

FAQ on Cisco Aironet Wireless Security

Document ID: 68583

Questions

Introduction

General FAQ

Troubleshooting and Design FAQ

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides information on the most frequently asked questions (FAQ) about Cisco Aironet Wireless Security.

General FAQ

Q. What is the need for Wireless Security?

A. In a Wired network, data remains in the cables that connect the end devices. But Wireless networks transmit and receive data through a broadcast of RF signals into the open air. Because of the broadcast nature that WLANs use, there is a greater threat of hackers or intruders who can access or corrupt the data. In order to alleviate this problem, all WLANs require the addition of:

1. User authentication to prevent unauthorized access to network resources.
2. Data privacy to protect the integrity and privacy of transmitted data.

Q. What are the different authentication methods that the 802.11 standard for Wireless LANs defines?

A. The 802.11 standard defines two mechanisms for authentication of Wireless LAN clients:

1. Open Authentication
2. Shared Key Authentication

There are two other commonly-used mechanisms as well:

1. SSID-based Authentication
2. MAC address Authentication

Q. What is Open Authentication?

A. Open Authentication is basically a null authentication algorithm, which means that there is no verification of the user or machine. Open Authentication allows any device that places an authentication request to the access point (AP). Open Authentication uses clear-text transmission to allow a client to associate to an AP. If no encryption is enabled, any device that knows the SSID of the WLAN can gain access into the network. If Wired Equivalent

Privacy (WEP) is enabled on the AP, the WEP key becomes a means of access control. A device that does not have the correct WEP key cannot transmit data through the AP even if authentication is successful. Neither can such a device decrypt data that the AP sends.

Q. What steps does Open Authentication involve for a client to associate with the AP?

1. The client sends a probe request to the APs.
2. The APs send back probe responses.
3. The client evaluates the AP responses and selects the best AP.
4. The client sends an authentication request to the AP.
5. The AP confirms authentication and registers the client.
6. The client then sends an association request to the AP.
7. The AP confirms the association and registers the client.

Q. What are the advantages and disadvantages of Open Authentication?

A. Here are the advantages and disadvantages of Open Authentication:

Advantages: Open Authentication is a basic authentication mechanism, which you can use with Wireless devices that do not support the complex authentication algorithms. Authentication in the 802.11 specification is connectivity-oriented. By design the requirements for authentication allow devices to gain quick access to the network. In such a case, you can use Open Authentication.

Disadvantages: Open Authentication provides no way to check if a client is a valid client and not a hacker client. If you do not use WEP encryption with Open Authentication, any user who knows the SSID of the WLAN can access the network.

Q. What is Shared Key Authentication?

A. Shared Key Authentication works similar to Open Authentication with one major difference. When you use Open Authentication with WEP encryption key, the WEP key is used to encrypt and decrypt the data, but is not used in the authentication step. In Shared Key Authentication, WEP encryption is used for authentication. Like Open Authentication, Shared Key Authentication requires the client and the AP to have the same WEP key. The AP that uses Shared Key Authentication sends a challenge text packet to the client. The client uses the locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request. If the AP can decrypt the authentication request and retrieve the original challenge text, the AP responds with an authentication response that grants access to the client.

Q. What steps does Shared Key Authentication involve for a client to associate with the AP?

1. The client sends a probe request to the APs.
2. The APs send back probe responses.
3. The client evaluates the AP responses and selects the best AP.
4. The client sends an authentication request to the AP.
5. The AP sends an authentication response that contains the unencrypted challenge text.
6. The client encrypts the challenge text with the WEP key and sends the text to the AP.

7. The AP compares the unencrypted challenge text with the encrypted challenge text. If the authentication can decrypt and retrieve the original challenge text, authentication is successful.

Shared Key Authentication uses WEP encryption during the client association process.

Q. What are the advantages and disadvantages of Shared Key Authentication?

A. In Shared Key Authentication, the client and the AP exchange the challenge text (clear text) and the encrypted challenge. Therefore, this type of authentication is vulnerable to man-in-the-middle attack. A hacker can listen to the unencrypted challenge and the encrypted challenge, and extract the WEP key (shared key) from this information. When a hacker knows the WEP key, the whole authentication mechanism is compromised and the hacker can access the WLAN network. This is the major disadvantage with Shared Key Authentication.

Q. What is MAC Address Authentication?

A. Although the 802.11 standard does not specify MAC Address Authentication, WLAN networks commonly use this authentication technique. Hence, most of the Wireless device vendors, including Cisco, support MAC Address Authentication.

In MAC Address Authentication, clients are authenticated based on their MAC address. The MAC addresses of the clients are verified against a list of MAC addresses stored locally on the AP or on an external authentication server. MAC authentication is a stronger security mechanism than the Open and Shared Key Authentications that 802.11 provides. This form of authentication further reduces the likelihood of unauthorized devices that can access the network.

Q. Why does MAC authentication not work with Wi-Fi Protected Access (WPA) in Cisco IOS Software Release 12.3(8)JA2?

A. The only level of security for MAC authentication is to check the MAC address of the client against a list of permitted MAC addresses. This is considered very weak. In earlier Cisco IOS Software releases, you could configure MAC authentication and WPA to encrypt the information. But because WPA itself has a MAC address that checks, Cisco decided not to allow this type of configuration in later Cisco IOS Software releases and decided only to improve security features.

Q. Can I use SSID as a method to authenticate wireless devices?

A. Service Set Identifier (SSID) is a unique, case sensitive, alphanumeric value that WLANs use as a network name. The SSID is a –mechanism that allows logical separation of wireless LANs. The SSID does not provide any data-privacy functions, nor does SSID truly authenticate the client to the AP. The SSID value is broadcast as clear text in Beacons, Probe Requests, Probe responses, and other types of frames. An eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer, for example, Sniffer Pro. Cisco does not recommend that you use the SSID as a method to secure your WLAN network.

Q. If I disable SSID broadcast, can I achieve enhanced security on a WLAN network?

A. When you disable SSID broadcast, SSID is not sent in Beacon messages. However, other frames such as, Probe Requests and Probe Responses still have the SSID in clear text. So you do not achieve enhanced Wireless security if you disable the SSID. The SSID is not designed, nor intended for use, as a security mechanism. In addition, if you disable SSID broadcasts, you can encounter problems with Wi-Fi interoperability for mixed-client deployments. Therefore, Cisco does not recommend that you use the SSID as a mode of security.

Q. What are the vulnerabilities found in 802.11 security?

A. The major vulnerabilities of 802.11 security can be summarized as follows:

- ◆ Weak device-only authentication: Client devices are authenticated, not users.
- ◆ Weak data encryption: Wired equivalent privacy (WEP) has been proven ineffective as a means to encrypt data.
- ◆ No message integrity: The integrity check value (ICV) has been proven ineffective as a means to ensure message integrity.

Q. What is the role of 802.1x authentication in WLAN?

A. In order to address the shortcomings and Security vulnerabilities in the original methods of authentication that the 802.11 standard defines, the 802.1X authentication framework is included in the draft for 802.11 MAC layer security enhancements. The IEEE 802.11 Task Group i (TG1) is currently developing these enhancements. The 802.1X framework provides the link layer with extensible authentication, normally seen only in the higher layers.

Q. What are the three entities that the 802.1x framework defines?

A. 802.1x framework requires these three logical entities to validate the devices on a WLAN network.



1. **Supplicant** The supplicant resides on the Wireless LAN client, and is also known as the EAP client.
2. **Authenticator** The authenticator resides on the AP.
3. **Authentication Server** The authentication server resides on the RADIUS server.

Q. How does a Wireless client authentication occur when I use the 802.1x authentication framework?

A. When the Wireless client (EAP client) becomes active, the Wireless client associates to the AP (authenticator). The client then sends authentication credentials to the AP, which in turn forwards the information to the authentication server. The authentication server validates the

credentials against the user database to determine if the user can be granted access to the network. The authentication server is usually a RADIUS or any other AAA server.

Q. What are the different EAP variants that I can use with the 802.1x authentication framework?

A. The 802.1x framework can use any of these EAP variants.

1. EAP-TLS – Extensible Authentication Protocol Transport Layer Security
2. EAP-FAST – EAP Flexible Authentication via Secured Tunnel
3. EAP-SIM – EAP Subscriber Identity Module
4. Cisco LEAP – Lightweight Extensible Authentication Protocol
5. EAP-PEAP – EAP Protected Extensible Authentication Protocol
6. EAP-MD5 – EAP-Message Digest Algorithm 5
7. EAP-OTP – EAP On-Time Password
8. EAP-TTLS – EAP Tunneled Transport Layer Security

Q. How do I choose an 802.1x EAP method from the different variants available?

A. The most important factor that you must consider is whether the EAP method is compatible with the existing network or not. In addition, Cisco recommends that you choose a method that supports mutual authentication.

Q. What is Cisco LEAP?

A. Lightweight Extensible Authentication Protocol (LEAP) is a Cisco proprietary method of authentication. Cisco LEAP is an 802.1X authentication type for wireless LANs (WLANs). Cisco LEAP supports strong mutual authentication between the client and a RADIUS server through a logon password as the shared secret. Cisco LEAP provides dynamic per-user, per-session encryption keys. LEAP is the least complicated method to deploy 802.1x, and requires only a RADIUS server. Refer to Cisco LEAP for information on LEAP.

Q. How does EAP-FAST work ?

A. EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process. The tunnel establishment relies on a Protected Access Credential (PAC) that EAP-FAST can be provisioned and managed dynamically by EAP-FAST through the authentication, authorization, and accounting (AAA) server (such as the Cisco Secure Access Control Server [ACS] v. 3.2.3). With a mutually authenticated tunnel, EAP-FAST offers protection from dictionary attacks and man-in-the-middle vulnerabilities. Here are the phases of EAP-FAST:

EAP-FAST not only mitigates risks from passive dictionary attacks and man-in-the-middle attacks, but also enables secure authentication based on currently deployed infrastructure.

- ◆ Phase 1: Establish mutually authenticated tunnel Client and AAA server use PAC to authenticate each other and establish a secure tunnel.
- ◆ Phase 2: Perform client authentication in the established tunnel Client sends user name and password to authenticate and establish client authorization policy.
- ◆ Optionally, Phase 0 EAP-FAST authentication infrequently uses this phase to enable the client to be dynamically provisioned with a PAC. This phase generates a

per-user access credential securely between the user and the network. Phase 1 of the authentication uses this per-user credential, known as the PAC.
Refer to Cisco EAP-FAST for more information.

Q. Are there documents on cisco.com which explain how to configure EAP in a Cisco WLAN network?

A. Refer to EAP Authentication with RADIUS Server for information on how to configure EAP authentication in a WLAN network.

Refer to Protected EAP Application Note for information on how to configure PEAP authentication.

Refer to LEAP Authentication with a Local RADIUS server for information on how to configure LEAP authentication.

Q. What is WEP Encryption?

A. WEP stands for Wired Equivalent Privacy. WEP is used to encrypt and decrypt data signals that transmit between WLAN devices. WEP is an optional IEEE 802.11 feature that prevents disclosure and modification of packets in transit and also provides access control for the use of the network. WEP makes a WLAN link as secure as a wired link. As the standard specifies, WEP uses the RC4 algorithm with a 40-bit or 104-bit key. RC4 is a symmetric algorithm because RC4 uses the same key for the encryption and the decryption of data. When WEP is enabled, each radio "station" has a key. The key is used to scramble the data before transmission of the data through the airwaves. If a station receives a packet that is not scrambled with the appropriate key, the station discards the packet and never delivers such a packet to the host.

Refer to Configuring Wired Equivalent Privacy (WEP) for information on how to configure WEP.

Q. What is Broadcast Key Rotation? What is the frequency of Broadcast Key Rotation?

A. Broadcast key rotation allows the AP to generate the best possible random group key. Broadcast key rotation periodically updates all clients capable of key management. When you enable broadcast WEP key rotation, the AP provides a dynamic broadcast WEP key and changes the key at the interval you set. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports non-Cisco wireless client devices or devices that you cannot upgrade to the latest firmware for Cisco client devices. Refer to Enabling and Disabling Broadcast Key Rotation for information on how to configure the broadcast key rotation feature.

Q. What is TKIP?

A. TKIP stands for Temporal Key Integrity Protocol. TKIP was introduced to address the shortcomings in WEP encryption. TKIP is also known as WEP key hashing and was initially called WEP2. TKIP is a temporary solution that fixes WEP's key reuse problem. TKIP uses the RC4 algorithm to perform encryption, which is the same as WEP. A major difference from WEP is that TKIP changes the temporal key every packet. The temporal key changes every packet because the hash value for every packet changes.

Q. Can devices that use TKIP interoperate with devices that use WEP encryption?

A. An advantage with TKIP is that WLANs with existing WEP-based APs and radios can upgrade to TKIP through simple firmware patches. Also, WEP-only equipment still interoperates with TKIP-enabled devices that use WEP.

Q. What is Message Integrity Check (MIC)?

A. MIC is yet another enhancement to address the vulnerabilities in WEP encryption. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters the message and then retransmits the altered message. The receiver does not know that the message is corrupt and not a legitimate one. In order to address this issue, the MIC feature adds a MIC field to the wireless frame. The MIC field provides a frame integrity check that is not vulnerable to the same mathematical shortcomings as the ICV. The MIC also adds a sequence number field to the wireless frame. The AP drops frames received out of order.

Q. What is WPA? How is WPA 2 different from WPA?

A. WPA is a standard-based security solution from the Wi-Fi Alliance that addresses the vulnerabilities in native WLANs. WPA provides enhanced data protection and access control for WLAN systems. WPA addresses all known Wired Equivalent Privacy (WEP) vulnerabilities in the original IEEE 802.11 security implementation and brings an immediate security solution to WLAN networks in both enterprise and small office, home office (SOHO) environments.

WPA2 is the next generation of Wi-Fi security. WPA2 is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA2 implements the National Institute of Standards and Technology (NIST)-recommended Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. WPA2 offers a higher level of security than WPA. WPA2 creates fresh session keys on every association. The encryption keys that WPA2 uses for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key.

Both WPA1 and WPA2 can use either TKIP or CCMP encryption. (It is true that some access points and some clients restrict the combinations, but there are four possible combinations). The difference between WPA1 and WPA2 is in the information elements that get put into the beacons, association frames, and 4-way handshake frames. The data in these information elements is basically the same, but the identifier used is different. The main difference in key handshake is that WPA2 includes the initial group key in the 4-way handshake and the first group key handshake is skipped, whereas WPA needs to do this extra handshake to deliver the initial group keys. Re-keying of the group key happens in the same way. The handshake occurs before the selection and use of the cipher suite (TKIP or AES) for the transmission of user datagrams. During the WPA1 or WPA2 handshake, the cipher suite to use is determined. Once selected, the cipher suite is used for all user traffic. Thus WPA1 plus AES is not WPA2. WPA1 allows for (but often is client side limited) either the TKIP or AES cipher.

For more information on WPA and WPA2, refer to Cisco Wi-Fi Protected Access, WPA2 AND IEEE 802.11I.

Q. What is AES?

A. AES stands for Advanced Encryption Standard. AES offers much stronger encryption. AES uses the Rijndael algorithm, which is a block cipher with 128-, 192-, and 256-bit key support and is much stronger than RC4. For WLAN devices to support AES, the hardware must support AES instead of WEP.

Q. What authentication methods are supported by a Microsoft Internet Authentication Service (IAS) server?

A. IAS supports these authentication protocols:

- ◆ Password Authentication Protocol (PAP)
- ◆ Shiva Password Authentication Protocol (SPAP)
- ◆ Challenge Handshake Authentication Protocol (CHAP)
- ◆ Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- ◆ Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)
- ◆ Extensible Authentication Protocol-Message Digest 5 CHAP (EAP-MD5 CHAP)
- ◆ EAP-Transport Layer Security (EAP-TLS)
- ◆ Protected EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (also known as PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS in the Windows 2000 Server supports PEAP-MS-CHAP v2 and PEAP-TLS when Windows 2000 Server Service Pack 4 is installed. For more information, refer to Authentication Methods for use with IAS .

Troubleshooting and Design FAQ

Q. Are there any best practices to deploy wireless security in an outdoor Wireless LAN?

A. Refer to Best Practices For Outdoor Wireless Security. This document provides information on security best practices to deploy an outdoor Wireless LAN.

Q. Can I use a Windows 2000 or 2003 server with Active Directory for a RADIUS server to authenticate wireless clients?

A. The Windows 2000 or 2003 server with an active directory can work as a RADIUS server. For information on how to configure this RADIUS server, you need to contact Microsoft, because Cisco does not support the windows server configuration.

Q. My site is about to migrate from an open wireless network (350 and 1200 series APs) to a PEAP network. I would like to have both the OPEN SSID (an SSID configured for Open Authentication) and the PEAP SSID (an SSID configured for PEAP Authentication) work on the same AP at the same time. This gives us time to migrate the clients to the PEAP SSID. Is there a way to concurrently host an Open SSID and a PEAP SSID on the same AP?

A. The Cisco APs support VLANs (layer 2 only). This is actually the only way to achieve what you want to do. You need to create two VLANs, (native and your other VLAN). Then

you can have a WEP key for one and no WEP key for another. This way, you can configure one of the VLANs for Open Authentication and the other VLAN for PEAP authentication. Refer to Using VLANs with Cisco Aironet Wireless Equipment if you want to understand how to configure VLANs.

Please note that you need to configure your switches for dot1Q and for inter VLAN routing, your L3 switch or your router.

Q. I want to set up my Cisco AP 1200 VxWorks to have the wireless users authenticate to a Cisco 3005 VPN concentrator. What configuration needs to be present on the AP and the clients to accomplish this?

A. There is no specific configuration necessary on the AP or the clients for this scenario. You must do all the configurations on the VPN concentrator.

Q. I am deploying a Cisco 1232 AG AP. I would like to know the most secure method I can deploy with this AP. I do not have an AAA server and my only resources are the AP and a Windows 2003 domain. I am familiar with how to use static 128-bit WEPs keys, non-broadcast SSID and MAC address restrictions. Users mostly work with windows XP workstations and some PDAs. What is the most secure implementation for this setup?

A. If you do not have a RADIUS server like the Cisco ACS, you can configure your AP as a local RADIUS server for LEAP, EAP-FAST or MAC authentication.

Note: A very important point that you must consider is whether you want to use your clients with LEAP or EAP-FAST. If so, your clients must have a utility to support LEAP or EAP-FAST. Windows XP utility only supports PEAP or EAP-TLS.

Q. PEAP authentication fails with the error "EAP-TLS or PEAP authentication failed during SSL handshake". Why?

A. This error can occur due to Cisco bug ID CSCee06008 (registered customers only) . PEAP fails with ADU 1.2.0.4. The workaround for this problem is to use the latest version of the ADU.

Q. Can I have WPA and Local MAC authentication on the same SSID?

A. The Cisco AP does not support local MAC authentication and Wi-Fi Protected Access Pre-share Key (WPA-PSK) in the same Service Set Identifier (SSID). When you enable local MAC authentication with WPA-PSK, WPA-PSK does not work. This problem occurs because local MAC authentication removes the WPA-PSK ASCII password line from the configuration.

Q. We currently have three Cisco 1231 Wireless APs setup with Ciphers 128-bit WEP encryption for our data VLAN. We do not broadcast the SSID. We do not have a separate RADIUS server in our environment.

Someone was able to determine the WEP key through a scanning tool, and used the tool for a couple of weeks to monitor our wireless traffic. How can we prevent this and make the network secure?

A. Static WEP is vulnerable to this issue, and can be derived if a hacker captures enough packets and is able to obtain two or more packets with the same initialization vector (IV).

There are several ways to prevent the occurrence of this issue:

1. Use dynamic WEP keys.
2. Use WPA.
3. If you have only Cisco adapters, enable Per Packet Key and MIC.

Q. If I have two different WLANs, both configured for Wi-Fi Protected Access (WPA)-Pre-Shared Key (PSK), can the pre-shared keys be different per WLAN? If they are different, does it affect the other WLAN configured with a different pre-shared key?

A. The setting of the WPA-PSK should be per WLAN. If you change one WPA-PSK, it should not affect the other WLAN that is configured.

Q. In my environment I use mostly Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), and Cisco Secure Access Control Server (ACS) 3.3 linked to Windows Active Directory (AD) accounts. The problem is when the user password is about to expire, Windows does not prompt the user to change the password. Eventually, the account expires. Is there a solution to make Windows prompt the user to change the password?

A. The Cisco Secure ACS password aging feature enables you to force users to change their passwords under one or more of these conditions:

- ◆ After a specified number of days (age-by-date rules)
- ◆ After a specified number of logins (age-by-uses rules)
- ◆ The first time a new user logs in (password change rule)

For details on how to configure Cisco Secure ACS for this feature, refer to Enabling Password Aging for the CiscoSecure User Database.

Q. When a user logs in wirelessly using LEAP they get their login script to map network drives. However, using Wi-Fi Protected Access (WPA) or WPA2 with PEAP authentication, the login scripts do not run. Both client and access point are Cisco as is the RADIUS (ACS). Why does the login script not run on the RADIUS (ACS)?

A. Machine authentication is mandatory for login scripts to work. This enables the wireless users to gain network access to load scripts before the user logs on.

For information on how to configure machine authentication with PEAP-MS-CHAPv2, refer to Configuring Cisco Secure ACS for Windows v3.2 With PEAP-MS-CHAPv2 Machine

Authentication.

Q. With Cisco Aironet Desktop Utility (ADU) release 3.0, when a user configures machine authentication for Extensible Authentication Protocol–Transport Layer Security (EAP–TLS), ADU does not allow the user to create a profile. Why?

A. This is because of Cisco bug ID CSCsg32032 (registered customers only) . This can happen if the client PC has the machine certificate installed and does not have a user certificate.

The workaround is to copy the machine certificate to the user store, create an EAP–TLS profile and then remove the certificate from the user store for the machine authentication only configuration.

Q. Is there any way to assign VLAN on the Wireless LAN based on client's MAC Address?

A. No. This is not possible. VLAN assignment from RADIUS server only works with 802.1x, not MAC Authentication. You can use RADIUS to push VSAs with MAC authentication, if the MAC addresses are authenticated at the RADIUS server (defined as userid/password in LEAP/PEAP).

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

Related Information

- [Wireless Network Security](#)
- [Wireless LAN Security White Paper](#)
- [Wireless LAN Security Overview](#)
- [Cisco Wi–Fi Protected Access, WPA2 AND IEEE 802.11I](#)
- [EAP–TLS Deployment Guide for Wireless LAN Networks](#)
- [Cisco LEAP](#)
- [Configuring Wired Equivalent Privacy \(WEP\)](#)
- [Wireless Product Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

