Q&A

Extensible Authentication Protocol— Flexible Authentication via Secure Tunneling

This document answers questions about Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), an EAP type from Cisco Systems®.

OVERVIEW

Q. What is EAP-FAST?

A. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a publicly accessible IEEE 802.1X EAP type developed by Cisco Systems®. It is available as an IETF informational draft.

Q. When did Cisco® submit EAP-FAST to the IETF?

A. Cisco submitted the EAP-FAST IETF informational draft on February 8, 2004. It was posted on February 10, 2004. Learn more about IETF or read the informational draft by visiting: http://ietf.org/home.html

Q. Why did Cisco develop EAP-FAST?

A. Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks.

Q. Does EAP-FAST provide protection from network attacks?

A. Yes. EAP-FAST provides protection from a variety of network attacks, including man-in-the-middle, authentication forging, weak IV attack (AirSnort), packet forgery (replay attack), and dictionary attacks.

Q. What customers will deploy EAP-FAST?

A. If an organization is using standards-based wireless LAN (WLAN) security such as Wi-Fi Protected Access (WPA or WPA2), which includes IEEE 802.1X for authentication, and the organization cannot implement strong password policies and does not want to rely on an 802.1X EAP type that requires digital certificates, that organization may choose to deploy EAP-FAST.

Q. Is EAP-FAST standards-based and standards-compliant?

A. EAP-FAST is compliant with IEEE 802.1X and IEEE 802.11i.

Q. Is Cisco EAP-FAST supported by the Cisco Unified Wireless Network?

A. Yes. The Cisco Unified Wireless Network supports a variety of Extensible Authentication Protocol (EAP) authentication types, including EAP-FAST. Like all EAP types, EAP-FAST can be used with WPA and WPA2 networks.

Q. What is the Cisco Unified Wireless Network?

A. The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the WLAN security, deployment, management, and control issues facing enterprises. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The Cisco Unified Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Unified Wireless Network supports an enterprise-ready, standards-based, wireless security solution that gives network administrators' confidence that their data will remain private and secure when they use Cisco wireless products, Cisco Aironet Series products, Cisco Compatible Extensions products or Wi-Fi Certified WLAN client devices. This enterprise-class wireless security solution supports robust wireless LAN security services that closely parallel the security available in a wired LAN. It fulfills the need for consistent, reliable, and secure mobile networking by delivering industry-leading WLAN security services. It mitigates sophisticated passive and active WLAN attacks, interoperates with a range of client devices and provides reliable, scalable, centralized security management. The Cisco Unified Wireless Network allows network administrators to deploy large-scale enterprise WLANs with scalable problem-free security administration that does not increase the burden on the IT staff.

FEATURES AND BENEFITS

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 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:

- **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 username and password to authenticate and establish client authorization policy.
- **Optionally, Phase 0**—This phase is used infrequently to enable the client to be dynamically provisioned with a PAC. During this phase, a per-user access credential is generated securely between the user and the network. This per-user credential, known as the PAC, is used in Phase 1 of EAP-FAST authentication.

Q. What are the main features and benefits of EAP-FAST?

A. EAP-FAST offers the following features and benefits:

- Standards-based:
  - IEEE 802.1X-based EAP type compliant with 802.11i
  - Is not proprietary
- Flexibility:
  - Designed to run on laptops, desktops, personal digital assistants (PDAs), phones, and application-specific devices (ASDs)
- Easy deployment and management:
  - Has an easy-to-use WLAN user GUI configuration with familiar interface
  - Supports Windows single sign on for Cisco Aironet clients and Cisco Compatible clients
  - Supports login script operation with existing Microsoft Active Directory domain
  - Helps enable the use of any user database such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and one-time password (OTP)
  - Does not use certificates, does not require Public Key Infrastructure (PKI) support on client devices
  - Is easily configured and distributed for Cisco Aironet client devices with the Cisco Aironet Configuration Administration Tool
  - Provides for a seamless migration from Cisco LEAP
  - Provides LDAP support with "manual provisioning" (batch-mode installation of client security credentials) available on Cisco Secure ACS 3.2.3 or later, Cisco Aironet, and Cisco Compatible client devices

- Multiple operating system support:
  - Supports Windows 2000, Windows XP, and Windows CE (Power PC 2002, Power PC 2003, and CE.Net 4.2) operating systems
- Advanced security features:
  - Creates a protected tunnel for authentication that mitigates dictionary and man-in-the-middle attacks
  - Provides full support for 802.11i, 802.1X, Temporal Key Integrity Protocol [TKIP] and Advanced Encryption Standard [AES]
  - Supports WPA and WPA2 authenticated key management on Windows XP and Windows 2000 client operating systems
  - Offers the strengths of Protected EAP (PEAP) Version 2 with the ease of deployment and ease of use afforded by Cisco LEAP
  - Supports Cisco Unified Wireless Network
  - Supports wireless domain services (WDS) and fast secure roaming with Cisco Centralized Key Management (CCKM)
  - Supports password expiration or change (Microsoft password change)
  - Supports IEEE 802.1X local authentication service

EAP TYPE COMPARISONS

Q. What are the differences between Protected Extensible Authentication Protocol (PEAP), EAP-FAST, Cisco LEAP, and EAP-Transport Layer Security (EAP-TLS)?

A. Table 1 provides a summary comparison of PEAP, EAP-FAST, Cisco LEAP, and EAP-TLS.

Table 1. PEAP, EAP-FAST, Cisco LEAP and EAP-TLS Comparison Chart

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
User Authentication Database and Server	OTP, LDAP, Novell NDS, Windows NT Domains, Active Directory	Windows NT Domains, Active Directory	Windows NT Domains, Active Directory, LDAP (limited)	Windows NT Domains, Active Directory	OTP, LDAP, Novell NDS, Windows NT Domains, Active Directory
Requires Server Certificates	Yes	Yes	No	No	Yes
Requires Client Certificates	No	No	No	No	Yes
Operating System Support	Driver: Windows XP, Windows 2000, Windows CE* *With third-party utility*: Other OS**	Driver: Windows XP, Windows 2000, Windows CE *With third-party utility*: Other OS**	Driver: Windows XP, Windows 2000, Windows CE*** *With third-party utility*: Other OS**	Driver: Windows 98, Windows 2000, Windows NT, Windows Me, Windows XP, Mac OS, Linux, Windows CE, DOS	Driver: Windows XP, Windows 2000, Windows CE *With third-party utility*: Other OS
Application-Specific Device (ASD) Support	No	No	Yes	Yes	No

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
Credentials Used	Client: Windows, Novell NDS, LDAP password; OTP or token Server: Digital certificate	Windows password	Windows password, LDAP user ID/password (manual provisioning required for Pac provisioning)	Windows password****	Digital certificate
Single Sign-On Using Windows Login	No	Yes	Yes	Yes	Yes
Password Expiration and Change	No	Yes	Yes	No	–
Works with Fast Secure Roaming	No	No	Yes	Yes	No
Works with Wi-Fi Protected Access (WPA) and WPA2	Yes	Yes	Yes	Yes	Yes

* PEAP/GTC is supported on Cisco Compatible Version 2 clients and above.

** Greater operating system coverage is available with Meetinghouse and Funk supplicants.

*** Cisco Aironet 350 Series WLAN client devices and Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapters (CB20A) support EAP-FAST on Windows XP, Windows 2000, and Windows CE operating systems.

**** Requires strong passwords. Read more at: Cisco Response to Dictionary Attacks on Cisco LEAP

Q. Is EAP-FAST a replacement protocol for Cisco LEAP?

A. EAP-FAST is another option for customers deploying IEEE 802.1X EAP networks. Customers can continue to deploy Cisco LEAP in conjunction with a strong password policy. Cisco LEAP offers a widely available, easy-to-deploy, proven authentication method with support for a variety of operating systems. If customers cannot implement a strong password policy, EAP-FAST is an option for them.

Q. How is EAP-FAST different from PEAP?

A. EAP-FAST does not require any server-side certificates and it is easier to deploy, scale, and manage for both wireless and wired networks. Both EAP types support authentication with Microsoft and LDAP databases. PEAP additionally supports OTP databases.

Q. Will Cisco Aironet access points continue to support multiple EAP types?

A. Yes. Cisco Aironet access points will continue to support a variety of EAP types. Cisco Aironet access points currently support Cisco LEAP, EAP-TLS, PEAP GTC, PEAP MS-CHAP v2, EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and now EAP-FAST.

DEPLOYMENT

Q. How do customers migrate from Cisco LEAP to EAP-FAST?

A. Because EAP-FAST does not require client or server certificates, migration from Cisco LEAP to EAP-FAST is simple.

- Client devices—Easy migration from Cisco LEAP to EAP-FAST for Cisco Aironet 350 Series and 5 GHz 54 Mbps (Cisco Aironet CB20A) client adapters is aided by the Cisco Aironet Configuration Administration Tool or the Cisco Aironet Client Administration Utility where IT administrators can define a new profile for EAP-FAST and bundle client configuration, firmware, driver, and Cisco Aironet Client Utility together or use the Cisco Aironet Installation Wizard files. Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter and Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter have built in support for EAP-FAST.
- Access points—Cisco Aironet Series autonomous and lightweight access points that support EAP authentication types have native support for EAP-FAST built in.
- Wireless LAN Controllers—Cisco wireless LAN controllers have built in support for EAP-FAST.
- AAA server—Customers using the Cisco Secure Access Control Server (ACS) need to upgrade to Version 3.2.3 or later to support EAP-FAST.

Q. Can EAP-FAST and Cisco LEAP co-exist on the same VLAN and Service Set Identifiers (SSIDs) during the migration phase?

A. Yes. Virtual LANS (VLANs) can be configured to simultaneously support EAP-FAST and Cisco LEAP.

Q. What Cisco wireless products support EAP-FAST?

A. The following Cisco wireless products support EAP-FAST. Download software at the Cisco Software Center.

- Access points
  - Cisco Aironet 1500 Series lightweight outdoor mesh access point
  - Cisco Aironet 1240AG Series access points running Cisco IOS® Software Version 12.3(7)JA or later
  - Cisco Aironet 1230AG Series and 1130 Series access points running Cisco IOS® Software Version 12.3(2)JA or later
  - Cisco Aironet 1300 Series access point/bridge running Cisco IOS Software Version 12.2(15)JA or later
  - Cisco Aironet 1200 Series, 1100 Series, and 350 Series access points running Cisco IOS Software Version 12.2(11)JA or later
  - Cisco Aironet 1200 Series, 350 Series, and 340 Series access points running VxWorks firmware Version 12.01T or later
  - Cisco Aironet 1000 Series lightweight access points
- Wireless LAN Controllers
  - Cisco 2000, 4100, or 4400 Series wireless LAN controllers
  - Cisco Catalyst® 6500 Series Wireless Services Module (WiSM)
  - Cisco Wireless LAN Controller Module (WLCM) for Integrated Services Routers
- Client devices
  - Cisco Aironet 350 Series and 5 GHz 54 Mbps (Cisco Aironet CB20A) client cards supporting Windows 2000 and Windows XP running Cisco Aironet Windows Installation Wizard Software Release 1.3 or later.
  - Cisco Aironet 350 Series and 5 GHz 54 Mbps (Cisco Aironet CB20A) client cards supporting Windows CE (Power PC 2002, Power PC 2003, and CE.Net 4.2) running Cisco Aironet software release version 2.50 for Windows CE or later
  - Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter
  - Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter
  - Cisco Compatible client devices running Cisco Compatible Extensions Version 3.
- AAA server
  - Cisco Secure ACS Version 3.2.3. or later supports EAP-FAST

Q. Can EAP-FAST be supported by any Wi-Fi vendor?

A. Yes. Because EAP-FAST is an IETF informational draft, any Wi-Fi vendor can use the informational draft to include EAP-FAST support on their products.

Q. Does EAP-FAST support IEEE 802.1X local authentication service?

A. Yes. Cisco Aironet autonomous access points running Cisco IOS Software 12.3(2)JA or later support IEEE 802.1X local authentication service with EAP-FAST. This feature allows a Cisco IOS Software-enabled device to authenticate wireless clients when connectivity to the AAA server is not available. It incorporates an IEEE 802.1X enabled Remote Authentication Dial-In User Service (RADIUS) server that supports EAP authentication types into Cisco IOS Software. This allows the Cisco Aironet autonomous access point to authenticate wireless clients when the WAN link is down or the RADIUS server at the central site is not available. It also provides remote site survivability by allowing an access point to continue to access local resources such as file servers or printers in remote site deployments with non-redundant WAN links.

WLAN SECURITY DOCUMENTS

Q. Where can I learn more about deploying all EAP types?

A. Several wireless security deployment guides are available. Please visit the Cisco Aironet Technical References website to view these documents.

Q. Where can I learn more about deploying secure WLANs?

A. Read the following documents to learn more about deploying secure WLANs:

- Wireless LAN Security White Paper
- Cisco Aironet Technical References

Q. Where can I learn more about WLAN security?

A. Please read the Cisco Wireless LAN Security brochure to learn more about WLAN security.

FOR MORE INFORMATION

For more information about the Cisco wireless security, visit: http://www.cisco.com/go/aironet/security

For more information about Cisco Unified Wireless Network, visit: http://www.cisco.com/go/unifiedwireless

Read the Cisco Wireless LAN Security brochure at:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_brochure09186a00801f7d0b.html

For more information about Cisco Aironet products, visit: http://www.cisco.com/go/aironet

For more information about Cisco Compatible client devices, visit: http://www.cisco.com/go/ciscocompatible/wireless

For more information about Cisco Secure ACS, visit: http://www.cisco.com/go/acs

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**