

Web Authentication (Web-Auth)

- **Uses**
- **Web-Auth and the Wireless Module**
- **Web-Auth for the ProCurve APs**
- **Pros and cons**
- **Configuration**

Comparing security options

Summary

Rev. 8.21

Pre-study Guide: 84

54

The next section describes Web-Auth, an authentication method used for:

- Companies that must provide limited access to guests
- Stations that do not support 802.1X
- Authentication through a familiar Web browser interface

Web-Auth Uses

Web-Auth Uses



- Web-Auth:
 - Authenticates users without 802.1X support
 - Authenticates users without special configuration
 - Allows unauthenticated users limited network access
- Web-Auth is typically used for:
 - Guest access
 - Courtesy or public networks
 - Small-to-medium businesses

Wireless network access used to be a perk. Today, however, users expect it. Now, in addition to accommodating regular employees, you probably need to provide wireless access for relative strangers as well. More and more customers and other guests clamor for services such as Internet access, and if you do not give it to them, someone else will.

In these situations, you cannot be sure that all users' stations will support 802.1X or particular EAP methods. You cannot help the users configure their stations correctly to complete the authentication. On the other hand, you cannot simply open your wireless network to anyone with a wireless NIC.

Web-Auth is one solution for this type of network access. Web-Auth makes it easy for users to connect to the Internet with a minimum of hassle.

Web-Auth Pros and Cons

Web-Auth Pros and Cons



Method	Pros	Cons
Web-Auth	<ul style="list-style-type: none"> • No need for 802.1X or special configuration on stations • Limited access for unauthenticated users 	<ul style="list-style-type: none"> • No requirement for encryption, although it is supported on some wireless devices • User interface required on the station

Rev. 8.21

Pre-study Guide: 86

56

Pros of Web-Auth

Security solutions such as WPA/WPA2 require specific capabilities, but any station can authenticate on a WLAN that uses Web-Auth as long as the user has a legitimate username and password and a Web browser.

Web-Auth also allows you to open parts of your network to guests by providing limited access to unauthenticated users. Choose Web-Auth when you want to provide limited network rights or simple Internet access to the public. For example, suppose your company is a retail store with wireless network access for managers and support staff. Customers, however, can bring their own devices and reach a Web page that provides information about products and upcoming promotions.

Other environments with external users who may benefit from Web-Auth include:

- Hospitals
- Universities
- Cafés, libraries, hotels, airports, and other businesses that provide courtesy wireless networks

Cons of Web-Auth

Web-Auth does not require encryption although encryption is an option on some wireless devices. For example, the ProCurve AP 530 and the Wireless Edge Services Module both support encryption as an option for Web-Auth WLANs.

Because Web-Auth requires interaction with the user, you cannot use it to authenticate stations or devices without a user interface.

Discussion Topics

Discussion Topics



- ✓ *Overview*
- ✓ *MAC authentication (MAC-Auth)*
- ✓ *WEP key as authentication (static WEP)*
- ✓ *802.1X*
- ✓ *WPA/WPA with preshared keys (WPA/WPA2-PSK)*
- ✓ *Web-Authentication (Web-Auth)*

Comparing security options

Summary

The next section compares all of the security options discussed, considering the benefits and costs each brings to particular environments.

Comparing Security Options

Comparing Security Options



Method	Authentication	Encryption	Management	Requirements
Local MAC-Auth	<ul style="list-style-type: none"> Easily spoofed Hardware-based 	None (Any can be added)	<ul style="list-style-type: none"> Complex Not scalable 	None
RADIUS MAC-Auth	<ul style="list-style-type: none"> Easily spoofed Hardware-based 	None (Any can be added)	<ul style="list-style-type: none"> Complex Centralized 	RADIUS server
Shared-key static WEP	Easily spoofed	Single easily cracked key	Separate on each AP	Almost all stations support WEP
Open-key static WEP	Easily spoofed if key is cracked	Single easily cracked key	Separate on each AP	Almost all stations support WEP

Rev. 8.21

Pre-study Guide: 89

58

This table and the ones that follow summarize the criteria you should consider when selecting a security option. Of course, you want to maximize security, while simplifying management.

Authentication

MAC addresses and WEP keys can be used for authentication credentials, but they are easily spoofed.

Encryption

Stronger encryption ciphers lead to stronger encryption. However, another important consideration is key management: How often is the same key reused? How are keys distributed?

Relying on static, frequently re-used keys, shared-key WEP and open-key WEP are quite insecure. MAC-Auth uses whatever type of encryption you configure for the WLAN, whether it is strong WPA, weaker WEP, or none at all. By itself, however, MAC-Auth provides no encryption at all.

Management

Wireless security usually requires user accounts or other security settings that must be coordinated between authentication servers and the supplicants (running on the wireless stations). The best solutions offer centralized management of these accounts. One of the disadvantages of MAC-Auth, particularly local MAC-Auth, is the complexity of adding every MAC address in the network to the allow list on every AP.

Static WEP, depending on the number of APs in your network, is rarely manageable enough for you to change the keys as often as necessary. In addition, you must distribute the static keys to every user, whether verbally, on hard copy, or through email—compromising network security every time a user loses the key or tells it to a friend.

Requirements

These, the least secure methods, require the least. The ProCurve AP 420, AP 530, and the Wireless Module support MAC-Auth. MAC-Auth is appealing because it requires nothing, not even a user interface, from the station. (RADIUS MAC-Auth, while easier to manage on multiple APs, requires a RADIUS server.)

Despite its well-publicized shortcomings, WEP is more secure than nothing, and most stations support it. However, most stations now also support the stronger WPA or WPA2 so you should select one of these options, rather than WEP.

Comparing Security Options: Continued

Comparing Security Options: Continued



Method	Authentication	Encryption	Management	Requirements
Dynamic WEP	<ul style="list-style-type: none"> Robust 802.1X User-based 	Securely distributed per-session keys	Centralized	<ul style="list-style-type: none"> RADIUS server* WEP and 802.1X on stations
WPA (with 802.1X)	<ul style="list-style-type: none"> Robust 802.1X User-based 	Securely generated per-frame keys	Centralized	<ul style="list-style-type: none"> RADIUS server* 802.1X on stations Software on stations to support TKIP
WPA2 (with 802.1X)	<ul style="list-style-type: none"> Robust 802.1X User-based 	<ul style="list-style-type: none"> Securely generated per-frame keys Strong AES block cipher 	Centralized	<ul style="list-style-type: none"> RADIUS server* 802.1X on stations Special hardware on stations to support AES

*The Wireless Module and AP 530 have an internal RADIUS server.

Rev. 8.21

Pre-study Guide: 91

59

This table displays options that feature the stronger security provided by 802.1X authentication.

Authentication

The most secure authentication method and the method best suited for enterprise settings, 802.1X requires each user to authenticate. The exact level of security depends on the EAP methods supported on your RADIUS servers and stations.

Security methods that use 802.1X authentication offer centralized management through a RADIUS server. Products such as ProCurve Identity Driven Manager (IDM) help you to configure network rights for user accounts.

Encryption

Dynamic WEP relies on securely generated session keys. Even with WEP's relatively weak encryption, frequent key rotation shortens a key's lifetime to the point that successful attacks are much rarer.

WPA and WPA2 both provide secure per-frame keys. Now the primary differences in security originate in the type of encryption algorithm. WPA2, which requires support for AES counter mode, provides greater security than WPA with TKIP.

Management

Dynamic WEP and WPA/WPA2 with 802.1X offer centralized management on a RADIUS server (or on a RADIUS server through IDM).

Requirements

All security solutions that use 802.1X require:

- An EAPOL-compliant RADIUS server
- 802.1X support on stations

If your network meets these requirements, you should typically configure WPA. You can also use the Wireless Module's or the AP 530's internal RADIUS server to meet the first requirement.

The greatest barrier to adopting WPA/WPA2, with all its benefits, is ensuring that all stations support the associated encryption. TKIP support requires a software upgrade for older stations, while AES might require special hardware for complex calculations. However, most stations support WPA or WPA2 by default.

Comparing Security Options: Continued

Comparing Security Options: Continued



Method	Authentication	Encryption	Management	Requirements
WPA-PSK	Same key for all users	Securely generated per-frame keys	Separate on each AP	Software on stations to support TKIP
WPA2-PSK	Same key for all users	<ul style="list-style-type: none"> Securely generated per-frame keys Strong AES block cipher 	Separate on each AP	Special hardware on stations to support AES
Web-Auth	User-based	<ul style="list-style-type: none"> Optional 	Centralized	<ul style="list-style-type: none"> RADIUS server Web server (optional)

Rev. 8.21

Pre-study Guide: 93

60

This table lists security options that do not use WEP or 802.1X.

Authentication

For WPA-PSK and WPA2-PSK, authentication is the weakest link. Any password shared among many users is prone to leaks.

Web-Auth offers user-based authentication (albeit of a type less secure than many forms of 802.1X).

Encryption

WPA-PSK and WPA2-PSK offer many of the advantages of WPA and WPA2—with less flexible, secure authentication—for networks without a RADIUS server. WPA-PSK's per-frame keys ultimately originate in a preshared key rather than a unique key for each station. However, both TKIP's key mixing algorithm and CCMP/AES's counter mode reduce the affect of sharing the PMK between stations.

Encryption is not required for Web-Auth, although many wireless devices support it as an option.

Management

With WPA-PSK, you must configure the same key separately on each AP and station; Web-Auth, on the other hand, offers centralized management for user accounts.

Requirements

WPA-PSK and WPA2-PSK do not require a RADIUS server—an advantage for companies that have not implemented such a server. However, stations must still support either TKIP or CCMP/AES's more intensive calculations. (The AP 430, AP 530, and Wireless Module support both TKIP and CCMP/AES. New wireless NICs support either or both of these protocols by default.)

Web-Auth, like 802.1X, requires a RADIUS server; however, the server does not have to be EAP- or EAPOL-compliant.

Summary

Summary



- MAC-Auth
- Static WEP
- 802.1X, including EAP methods
- Dynamic WEP
- WPA and WPA2
- WPA-PSK and WPA2-PSK
- Web-Auth

Rev. 8.21

Pre-study Guide: 95

61

This guide has discussed the three requirements for wireless security—authentication, encryption, and integrity checks—and the many security options developed to meet these requirements on a wireless network.

You should now be able to weigh each security option's relative benefits and costs and select an option that meets your network's requirements.

You have learned about:

- MAC-Auth
- Static WEP
- 802.1X, including EAP methods
- Dynamic WEP
- WPA and WPA2
- WPA-PSK and WPA2-PSK
- Web-Auth



To find out more about ProCurve Networking products and solutions, visit our web site at www.procurve.com

© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.