Product Overview

This chapter contains the following information about the Cisco SIP IP phone:

What is Session Initiation Protocol?

Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between two or more end points.

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* provides the ability to control the attributes of an end-to-end call.

SIP provides the capabilities to:

- Determine the location of the target end point—SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target end point—Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between the end points. Conferences are established using only the media capabilities that can be supported by all end points.
- Determine the availability of the target end point—If a call cannot be completed because the target end point is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target end point was unavailable.
- Establish a session between the originating and target end point—If the call can be completed, SIP establishes a session between the end points. SIP also supports mid-call changes, such as the addition of another end point to the conference or the changing of a media characteristic or codec.
- Handle the transfer and termination of calls—SIP supports the transfer of calls from one end point to another. During a call transfer, SIP simply establishes a session between the transferee and a new end point (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

Note The term *conference* means an established session (or *call*) between two or more end points. In this document, the terms conference and call are used interchangeably.

Components of SIP

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:

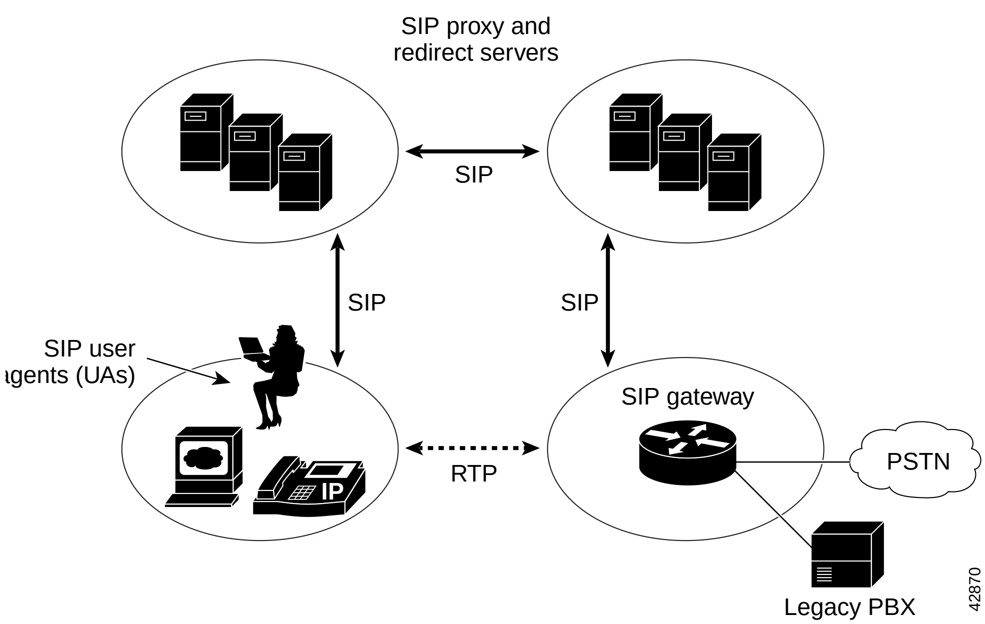
- User agent client (UAC)—A client application that initiates the SIP request.
- User agent server (UAS)—A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

Typically, a SIP end point is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.

From an architecture standpoint, the physical components of a SIP network can also be grouped into two categories: clients and servers. Figure 1-1 illustrates the architecture of a SIP network.

Note In addition, the SIP servers can interact with other application services, such as Lightweght Directory Access Protocol (LDAP) servers, a database application, or an extensible markup language (XML) application. These application services provide back-end services such as directory, authentication, and billing services.

Figure 1-1 SIP Architecture



SIP Clients

SIP clients include:

- Phones—Can act as either a UAS or UAC. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
- Gateways—Provide call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

SIP Servers

SIP servers include:

- Proxy server—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect server—Receives SIP requests, strips out the address in the request, checks its address tables for any other addresses that may be mapped to the one in the request, and then returns the results of the address mapping to the client. Basically, redirect servers provide the client with information about the next hop or hops that a message should take and then the client contacts the next hop server or UAS directly.
- Registrar server—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

What is the Cisco SIP IP Phone?

Cisco SIP IP phones are full-featured telephones that can be plugged directly into an IP network and used very much like a standard private branch exchange (PBX) telephone. The Cisco SIP IP phone is an IP telephony instrument that can be used in VoIP networks.

The Cisco SIP IP phone model terminals can attach to the existing in place data network infrastructure, via 10BaseT/100BaseT interfaces on an Ethernet switch. When used with a voice-capable Ethernet switch (one that understands Type of Service [ToS] bits and can prioritize VoIP traffic), the phones eliminate the need for a traditional proprietary telephone set and key system/PBX.

The Cisco SIP IP phone complies with RFC 2543.

Figure 1-2 illustrates physical features of the Cisco SIP IP phone:

Figure 1-2 Cisco SIP IP Phone Physical Features

- LCD screen—Desktop which displays information about your Cisco SIP IP phone, such as the time, date, your phone number, caller ID, line/call status and the soft key tabs.
- Line or speed dial buttons—Opens a new line or speed dials the number on the LCD screen.
- Footstand adjustment—Adjusts the angle of the phone base.
- Soft keys—Activates the feature described by the text message directly above on the LCD screen.
- Information (***i***) button—Provides online help for selected keys or features and network statistics about the active call. This feature will be available in a future release.
- On-screen mode buttons—Retrieves information about current settings, recent calls, available services, and voice mail messages.
- Volume buttons—Adjusts the volume of the handset, headset, speaker, ringer and adjusts the brightness contrast settings on the LCD screen.
- Function toggles—Includes these options:
  - Headset and speaker—Toggles these functions enabling you to answer the phone using a headset or speakerphone.
  - Mute—Stops or resumes voice transmission.
- Scroll key—Enables you to move among different soft key options displayed on LCD screen.
- Dialing pad—Press the dial pad buttons to dial a phone number. Dial pad buttons work exactly like those on your existing telephone.
- Handset—Lift the handset and press the dial pad numbers to place a call, review voice mail messages, answer a call, and so on.

Supported Features

In addition to the physical features illustrated in Figure 1-2, the Cisco SIP IP phone also provides the following:

- An adjustable ring tone
- A hearing-aid compatible handset
- Headset compatibility
- An integrated two-port Ethernet switch that allows the telephone and a computer to share a single Ethernet jack
- A direct connection to a 10BaseT or 100BaseT Ethernet (RJ-45) network (half- or full-duplex connections are supported)
- A large (4.25 x 3 in.) display with adjustable contrast
- G.711 (u-law and a-law) and G.729a audio compression
- IP address assignment—Dynamic Host Configuration Protocol (DHCP) client or manually configured via a local setup menu
- Ability to:
  - Configure Ethernet port mode and speed
  - Register with or unregister from a proxy server
  - Specify a TFTP boot directory
  - Configure a label for phone identification display purposes
  - Configure a name for caller identification purposes for each active line on a phone
  - Configure a 12- or 24-hour user interface time display
- In-band dual-tone multifrequency (DTMF) support for touch-tone dialing
- Out-of-band DTMF signaling for codecs that do not transport the DTMF signaling correctly (for example, G.729 or G.729A)
- Local or remote (using the SIP 183 Ringing message) call progress tone
- AVT payload type negotiation
- Network startup via DHCP and Trivial File Transfer Protocol (TFTP)
- Dial plan support that enables automatic dialing and automatic generation of a secondary dial tone
- Current date and time support via Simple Network Time Protocol (SNTP) and time zone and daylight savings time support
- Call redirection information support via the CC-Diversion header
- Third-party call control via delayed media negotiation. A delayed media negotiation is one where the Session Description Protocol (SDP) information is not completely advertised in the initial call setup.
- Support for endpoints specified as Fully Qualified Domain Names (FQDNs) in the SDP.
- Local directory configuration (save and recall) and automatic dial completion—Each time a call is successfully made or received, the number is stored in a local directory that is maintained on the phone. The maximum number of entries is 32. Entries are aged-out based on their usage and age. The oldest entry called the least number of times is overwritten first. This feature cannot be programmed by the user, however, up to 20 entries can be “locked” (via the Locked soft key) so that they will never be deleted.

- Message Waiting Indication (via unsolicited NOTIFY)—Lights to indicate that a new voice message is in a subscriber's mailbox. If the subscriber listens to the message but does not save or delete the message, the light remains on. If a subscriber listens to the new message or messages, and saves or deletes them, the light goes off. The message waiting indicator is controlled by the voicemail server. The indication will be saved over a phone upgrade or reboot.
- Speed dial to voicemail via the messages button
- Remote reset support (via the Event header in NOTIFY messages)
- The following call options:
  - Call forward (network)—Allows the Cisco SIP IP phone user to request forwarding service from the network (via a third party tool that enables this feature to be configured). When a call is placed to the user's phone, it is redirected to the appropriate forward destination by the SIP proxy server.
  - Call hold—Allows the Cisco SIP IP phone user (user A) to place a call (from user B) on hold. When user A places user B on hold, the 2-way RTP voice path between user A and user B is temporarily disconnected but the call session is still connected. When user A takes user B off hold, the 2-way RTP voice path is reestablished.
  - Call transfer—Allows the Cisco SIP IP phone user (user A) to transfer a call from one user (user B) to another user (user C). User A places user B on hold and calls user C. If user C accepts the transfer, a session is established between user B and user C and the session between user A and user B is terminated.
  - Three-way calling—Allows a "bridged" 3-way call. When a 3-way call is established, the Cisco SIP IP phone through which the call is established acts as a bridge, mixing the audio media for the other parties.
  - Do not disturb—Allows the user to instruct the system to intercept incoming calls during specified periods of time when the user does not want to be disturbed.
  - Multiple directory numbers—Allows the Cisco SIP IP phone to have up to six directory numbers or lines.
  - Call waiting—Plays an audible tone to indicate that an incoming call is waiting. The user can then put the existing call on-hold and accept the other call. The user can alternate between the two calls.
  - Direct number dialing—Allows users to initiate or receive a call using a standard E.164 number format in a local, national, or international format.
  - Direct URL dialing—Provides the ability to place a call using an email address instead of a phone number.
  - Caller ID blocking—Allows the user to instruct the system to block their phone number or email address from phones that have caller identification capabilities.
  - Anonymous call blocking—Allows the user to instruct the system to block any calls for which the identification is blocked.
- User-defined proxy routing

  The "Route" attribute of the Template tag in the dial plan template file can be used to indicate which proxy (default, emergency, FQDN) that the call should be initially routed to. For example, to configure an emergency proxy, specify value of the "Route" attribute as "emergency".

- Backup SIP proxy

  When the primary proxy does not respond to the INVITE message sent by the Cisco SIP IP Phone after the configured number of retries, the Cisco SIP IP Phone sends the INVITE to the backup proxy. This is independent from which proxy is defined in the "Route" attribute in the dial plan template used.

  The Cisco SIP IP Phone does not have to register with the backup proxy. All interactions, such as authentication challenges, with the backup proxy is treated the same as the interactions with the primary proxy.

  The backup proxy is only used with new INVITE messages. Once the backup proxy is used, it is active for the duration of the call.

  The location of the backup SIP proxy can be defined as an IP address in the default configuration file. See proxy_backup and proxy_backup_port parameters in Modifying the Default SIP Configuration File in Chapter 3, "Managing Cisco SIP IP Phones".

- Emergency SIP proxy

  An optional emergency SIP proxy can be configured with the "Route" attribute of the Template tag in the Dial Plan template file. See "Support of user-defined proxy routing".

  When an emergency SIP proxy is configured and a call is initiated, the phone generates an INVITE message to the address specified in the proxy_emergency parameter. The emergency proxy is used for the call duration.

  The location of the emergency proxy can be defined as an IP address in the default configuration file. See proxy_emergency and proxy_emergency_port parameters in Modifying the Default SIP Configuration File in Chapter 3, "Managing Cisco SIP IP Phones".

  Support of DNS SRV

  DNS SRV is the Domain Name Server RR used to locate servers for a given service.

  SIP on Cisco's SIP IP Phones use DNS SRV query to determine the IP address of the SIP Proxy or the Redirect Server. The query string generated is in compliance with RFC2782, and prepends the protocol label with an underscore "_"; as in "_protocol._transport.". The addition of the underscore reduces the risk of the same name being used for unrelated purposes.

  Also in compliance with RFC 2782 and the draft-ietf-sip-srv-01 spec. is that the system can remember multiple IP addresses and use them properly. In the draft-ietf-sip-srv-01 spec, it is assumed that all proxies returned for the SRV record are equivalent such that the phone can register with any of the proxies and initiate a call using any other proxy.

- Configurable VAD

  VAD can be enabled or disabled with enable_vad parameter. Value 0 for disable, and value 1 for enable. See enable_vad parameter in Modifying the Default SIP Configuration File in Chapter 3, "Managing Cisco SIP IP Phones".

  Three-way conferencing

  Three-way conferencing supports one phone conferencing with two other phones by providing mixing on the initiating phone. To set up a 3-way conference call, see documentation on Making Conference Calls in "Getting Started with the Cisco IP Phone 7960". See Release Note for limitations.

- Distinctive Alerting

  If the INVITE message contains an Alert-Info header, distinctive ringing is invoked, Format of the header is "Alert-info: x". "x" can be any number. This header is only received by the phone and is not generated by the phone.

Distinctive ringing is supported when the phone is idle or during a call. In the idle mode, the phone rings with a different cadence. The selected ringing type plays twice with a short pause in between. In call-waiting mode, two short beeps are generated instead of one long beep.

Note For information on how to use the standard telephony features and URL dialing, refer to the *Getting Started Cisco IP Phone 7960* and *Quick Reference Cisco IP Phone 7960* documents.

Supported Protocols

The Cisco SIP IP phone supports the following standard protocols:

- Domain Name System (DNS)

  DNS is used in the Internet for translating names of network nodes into addresses. SIP uses DNS to resolve the host names of end points to IP addresses.

- Dynamic Host Control Protocol (DHCP)

  DHCP is used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention. If using DHCP, you can connect Cisco SIP IP phones to the network and become operational without having to manually assign an IP address and additional network parameters.

  The Cisco SIP IP phone complies with the DHCP specifications documented in RFC 2131. By default, Cisco SIP IP phones are DHCP-enabled.

- Internet Control Message Protocol (ICMP)

  ICMP is a network layer Internet protocol that enables hosts to send error or control messages to other hosts. ICMP also provides other information relevant to IP packet processing.

  The Cisco SIP supports ICMP as it is documented in RFC 792.

- Internet Protocol (IP)

  IP is a network layer protocol that sends datagram packets between nodes on the Internet. IP also provides features for addressing, type-of-service (ToS) specification, fragmentation and reassembly, and security.

  The Cisco SIP IP phone supports IP as it is defined in RFC 791.

- Real-Time Transport Protocol (RTP)

  RTP transports real-time data (such as voice data) over data networks. RTP also has the ability to obtain Quality of Service (QoS) information.

  The Cisco SIP IP phone supports RTP as a media channel.

- Session Description Protocol (SDP)

  SDP is an ASCII-based protocol that describes multimedia sessions and their related scheduling information.

  The Cisco SIP IP phone uses SDP for session description.

- Simple Network Time Protocol (SNTP)

  SNTP sychronizes computer clocks on an IP network. The Cisco SIP IP phones use SNTP for their date and time support.

- Trivial File Transfer Protocol (TFTP)

  TFTP allows files to be transferred from one computer to another over a network.

  The Cisco SIP IP phone uses TFTP to download configuration files and software updates.

- User Datagram Protocol (UDP)

  UDP is a simple protocol that exchanges data packets without acknowledgments or guaranteed delivery. SIP can use UDP as the underlying transport protocol. If UDP is used, retransmissions are used to ensure reliability.

  The Cisco SIP IP phone supports UDP as it is defined in RFC 768 for SIP signaling.

Prerequisites

For the Cisco SIP IP phone to successfully operate as a SIP endpoint in your network, your network must meet the following requirements:

- A working IP network is established.

  For more information about configuring IP, refer to *Cisco IOS IP and IP Routing Configuration Guide*.

- VoIP is configured on your Cisco routers.

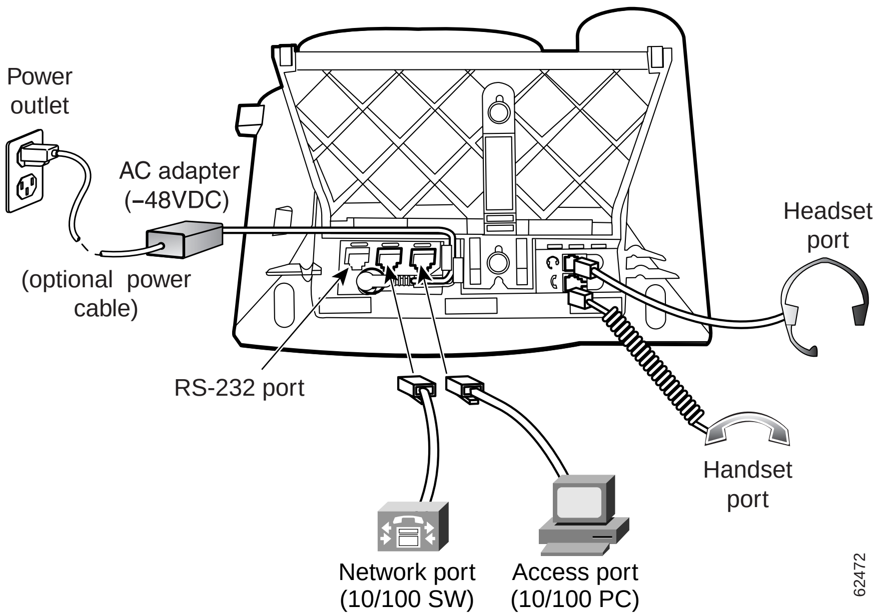
  For more information about configuring VoIP, refer to the *Cisco IOS Release 12.1 Multiservice Applications Configuration Guide* for the appropriate access platform. For more information about configuring SIP VoIP, refer to the *Enhancements to SIP for VoIP on Cisco Access Platforms*.

- VoIP gateways are configured for SIP.
- A TFTP server is active and contains the latest Cisco SIP IP phone firmware image in its root directory.
- A proxy server is active and configured to receive and forward SIP messages.

Cisco SIP IP Phone Connections

The Cisco SIP IP phone has connections for connecting to the data network, for providing power to the phone, and for connecting a headset to the phone. Figure 1-3 illustrates the connections on the Cisco SIP IP phone.

Figure 1-3 Cisco SIP IP Phone Cable Connections



Connecting to the Network

The Cisco SIP IP phone has two RJ-45 ports that each support 10/100 Mbps half- or full-duplex Ethernet connections to external devices—network port (labeled 10/100 SW) and access port (labeled 10/100 PC). You can use either Category 3 or 5 cabling for 10 Mpbs connections, but use Category 5 for 100 Mbps connections. On both the network port and access port, use full-duplex mode to avoid collisions.

Network Port (10/100 SW)

Use the network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from the Cisco Catalyst switch over this connection. See the "Connecting to Power" section on page 1-10 for details.

Access Port (10/100 PC)

Use the access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Connecting to Power

The Cisco SIP IP phone can be powered by the following sources:

- External power source—Optional Cisco AC adaptor and power cord for connecting to a standard wall receptacle.
- WS-X6348-RJ45V 10/100 switching module—Provides inline power to the Cisco SIP IP phone when connected to a Catalyst 3500, 4000, or 6000 family 10/100BaseTX switching module.

  This module sends power on pins 1 & 2 and 3 & 6.

- WS-PWR-PANEL—Power patch panel provides power to the Cisco SIP IP phone which allows the Cisco SIP IP phone to be connected to existing Catalyst 4000, 5000, and 6000 family 10/100BaseTX switching modules.

  This module sends power on pins 4, 5, 7, and 8.
- WS-X4148-RJ45V—48 port 10/100 Ethernet with inline power module for the Catalyst 4006.
- WS-X4095-PEM—VoIP DC Power Entry module for the Catalyst 4006.
- WS-X4608-2PSU and WS-X4608—External -48V DC power shelf common equipment for the Catalyst 4006 with two AC-to-DC PSUs and one empty bay for redundant option and the 110V 15A AC-to48V DC PSU redundant option for the power shelf
- WS-C3524-PWR-XL-EN—Catalyst 3524-PWR XL switch

Note Only the network port (labeled 10/100 SW) supports inline power from the Cisco Catalyst switches.

For redundancy, you can use the Cisco AC adapter even if you are using inline power from the Cisco Catalyst switches. The Cisco SIP IP phone can share the power load being used from the inline power and external power source. If either the inline power or the external power goes down, the phone can switch entirely to the other power source.

To use this redundancy feature you *must* set the inline power mode to auto on the Cisco Catalyst switch. Next, connect the un-powered Cisco SIP IP phone to the network. After the phone powers up, connect the external power supply to the phone.

Using a Headset

The Cisco SIP IP phone supports a four or six-wire headset jack. Specifically, the Cisco SIP IP phone supports the following Plantronics headset models:

- Tristar Monaural
- Encore Monaural H91
- Encore Binaural H101

The Volume and Mute controls will also adjust volume to the earpiece and mute the speech path of the headset. The headset activation key is located on the front of the Cisco SIP IP phone.

Note When using a headset, an amplifier is not required. However, a coil cord is required to connect the headset to the headset port on the back of your Cisco IP Phone 7960. For information on ordering compatible headsets and coil cords for the Cisco IP phone 7960, see http://cisco.getheadsets.com or http://vxicorp.com/cisco.

The Cisco SIP IP Phone with a Catalyst Switch

To function in the IP telephony network, the Cisco SIP IP phone must be connected to a networking device, such as a Catalyst switch, to obtain network connectivity.

The Cisco SIP IP phone has an internal Ethernet switch, which enables it to switch traffic coming from the phone, access port, and the network port.

If a computer is connected to the access port, packets traveling to and from the computer and to and from the phone share the same physical link to the switch and the same port on the switch.

This configuration has these implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis, and additional IP addresses might not be available to assign the phone to a port so that it belongs to the same subnet as other devices (PC) connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN on each of the ports connected to a phone. The switch port configured for connecting a phone would have separate VLANs configured for carrying:

- Voice traffic to and from the Cisco SIP IP phone (auxiliary VLAN)
- Data traffic to and from the PC connected to the switch through the access port of the Cisco SIP IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses.

For more information, refer to the documentation included with the Cisco Catalyst switch.