FIPS 140-2 Non-Proprietary Security Policy for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961. This policy describes how the Cisco Unified IP Phone 6921, 6941, 6945, and 6961meet the requirements of FIPS 140-2. This document also includes instructions for configuring the phones in FIPS mode.

This policy was prepared as part of the Level 1 FIPS 140-2 validation for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

This document includes the following sections:

- FIPS 140-2 Submission Package
- Overview
- Physical Characteristics and Phone Interfaces
- Roles and Services
- Self-Tests
- Mitigation of Other Attacks
- Secure Operation
- Non-FIPS Approved Algorithms
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the complete submission package contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See Obtaining Technical Assistance for more information.

Overview

Today, more organizations can take advantage of Cisco Unified Communications, thanks to these affordable IP endpoints. The Cisco Unified IP Phones 6921, 6941, 6945, and 6961 deliver cost-effective, full-featured voice communication services in a clutter-free and earth-friendly, ergonomic design. Cisco Unified IP Phones 6921, 6941, 6945, and 6961 endpoints are earth-friendly. They are made with recyclable and reground plastics, so they are earth-responsible solutions. A deep-sleep power option, on select models, reduces power consumption by up to 50 percent in off-work hours, a feature that is good for your company's profitability and good for the planet too.

The Data Sheet for the 6921 can be found on the Cisco website at http://goo.gl/bUerE

Figure 1 - The Cisco Unified IP Phone 6921

The Data Sheet for the 6941 can be found on the Cisco website at http://goo.gl/YNyOj

Figure 2 - The Cisco Unified IP Phone 6941

The Data Sheet for the 6945 can be found on the Cisco website at http://goo.gl/VkjO5

Figure 3 - The Cisco Unified IP Phone 6945

The Data Sheet for the 6961 can be found on the Cisco website at http://goo.gl/9RtmJ

Figure 4 - The Cisco Unified IP Phone 6961

Cryptographic Module Validation Level

Validation Level by Section lists the level of validation for each area in the FIPS PUB 140-2.

Table 1 Validation Level by Section

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1

11	Mitigation of Other Attacks	N/A
	Overall Level	**1**

Physical Characteristics and Phone Interfaces

The logical interfaces and their mapping for the 6921, 6941, 6945, and 6961 Phones are described in Table 2:

Table 2 Cisco 6921, 6941, 6945, and 6961 Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
Phone Keypad, Data Port, Phone Microphone,	Data Input
Phone Speaker, Data Port, Display	Data Output
Phone Keypad, Data Port and Power Port	Control Input
Phone Display, Phone Speaker, message waiting light, LEDs	Status Output

Roles and Services

The 6921, 6941, 6945, and 6961 phones can be accessed by plugging the phones into the network.

As required by FIPS 140-2, there are two main roles in the 6921, 6941, 6945, and 6961 Phones that operators may assume: a Crypto Officer role and User role. The respective services for each role are described in the Crypto Officer Services, and the User Services.

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the phones. For the purposes of this testing, the Crypto Officer will be defined as the operations and processes performed by the Cisco Unified Call Manager (CUCM). The authentication mechanism associated with the Crypto-Officer has not been tested for FIPS level one validation. The Crypto Officer services consist of the following:

- Establish TLS sessions for configuration
- Perform configuration of the phone
- Transport Keys to the phone
- View Status of the phone
- Restart the phone (Restart the connection between the phone and CUCM)
- Reset the phone
- Initiate Self-tests by rebooting the phone.

User Services

A user initializes the phone by turning it on. There is no login interface for the phone, as level 1 allows for implicit role assumptions. Some services may require the menu key to access the features. The services available to the User role consist of the following:

- Make and Receive Calls (Encrypt/Decrypt data)
- Run Self-Tests
- Customize keypad parameters
- View and edit network profile parameters (SSID, DHCP Server, TFTP Server, etc.)
- View and edit system configuration
- View and edit device information (CallManager, Network, HTTP, Locale, QoS, and UI information)
- Display Model Information
- View Phone Status (Phone status, network statistics, call statistics, firmware versions, etc.)

Cryptographic Key Management

The phone uses a variety of Critical Security Parameters during operation. Table 3 lists the cryptographic keys used by Cisco 6921, 6941, 6945, and 6961 phones.

Table 3 Secret and Private Cryptographic Keys Used by Cisco 6921, 6941, 6945, and 6961 phones

#	Key/CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
1	Configuration File AES-128 Key	Generated by the CUCM	Key used to decrypt the configuration file once it is on the phone	Stored in volatile memory	Power Cycle or Device Reset
2	sRTP Master Key (AES)	Generated by the CUCM and sent to phone in TLS session	Key used to generate sRTP session keys	Stored in volatile memory	upon end of call or device reset.
3	sRTP Encryption key (AES)	Generated via the sRTP protocol	Key used to encrypt/decrypt sRTP packets	Stored in volatile memory	upon end of call or device reset.
4	sRTP Authentication key (HMAC)	Generated via the sRTP protocol	Key used to authenticate sRTP packets	Stored in volatile memory	upon end of call or device reset.
5	CUCM TLS Session Encryption key (AES)	Generated via the TLS Protocol	TLS sessions keys based on the Locally Significant Certificate (LSC) for derivation	Stored in volatile memory	upon end of call or device reset.
6	CUCM TLS Session Authentication key (HMAC)	Generated via the TLS Protocol	TLS sessions keys based on the LSC for derivation	Stored in volatile memory	upon end of call or device reset.
7	Webserver TLS Session Encryption key (AES/TDES)	Generated via the TLS Protocol	TLS sessions keys based on the LSC for derivation	Stored in volatile memory	upon end of call or device reset
8	Webserver TLS Session Authentication key (HMAC)	Generated via the TLS Protocol	TLS sessions keys based on the LSC for derivation	Stored in volatile memory	upon end of call or device reset.

9	RNG Seed Key	Multiple data bytes (16-bytes) retrieved from a 32-bytes Hardware based entropy source (time, clock, thermal noise, interrupts, and memory, etc).	Seed Key used to randomize the initialization of the RNG	Stored in volatile memory	Reset or loss of power
10	RNG Seed	Multiple data bytes (16-bytes) retrieved from a 32-bytes Hardware based entropy source (time, clock, thermal noise, interrupts, and memory, etc).	Seed used to randomize the initialization of the RNG	Stored in volatile memory	Reset or loss of power
11	LSC Private Key (RSA)	Generated by the module but converted into a certificate by the CAPF/CUCM (Note that the RSA keys generated must be at least a 1024 bit key)	Private key for locally issued certificates. Used for TLS negotiation with CUCM and Web Clients	/ flash0/sec/lsc0/phone Key.pvt	Zeroized by resetting phone to default settings

The services accessing the Critical Service Parameters (CSPs), the type of access and which role accesses the CSPs are listed in Table 4.

Table 4 Cisco 6921, 6941, 6945, and 6961 Phones Validation Level by Section

CSP/Role/Service Access Policy	Critical Security Parameter	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11
Role/Service												
User Role												
Make and Receive Calls												
Run Self-Tests												

Customize Sound, Display, and keypad parameters												
View and Edit Network Profile Parameters												
View and Edit System Configuration												
View and Edit Device information												
Display Model Information												
View Phone Status												
Crypto-Officer Role												
Establish TLS sessions for configuration		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Perform configuration of the phone		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Transport Keys to the phone		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
View Status of the phone		r	r	r	r	r	r	r	r	r	r	r
Reboot the phone		d	d	d	d	d	d	d	d	d	d	
Reset the phone		d	d	d	d	d	d	d	d	d	d	d
Initiate Self-tests		d	d	d	d	d	d	d	d	d	d	

r = read w = write d = delete

Self-Tests

The 6921, 6941, 6945, and 6961 Phones include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Table 5 6921, 6941, 6945, and 6961 Power-On Self-Tests

Implementation	Tests Performed
TI DSP Library	• AES KAT • HMAC SHA-1 KAT
OpenSSL 0.9.8K	• RSA KAT (signature/verification) • AES KAT • Triple-DES KAT • HMAC SHA-1 KAT • RNG KAT
SMAPI from Broadcom EPT library	• AES KAT • HMAC SHA-1 KAT
Module Firmware	• Firmware Integrity Test

The phone performs all power-on self-tests automatically at boot when FIPS mode is enabled. The power-on self-tests are performed after the cryptographic systems are initialized. In the unlikely event that a power-on self-test fails, the module transitions into an error state and an error message is displayed via status output interface.

.

Table 6 lists the conditional self-tests that the 6921, 6941, 6945, and 6961 phones perform.

Table 6 6921, 6941, 6945, and 6961 Conditional Self-Tests

Implementation	Tests Performed
TI DSP Library	• Conditional Bypass test
OpenSSL 0.9.8K	• Pairwise consistency test for RSA • Continuous Random Number Generator Test for the FIPS-approved RNG
SMAPI from Broadcom EPT library	• Conditional Bypass test

Mitigation of Other Attacks

The 6921, 6941, 6945, and 6961 do not claim to mitigate any attacks in a FIPS-approved mode of operation.

Secure Operation

The Cisco 6921, 6941, 6945, and 6961 phones meet FIPS 140-2 Level 1 requirements. This section describes how to place and keep the phone in a FIPS-approved mode of operation. Operating the phone without maintaining the following settings will remove the phone from the FIPS-approved mode of operation.

Crypto Officer Guidance – System Initialization

The Crypto Officer must create a device security profile in Call manager. Below, find instructions on creating the device security profile.

1. Login to Call Manager
2. Navigate to System -> Security Profile -> Phone Security Profile.
3. Click the Add New button
4. Select “Cisco 6921, 6941, 6945 or 6961” from the drop down box and click next.
5. From the Drop down box, select SCCP for the security protocol profile and click next.
6. In the Name box, give an appropriate name such as “Cisco 6921, 6941, 6945 or 6961 FIPS Security Profile”, or “Cisco 69xx FIPS Security Profile”, followed by an appropriate description.
7. In the section titled, “Phone Security Profile CAPF Information, Select the “Authentication Mode” to be “By Existing Certificate (Precedence to LSC), and select the key size to be 2048 bits.
8. While still in the “Phone Security Profile CAPF Information”, select the device security mode to “encrypted”
9. Click “Save”

Crypto Officer Guidance – System Configuration

The Cisco 6921, 6941, 6945, and 6961 phones were validated with software version 9.2(1)SR1. This is the only allowable image for the FIPS-approved mode of operation. The image names can be found below, in Table 7

Table 7 FIPS Image names

Cisco Unified IP Phone model	Image Name
6921, 6941, and 6961	cmterm-69xx-sccp.9-2-1-0.cop.sgn
6945	cmterm-6945-sccp.9-2-1-0.cop.sgn

The Crypto Officer must configure and enforce the following initialization steps:

Login to Call Manager

- Navigate to phone page
- Select the 6921, 6941, 6945 or 6961 in the list of phones
- Click on the phone in question to navigate to the configuration page.

- Find the section titled “Product Specific Configuration Layout” and make sure that both web access and SSH are disabled
- Find the section titled “Protocol Specific Information” and select the device security profile that you created in the previous section above.
- At the bottom of the list of configuration items, select to enable FIPS mode.
- Save the configurations by clicking on save.
- Reset the phone by clicking reset

Approved Cryptographic Algorithms

The Cisco 6921, 6941, 6945, and 6961 phones support many different cryptographic algorithms; however, when configured for FIPS compliant operation (by following the instructions of this section, the module will only utilize FIPS-approved and FIPS allowed cryptographic algorithms. Table 8 lists all FIPS approved algorithms supported by the module.

Table 8 6921, 6941, 6945, and 6961 Algorithm Certificates

Algorithm	TI DSP Library	OpenSSL Library	SMAPI from Broadcom
AES	1748	1746	1751
Triple-DES	N/A	1131	N/A
SHA-1	1535	1533	1538
HMAC SHA-1	1025	1023	1028
RNG	N/A	930	N/A
RSA	N/A	867	N/A

Non-FIPS Approved Algorithms

The 6921, 6941, 6945, and 6961 implement the following non-FIPS-approved cryptographic algorithms:

- MD5
- MD5 HMAC
- RSA (allowed in FIPS mode for key transport) (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)

Related Documentation

This document deals only with operations and capabilities of the phone in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the phone from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the 6921, 6941, 6945, and 6961 phones.

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

Definition List

AES—Advanced Encryption Standard

CMVP—Cryptographic Module Validation Program

CUCM-Cisco Unified Call Manager

CSP—Critical Security Parameter

DES—Data Encryption Standard

FIPS—Federal Information Processing Standard

HMAC—Hash Message Authentication Code

HTTP—Hyper Text Transfer Protocol

KAT—Known Answer Test

LED—Light Emitting Diode

MAC—Message Authentication Code

NIST—National Institute of Standards and Technology

NVRAM—Non-Volatile Random Access Memory

OSCP—Online Certificate Status Protocol

RAM—Random Access Memory

RNG—Random Number Generator

RSA—Rivest Shamir and Adleman method for asymmetric encryption

SHA—Secure Hash Algorithm

SSL—Secure Sockets Layer

Triple-DES—Triple Data Encryption Standard

TLS—Transport Layer Security

VOIP - Voice over IP Protocol

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.