FIPS 140-2 Security Policy for Cisco 4402 and 4404 Wireless LAN Controllers

Level 2 Validation
Version 1.11
October 3, 2006

This security policy contains these sections:

This document may be freely distributed.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco 4402 and 4404 Wireless LAN Controllers (collectively referred to as *the module*) support Cisco Aironet Lightweight access points operating in Lightweight Access Point Protocol (LWAPP) mode and configured with Wi-Fi Protected Access 2 (WPA2) security. WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i standard.

It automatically detects, authorizes and configures access points, setting them up to comply with the centralized security policies of the wireless LAN. In a wireless network operating in this mode, WPA2 protects all wireless communications between the wireless client and other trusted networked devices on the wired network with AES-CCMP encryption. LWAPP protects all control and bridging traffic between trusted network access points and the module with AES-CCM encryption.

The module supports HTTPS using TLS, LWAPP, WPA2 (802.11i), and RADIUS KeyWrap (using AES key wrapping). HTTPS using TLS uses 1536 bit modulus RSA keys to wrap 128 bit AES symmetric keys, and RADIUS KeyWrap uses 128 bit AES keys as key encrypting keys to wrap AES keys of up to 256 bits. It is a multiple-chip standalone cryptographic module, compliant with all requirements of FIPS 140-2 Level 2. The cryptographic boundary of the module includes all hardware and software. The evaluated platform consists of model numbers 4402 and 4404, with firmware version 3.2.116.21, hardware revision A0 and opacity baffle version 1.0.

In the FIPS mode of operations, the module supports WPA2 (802.11i), HTTPS using TLS, LWAPP and RADIUS KeyWrap for network communications, and uses the following cryptographic algorithm implementations:

- AES (software)
- AES-CCM (software)
- SHA-1 (software)
- HMAC SHA-1 (software)
- FIPS 186-2 Random Number Generator (software)
- RSA signature generation and verification (software)

The module is interoperable with all FIPS 140-2 validated wireless LAN clients that support the ratified IEEE 802.11i standard.

This document details the security policy for the module.

Physical Security Policy

Put tamper evident labels over the service port on the front panel as shown in Figure 1, on the rear panel and the removable cover as shown in Figure 2. Screw the opacity baffle onto the right side of the module, and affix tamper evident labels on the top and bottom as shown in Figure 3 and Figure 4. Figure 5 shows the full cryptographic boundary of the module, which includes the modules case and the opacity baffle.

Figure 1 Placement of Tamper-evident Labels (Front View)

Figure 2 Placement of Tamper-evident Labels (Rear View)

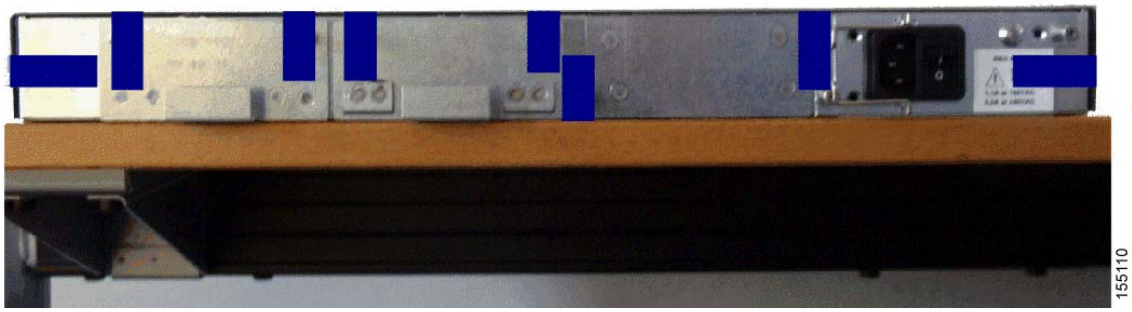

Figure 3 Placement of Opacity Baffle (Top View)

Figure 4 Placement of Opacity Baffle (Bottom View)

Figure 5 Cryptographic Boundary

Caution Due to decreased airflow when using the opacity shield, which is required for FIPS 140-2 validation, the operating temperature of 0º C to 40º C is impacted. When the opacity shield is installed, operating requirements will only be met by deploying the module in a climate control environment of 0º C to 34º C.

Secure Configuration

Initial configuration of the module shall be performed over a local link through the console connection. After the first three steps below, remote access through HTTPS may be used for subsequent configuration. The service port shall not be used to configure the module. For connecting using HTTPS, the Crypto Officer shall configure their web browsers so that only TLS v1.0 is used.

Only the 3.2.116.21 LWAPP software may be loaded on the wireless LAN controllers for distribution to access points.

Follow these steps to prepare the secure configuration for the module:

1. Enable FIPS Mode of Operations
2. Disable Boot Break
3. Configure HTTPS Key
4. Configure Authentication Data
5. Configure RADIUS KeyWrap KEK and MACK Keys
6. Configure Ciphersuites for 802.11i
7. Save and Reboot

Enable FIPS Mode of Operations

The following CLI command places the controller in FIPS mode of operations, enabling all necessary self tests and algorithm restrictions:

```
> config switchconfig fips-prerequisite enable
```

Disable Boot Break

The following CLI command prevents breaking out of the boot process. It must be executed after enabling FIPS mode of operations.

```
> config switchconfig boot-break disable
```

Configure HTTPS Key

The following command configures the controller to use device keys for the HTTPS server. It must be executed after enabling FIPS mode of operations:

```
> config certificate use-device-certificate webadmin
```

Configure Authentication Data

All users shall have a password containing 8 or more characters, including numbers and letters. A crypto officer can use the following CLI command to set user passwords:

```
>config mgmtuser password username password
```

Note that this and all subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document.

Configure RADIUS KeyWrap KEK and MACK Keys

The following CLI commands configure the RADIUS secret and AES-key wrap KEK and MACK:

```
> config radius auth add index ip-address port hex secret
> config radius auth keywrap add hex kek mack index
> config radius auth keywrap enable
```

Configure Ciphersuites for 802.11i

The following CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:

```
> config wlan create index ssid
> config wlan security 802.1x disable index
> config wlan security wpa2 enable index
> config wlan radius_server auth add index radius-server-index
> config wlan enable index
```

Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

```
> save config
> reset system
```

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

The module supports these three roles:

- AP Role—This role is filled by an access point associated with the controller.
- User Role—This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with read-only privileges.

- Crypto Officer (CO) Role—This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module. The product documentation refers to this role as a management user with read-write privileges.

The module does not support a maintenance role.

Services

All services can be viewed by typing **?** from within the appropriate roles. This command shows all the services available to the role currently logged in. The services provided are summarized in Table 1.

Table 1 Module Services

Service	Role	Purpose
Self Test and Initialization	CO	Cryptographic algorithm tests, software integrity tests, module initialization.
System Status	User or CO	The LEDs show the network activity and overall operational status, and the command line status commands output system status.
Key Management	CO	Key and parameter entry, key output, key zeroization.
Module Configuration	CO	Selection of non-cryptographic configuration settings.
LWAPP	AP	Establishment and subsequent data transfer of an LWAPP session for use between the module and the AP.[1]
TLS	CO	Establishment and subsequent data transfer of a TLS session for use between the module and the CO.
802.11i	AP	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point.
RADIUS KeyWrap	Any	Establishment and subsequent receive 802.11i PMK from the RADIUS server.

1. LWAPP uses RSA key wrapping which provides between 80 and 128 bits of effective symmetric key strength.

The module does not support a bypass capability in the approved mode of operations.

Ports and Interfaces

The module has the following physical ports and interfaces:

- Service and Utility Ethernet interfaces. These interfaces are not used in FIPS mode of operations.
- Console serial port
- Two (4402) or four (4404) Small Form-factor Pluggable (SFP) interfaces
- Power port

- LEDs
  - Link and activity indicators for the Ethernet and SFP interfaces
  - PS1/PS2 power supply status indicators. Red indicates a power supply error.
  - Status LED. Green indicates the module is operating normally.
  - Alarm LED. Red indicates a module system error.

User and CO Authentication

When a user first connects to the module through the console port, the module prompts the user to enter a username and password. The user is authenticated based on the password provided. Once the user has been authenticated, the module provides services to that user based on whether they have read-only privileges (the user role) or read-write privileges (the CO role). No characters are output to the terminal when users authenticate. If the incorrect password is entered, the module will re-prompt for the password with the message *Access Denied*.

After the module power cycles, a user must reauthenticate.

The module supports password based authentication for local access via the CLI .

The security policy stipulates that all user passwords must contain 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

AP Authentication

The module performs mutual authentication with an access point through the LWAPP protocol, using an RSA key pair with 1536 bit modulus, which has an equivelent symmetric key strength of 96 bits. An attacker would have a 1 in 2^{96} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $7.9x10^{23}$ attempts per minute, which far exceeds the operational capabilities of the module to support.

Cryptographic Key Management

Cryptographic keys are stored in plaintext form, in flash for long term storage and in SDRAM for active keys. The AES key wrap KEK and AES key wrap MAC keys are input by the CO in plaintext over a local console connection. The PMK is input from the Radius server encrypted with the AES key wrap protocol. RSA public keys are output in plaintext in the form of X.509 certificates. The LWAPP session key is output wrapped with the AP's RSA key, and the TK and GTK are output encrypted with the LWAPP session key. Any keys not explicitly mentioned are not input or output.

Table 2 lists the secret and private cryptographic keys and CSPs used by the module. Table 3 lists the public keys used by the module. Table 4 lists the access to the keys by service.

Table 2 Secret and Private Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description and Zeroization
PRNG seed key	FIPS 186-2	Flash	This is the seed key for the PRNG.
PRNG seed	FIPS 186-2	SDRAM	This is the seed for the PRNG.
User Password	Shared secret	Flash	Identity based authentication data for a user.
bsnOldDefaultIdCert	RSA	Flash	1536-bit RSA private key used to authenticate to the access point, generated during the manufacturing process.
bsnDefaultIdCert	RSA	Flash	1536-bit RSA private key, not used in FIPS mode.
bsnSslWebadminCert	RSA	Flash	1536-bit RSA private key used for HTTPS-TLS, generated during the manufacturing process.
bsnSslWebauthCert	RSA	Flash	1024-bit RSA private key, not used in FIPS mode.
TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new TLS session keys can be created.
TLS Encryption Key	AES	SDRAM	AES key used to encrypt session data.
TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for integrity protection.
LWAPP Session Key	AES-CCM	SDRAM	The session key used to encrypt and integrity check LWAPP traffic.
802.11i Pairwise Master Key (PMK)	Shared secret	SDRAM	The PMK is a secret shared between an 802.11 supplicant and authenticator, and is used to establish the other 802.11i keys.
802.11i Key Confirmation Key (KCK)	HMAC- SHA-1	SDRAM	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.
802.11i Key Encryption Key (KEK)	AES	SDRAM	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.
802.11i Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The PTK, also known as the CCMP key, is the 802.11i session key for unicast communications.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description and Zeroization
AES KeyWrap KEK	AES	Flash	The key encrypting key used by the AES Key Wrap algorithm to protect the PMK for the 802.11i protocol.
AES KeyWrap MACK	AES	Flash	The MAC key used by the AES Key Wrap algorithm to authenticate RADIUS conversation.

Table 3 Public Keys

Name	Algorithm	Storage	Description and Zeroization
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used for LWAPP authentication.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, used to validate the controller's firmware image.
bsnDefaultCaCert	RSA	Flash	Verification certificate, used for LWAPP authentication.
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, used with LWAPP to validate the certificate that authenticates the access point.
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the access point.
cscoDefaultDevCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the access point.
cscoDefaultR3CaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations.
bsnOldDefaultIdCert	RSA	Flash	Authentication certificate, used to authenticate to the access point.
bsnDefaultIdCert	RSA	Flash	Authentication certificate, not used in FIPS mode of operations.
bsnSslWebadminCert	RSA	Flash	Server certificate used for HTTPS-TLS.

Table 4 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG seed
System Status	• None

Table 4 Key/CSP Access by Service

Service	Key Access
Key Management	• None
Module Configuration	• Modify user passwords
LWAPP	• Verify with cscoDefaultNewRootCaCert and cscoDefaultMfgCaCert • Sign with bsnOldDefaultIdCert Private Key • Read (and transmit) bsnOldDefaultIdCert Certificate • Establish and then encrypt/decrypt with LWAPP Session Key
TLS	• Sign with bsnSslWebadminCert Private Key • Read (and transmit) bsnSslWebadminCert Public Key • Establish TLS Pre-Master Key • Establish and then perform cryptographic operations with TLS Encryption Key and TLS Integrity Key
802.11i	• Compute KCK, KEK, and PTK from PMK • Generate GTK • Encrypt/decrypt using KEK • Authenticate data using KCK
RADIUS	• Decrypt 802.11i PMK using KeyWrap KEK • Authenticate data using KeyWrap MACK

Key Zeroization

All keys in the module may be zeroized by entering this CLI command:

```
> config switchconfig key-zeroize controller
```

After this step, power cycle the module and hold down the escape key in order to initiate a memory test that will clear any residual keys from the RAM.

Disallowed Security Functions

These cryptographic algorithms are not approved and may not be used in FIPS mode of operations:

- RC4
- MD5
- HMAC MD5
- 3DES
- AES-CTR

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of AES, AES-CCM, SHA-1, HMAC SHA-1, RNG and RSA algorithms
- Continuous random number generator test for Approved and non-Approved RNGs

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html