CHAPTER 4

Configuring the Cisco VoIP Infrastructure Solution for SIP

This chapter provides scenario-based examples of how to configure the components of the Cisco VoIP Infrastructure Solution for SIP. It includes the following sections:

Configuring the Routers

Before you can configure your access server or router to use VoIP, you must first complete the following tasks:

- Install the voice feature card (VFC) or a voice network module (VNM) into the appropriate bay of your Cisco access server or router. For more information about the physical characteristics and capacity, memory requirements, or installation instructions for the VNM or VFC, refer to the installation documentation supplied with your VNM or VFC.
- Complete basic configuration for your router or access server. For more information about these basic configuration tasks, refer to the software installation and configuration guide that shipped with your device. For more information about configuring IP, refer to the "IP Overview," "Configuring IP Addressing," and "Configuring IP Services" chapters in the *Cisco IOS IP and IP Routing Configuration Guide*.
- Complete your company dial plan.
- Establish a working telephony network based on your company dial plan.

- Integrate your dial plan and telephony network into your existing IP network topology. How you merge your IP and telephony networks depends on your particular network topology. In general, we recommend the following suggestions:
  - Use canonical numbers wherever possible. It is important to avoid situations where numbering systems are significantly different on different routers or access servers in your network.
  - Make routing or dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.
- Contact your PBX vendor for instructions about how to reconfigure the appropriate PBX interfaces.
- For each Cisco AS5300 access server installed in your solution that will connect to the Cisco SS7 Interconnect for Voice Gateway Solution, configure the access gateway by performing the tasks listed in the "Configuring the Cisco AS5300 Universal Access Server" section on page 4-27.

Configuring VoIP Support

After you have configured your router or access server for basic IP support, you are ready to configure the device to support VoIP. To configure basic VoIP, perform the following tasks:

- Configure IP networks for real-time voice traffic (required)
- Configure VoIP over Frame Relay (optional)
- Configure analog voice ports (required)
- Configure digital voice ports (required)
- Configure dial peers (required)
- Configure number expansion (optional)
- Optimize dial peer and network interface configurations (optional)
- Simulate a trunk connection (optional)

Note For complete information about configuring VoIP, see the "Configuring Voice over IP" chapter of the *Cisco IOS Multiservice Applications Configuration Guide*.

Configuring the Cisco SIP Gateway

After you have configured the basic VoIP support, you must configure the router or access server to function as a Cisco SIP gateway. To configure SIP support, perform the following tasks:

- Configure the session transport type to use SIP across all dial peers.
- Configure each dial peer as follows:
  - Specify **sipv2** as the session protocol type.
  - Specify the global SIP server as the session target.

Note Cisco Systems VoIP routers support a standard numbering scheme. This scheme complies to the ITU-T E.164 recommendations. For example, in North America, the North American Numbering Plan (NANP) is used, which consists of an area code, an office code, and a station code. Area codes are assigned geographically, office codes are assigned to specific switches, and station codes identify a specific port on that switch. The format in North America is 1Nxx-Nxx-xxxx, where N = digits 2 through 9 and x = digits 0 through 9. Internationally, each country is assigned a one- to three-digit country code; the country's dialing plan follows the country code.

However, by default, the SIP gateway tags called numbers that have 11 or more digits as “unknown” when sending SETUP messages to the PSTN switch.

To accommodate such situations, you must define translation rules on the outbound POTS dial peer to convert the “type of number” to the correct value. Translation rules manipulate the called number digits and the “type of number” value associated with the called digits.

Note For complete information about configuring SIP on your router or access server, see the *Enhancements for the Session Initiation Protocol for VoIP on Cisco Access Platforms* feature documentation for Cisco IOS Software Release 12.1(3)T.

Configuring the Cisco SIP IP Phones

The Cisco SIP IP phones obtain their configuration parameters from network devices during their boot-up process. Network parameters can be configured manually or obtained from a DHCP server. SIP parameters can be configured manually or obtained from a TFTP server.

Before you configure the Cisco SIP IP phones, you should obtain the following files from Cisco’s Connection Online (CCO) and place them in the root directory of your TFTP server:

File	Description
OS79XX.TXT	(Required) Enables the phone to automatically determine and initialize for the VoIP environment in which it is being installed. After downloading this file, you will need to use an ASCII editor to open it and specify the file name (without the file extension) of the image version that you plan to run on your phones.
SIPDefaultGeneric.cnf	(Optional) File in which to configure SIP parameters intended for all phones.
SIPConfigGeneric.cnf	(Required) File which can be used as a template to configure SIP parameters specific to a phone. When customized for a phone, this file must be renamed to the MAC address of the phone.
RINGLIST.DAT	(Optional) Lists audio files that are the custom ring type options for the phones. The audio files listed in the RINGLIST.DAT file must also be in the root directory of the TFTP server.

P0S3*xxyy*.bin (where *xx* is the version number and *yy* is the subversion number)	(Required) The Cisco SIP IP phone firmware image.
dialplan.xml	(Optional) North American example dial plan.
syncinfo.xml	(Optional) Controls the image version and associated sync value to be used for remote reboots.

Note For complete information about configuring the Cisco SIP IP phone, see the *Cisco SIP IP Phone 7960 Administration Guide, Version 2.0.*

Configuring Startup Network Parameters

Network parameters are the parameters that are required for the phone to connect to the network. They can be configured manually or obtained from a DHCP server. We recommend that you use the DHCP server to distribute network parameters.

If you use DHCP to configure the network parameters, ensure that the following DHCP options have been configured on your DHCP server before you connect your Cisco SIP IP phone:

- dhcp option #50 (IP address)
- dhcp option #1 (IP subnet mask)
- dhcp option #3 (Default IP gateway)
- dhcp option #15 (Domain name)
- dhcp option #6 (DNS server IP address)
- dhcp option #66 (TFTP server IP address)

Configuring SIP Parameters

The SIP parameters are the parameters that the IP phone needs to operate in a SIP environment. The firmware image version that the phone should be running is also defined in the configuration file. Each phone must have its own configuration file.

Upon startup or reboot, Cisco SIP IP phones request their configuration files from the TFTP server. If a configuration file is unavailable on the TFTP server, the phone will use the SIP parameters that were last stored in Flash (as described in the “Configuring the Phone's SIP Settings” section of the *Cisco SIP IP Phone 7960 Administration Guide*).

There are two types of configuration files:

- Parameters that are common to all phones can be specified in the default configuration file (SIPDefault.cnf). These parameters can include the image version, the preferred codec, and the address of the proxy server.
- Parameters that are specific to a phone, such as the URL or E.164 number assigned to each line, should be specified in a phone-specific configuration file. The name of the phone-specific configuration file must be SIP*XXXXYYYYZZZZ*.cnf, where *XXXXYYYYZZZZ* is the MAC address of the phone. All characters in the file name must be capitalized and the extension (.cnf) must be lower case.

Using an ASCII text editor, edit the default configuration file and specify the desired parameters. Then, using an ASCII text editor, create a configuration file for each phone that you plan to install. You can define settings for up to six lines.

The SIP phone system parameters (typically defined in the default configuration file) are as follows:

- **image_version**—Firmware version that the Cisco SIP IP phone should run.

  Enter the name of the image version (as released by Cisco). Do not enter the extension. You cannot change the image version by changing the file name because the version is also built into the file header. Trying to change the image version by changing the file name will cause the firmware to fail when it compares the version in the header against the file name.
- **proxy1_address**—IP address of the primary SIP proxy server that will be used by the phones. Enter this address in IP dotted-decimal notation.
- **proxy1_port**—Port number of the primary SIP proxy server. This is the port on which the SIP client will listen for messages. Default is 5060.
- **tos_media**—Type of Service (ToS) level for the media stream being used. Valid values are:
  - 0 (IP_ROUTINE)
  - 1 (IP_PRIORITY)
  - 2 (IP_IMMEDIATE)
  - 3 (IP_FLASH)
  - 4 (IP_OVERIDE)
  - 5 (IP_CRITIC)

  Default is 5.
- **preferred_codec**—CODEC to use when initiating a call. Valid values are g711alaw, g711ulaw, and g729a. Default is g711ulaw.
- **dtmf_inband**—Whether to detect and generate in-band signaling format. Valid values are 1 (generate DTMF digits in-band) and 0 (do not generate DTMF digits in-band). Default is 1.
- **dtmf_db_level**—In-band DTMF digit tone level. Valid values are:
  - 1 (6 db below nominal)
  - 2 (3 db below nominal)
  - 3 (nominal)
  - 4 (3 db above nominal)
  - 5 (6 db above nominal)

  Default is 3.

- **dtmf_outofband**—Whether to generate the out-of-band signaling (for tone detection on the IP side of a gateway) and if so, when. The Cisco SIP IP phone supports out-of-bound signaling via the AVT tone method. Valid values are:
  - none—Do not generate DTMF digits out-of-band.
  - avt—If requested by the remote side, generate DTMF digits out-of-band (and disable in-band DTMF signaling), otherwise, do not generate DTMF digits out-of-band.
  - avt_always—Always generate DTMF digits out-of-band. This option disables in-band DTMF signaling.

  Default is avt.
- **dtmf_avt_payload**—Payload type for AVT packets. Possible range is 96 to 127. If the value specified exceeds 127, the phone will default to 101.
- **timer_t1**—Lowest value (in milliseconds) of the retransmission timer for SIP messages. The valid value is any positive integer. Default is 500.
- **timer_t2**—Highest value (in milliseconds) of the retransmission timer for SIP messages. The valid value is any positive integer greater than timer_t1. Default is 4000.
- **timer_invite_expires**—The amount of time, in seconds, after which a SIP INVITE will expire. This value is used in the Expire header field. The valid value is any positive number, however, we recommend 180 seconds. Default is 180.
- **sip_retx**—Maximum number of times a SIP message other than an INVITE request will be retransmitted. The valid value is any positive integer. Default is 10.
- **sip_invite_retx**—Maximum number of times an INVITE request will be retransmitted. The valid value is any positive integer. Default is 6.
- **proxy_register**—Whether the phone must register with a proxy server during initialization. Valid values are 0 and 1. Specify 0 to disable registration during initialization. Specify 1 to enable registration during initialization. Default is 0.

  After a phone has initialized and registered with a proxy server, changing the value of this parameter to 0 will unregister the phone from the proxy server. To re-initiate a registration, change the value of this parameter back to 1.

  Note If you enable registration, and authentication is required, you must specify values for the line*x*_authname and line*x*_password parameters (where *x* is a number 1 through 6) in the phone-specific configuration file.

- **timer_register_expires**—The amount of time, in seconds, after which a REGISTRATION request will expire. This value is inserted into the Expire header field. The valid value is any positive number, however, we recommend 3600 seconds. Default is 3600.
- **messages_uri**—Number to call to check voice mail. This number will be called when the **Messages** key is pressed.
- Date, Time, and Daylight Savings Time parameters:
  - **sntp_mode**—Mode in which the phone will listen for the SNTP server.
  - **sntp_server**—IP address of the SNTP server from which the phone will obtain time data.
  - **time_zone**—Time zone in which the phone is located.
  - **dst_offset**—Offset from the phone’s time when DST is in effect.
  - **dst_start_month**—Month in which DST starts.

  - **dst_start_day**—Day of the month on which DST begins.
  - **dst_start_day_of_week**—Day of the week on which DST begins.
  - **dst_start_week_of_month**—Week of month in which DST begins.
  - **dst_start_time**—Time of day on which DST begins.
  - **dst_stop_month**—Month in which DST ends.
  - **dst_stop_day**—Day of the month on which DST ends.
  - **dst_stop_day_of_week**—Day of the week on which DST ends.
  - **dst_stop_week_of_month**—Week of month in which DST ends.
  - **dst_stop_time**—Time of day on which DST ends.
  - **dst_auto_adjust**—Whether or not DST is automatically adjusted on the phones.
- **dnd_control**—Whether the Do Not Disturb feature is enabled or disabled by default on the phone or whether the feature is permanently enabled. When the feature is permanently enabled, a phone is a “call out” phone only. When the Do Not Disturb feature is turned on, the phone will block all calls placed to the phone and log those calls in the Missed Calls directory. Valid values are:
  - **0**—The Do Not Disturb feature is off by default, but can be turned on locally via the phone’s user interface.
  - **1**—The Do Not Disturb feature is on by default, but can be turned off locally via the phone’s user interface.
  - **2**—The Do Not Disturb feature is off permanently and cannot be turned on and off locally via the phone’s user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - **3**—The Do Not Disturb feature is on permanently and cannot be turned on and off locally via the phone’s user interface. This setting sets the phone to be a “call out” phone only. If specifying this value, specify this parameter in the phone-specific configuration file.
- **callerid_blocking**—Whether the Caller ID Blocking feature is enabled or disabled by default on the phone. When enabled, the phone will block its number or email address from phones that have caller identification capabilities. Valid values are:
  - 0—The Caller ID Blocking feature is disabled by default, but can be turned on and off via the phone’s user interface. When disabled, the caller identification is included in the Request-URI header field.
  - 1—The Caller ID Blocking feature is enabled by default, but can be turned on and off via the phone’s user interface. When enabled, “Anonymous” is included in place of the user identification in the Request-URI header field.
  - 2—The Caller ID Blocking feature is disabled permanently and cannot be turned on and off locally via the phone’s user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Caller ID Blocking feature is enabled permanently and cannot be turned on and off locally via the phone’s user interface. If specifying this value, specify this parameter in the phone-specific configuration file.

- **anonymous_call_block**—Whether the Anonymous Call Block feature is enabled or disabled by default on the phone. Valid values are:
  - 0—The Anonymous Call Blocking feature is disabled by default, but can be turned on and off via the phone's user interface. When disabled, anonymous calls will be received.
  - 1—The Anonymous Call Blocking feature is enabled by default, but can be turned on and off via the phone's user interface. When enabled, anonymous calls will be rejected
  - 2—The Anonymous Call Blocking feature is disabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Anonymous Call Blocking feature is enabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
- **tftp_cfg_dir**—Path to the TFTP subdirectory in which phone-specific configuration files are stored.
- **network_media_type**—Ethernet port negotiation mode. Valid values are:
  - Auto—Port is auto-negotiated.
  - Full100—Port is configured to be a full-duplex, 100MB connection.
  - Half100—Port is configured to be a half-duplex, 100MB connection.
  - Full10—Port is configured to be a full-duplex, 10MB connection.
  - Half10—Port is configured to be a half-duplex, 10MB connection.

  Default is Auto.
- **autocomplete**—Whether to have numbers automatically completed when dialing. Valid values are 0 (disable auto completion) or 1 (enable auto completion). Default is 1.
- **sync**—Value against which to compare the value in the syncinfo.xml before performing a remote reboot. Valid value is a character string up to 32 characters long.
- **time_format_24hr**—Whether a 12 or 24-hour time format is displayed by default on the phone's user interface. Valid values are:
  - 0—The 12-hour format is displayed by default but can be changed to a 24-hour format via the phone's user interface.
  - 1—The 24-hour format is displayed by default but can be changed to a 12-hour format via the phone's user interface.
  - 3—The 12-hour format is displayed and cannot be changed to a 24-hour format via the phone's user interface.

The SIP phone-specific parameters (typically defined in the phone-specific configuration file) are as follows:

- **line*x*_name**—Number or e-mail address used when registering. When entering a number, enter the number without any dashes. For example, enter 555-1212 as 5551212. When entering an e-mail address, enter the e-mail ID without the host name.
- **line*x*_shortname**—Name or number associated with the line*x*_name as you want it to display on the phone's LCD if the line*x*_name length exceeds the allowable space in the display area. For example, if the line*x*_name value is the phone number 111-222-333-4444, you can specify 34444 for this parameter to have 3444 display on the LCD instead. Alternately, if the value for the linex_name parameter is the email address "username@company.com", you can specify the "username" to have just the user name appear on the LCD instead.

This parameter is used for display-only purposes. If a value is not specified for this parameter, the value in the line*x*_name variable is displayed.

- **line*x*_authname**—Name used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the line*x*_authname parameter for a line when registration is enabled, the value defined for line 1 is used. If a value is not defined for line 1, the default line1_authname is UNPROVISIONED.
- **line*x*_password**—Password used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the line*x*_password parameter for a line when registration is enabled, the value defined for line 1 is used. If a value is not defined for line 1, the default line1_password is UNPROVISIONED.
- **linex_displayname**—Identification as it should appear for caller identification purposes. For example, instead of jdoe@company.com displaying on phones that have caller ID, you can specify John Doe in this parameter to have John Doe displayed on the callee end instead. If a value is not specified for this parameter, nothing is used.
- **dnd_control**—Whether the Do Not Disturb feature is enabled or disabled by default on the phone or whether the feature is permanently enabled, making the phone a “call out” phone only. When the Do Not Disturb feature is turned on, the phone will block all calls placed to the phone and log those calls in the Missed Calls directory. Valid values are:
  - 0—The Do Not Disturb feature is off by default, but can be turned on locally via the phone’s user interface.
  - 1—The Do Not Disturb feature is on by default, but can be turned off locally via the phone’s user interface.
  - 2—The Do Not Disturb feature is off permanently and cannot be turned on and off locally via the phone’s user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Do Not Disturb feature is on permanently and cannot be turned on and off locally via the phone’s user interface. This setting sets the phone to be a “call out” phone only. If specifying this value, specify this parameter in the phone-specific configuration file.

Note This parameter is best configured in the SIPDefault.dnf file unless configuring a phone to be a “call-out” phone only. When configuring a phone to be a “call-out” phone, define this parameter in the phone-specific configuration file.

- **phone_label**—Label to display on the top status line of the LCD. This field is for end-user display only purposes. For example, a phone’s label can display “John Doe’s phone.” Approximately up to 11 characters can be used when specifying the phone label.

Note For complete information about creating and modifying configuration files, see the *Cisco SIP IP Phone 7960 Administration Guide, Version 2.0.*

Configuring the Cisco SIP Proxy Server

You configure the Cisco SIP Proxy Server by defining directives in a main configuration file. The Cisco SIP Proxy Server main configuration file is sipd.conf. A default sipd.conf configuration file is copied into */usr/local/sip/conf/* when installed on Linux platforms and copied into */opt/sip/conf* on Solaris platforms. This default configuration file should be customized to your environment.

Before beginning any of the configuration tasks in this chapter, change to the directory in which the sipd.conf file is located and open the file using vi or any text editor.

Note For complete information about configuring the Cisco SIP Proxy Server, see the *Cisco SIP Proxy Server Administrator Guide*.

Similar to the Apache Server, the Cisco SIP Proxy Server directives can be grouped into major categories. The major categories of Cisco SIP Proxy Server directives are:

- Server global directives—Define the overall operation of the Cisco SIP Proxy Server.
- Host-specific directives—Define the basic configuration of the main Cisco SIP Proxy Server which will respond to requests that are not handled by a virtual host.

  The term virtual host refers to maintaining more than one server on one machine, as differentiated by their hostname. For example, companies sharing a web server can have their own domains (www.company1.com and www.company2.com) and access to the web server. Virtual hosts are not supported in Cisco SIP Proxy Server Version 1.1.
- Core SIP server directives—Define the primary SIP functionality of the Cisco SIP Proxy Server; SIP message handling. If a core SIP server directive is not specified, the server will use the default.
- SIP server module directives—Define the Cisco SIP Proxy Server interfaces and additional functionality on a per-module basis.

Configuring Global Directives

The server global directives are generic server directives that define the overall operation of the server. These directives exclude those that configure protocol-specific (HTTP or SIP) details. For example, in the global directive section of the sipd.conf file, you can specify the directory in which the Cisco SIP software resides and how child processes of the Cisco SIP Proxy Server will function.

Note The directives that configure the Cisco SIP Proxy Server global environment are standard Apache directives. If the default for an Apache directive has been changed for the Cisco SIP Proxy Server usage, the new default is documented. For more detail on Apache directives, see www.apache.org.

To configure the server global directives, define values as necessary for the following directives:

- **ServerRoot**—Directory in which the Cisco SIP Proxy Server configuration, error, and log files reside (*bin/*, *conf/*, and *logs/*). On Linux, the default directory for these subdirectories is */usr/local/sip*. On Solaris, the default directory is */opt/sip*. Do not add a forward slash (/) to the end of the directory path.

  Note If the server is to be on a NFS or networked mounted filesystem, refer to LockFile documentation at http://www.apache.org/docs/mod/core.html#lockfile.

- **LockFile**—Path to the lockfile used when the Cisco SIP Proxy Server is compiled with either USE_FCNTL_SERIALIZED_ACCEPT or USE_FLOCK_SERIALIZED_ACCEPT. This directive should normally be left at its default value. The main reason for changing it is if the logs directory is NFS mounted, since the lockfile must be stored on a local disk. The PID of the main server process is automatically appended to the filename. Default is *logs/accept.lock*.
- **PidFile**—Path and file to which the Cisco SIP Proxy Server records its process ID when it is started. If the filename does not begin with a forward slash (/), it is assumed to be relative to the ServerRoot. Default is *logs/sipd.pid*.
- **ScoreBoardFile**—Memory-mapped file in which internal server-process information is stored. The ScoreBoardFile is automatically created if your architecture requires it. If this file is automatically created, ensure that no two servers share the same file. Default is *logs/apache_runtime_status*.
- **prefork MPM module**—How the Cisco SIP Proxy Server child processes will operate. When configured, child processes are monitored. When necessary, additional child processes are spawned to process incoming SIP requests and responses. When the monitor determines that too few requests and responses are taking place, it tears down some of the idle child processes.

  Note The maximum and minimum values for the following prefork MPM module directives are dependent on your available platform resources. Modify as required. The prefork module directives are ignored if the `ONE_PROCESS` environmental variable has been set.

  To configure the prefork module, specify values for the following directives:

  - **StartServers**—Number of child processes to create when the Cisco SIP Proxy Server starts. Default is 5.
  - **MinSpareServers**—Minimum number of idle child processes (not handling requests). Default is 5.
  - **MaxSpareServers**—Maximum number of idle child processes (not handling requests). Idle child processes that exceed this number are torn down. Do not set this parameter to a large number. Default is 10.
  - **MaxClients**—Maximum number of simultaneous requests that can be supported; not more than this number of child processes will be created. Default is 20.
  - **MaxRequestsPerChild**—Maximum number of requests that a child process can process. If this number is exceeded, the child process will be torn down. Default is 0.
- **Listen**—Bind the server to specific IP addresses and specify whether the server should listen to more than one IP address or port; by default it responds to requests on all IP interfaces, but only on the port specified in the Port directive.

Configuring the Host-Specific Directives

The server host-specific directives define the basic configuration of the Cisco SIP Proxy Server. The basic configuration consists of values used by the main server which responds to requests that are not handled by a virtual host. The host-specific directives define not only the server access and error logs, but with what frequency logs will be rotated as well.

Note The directives that define the basic configuration of the Cisco SIP Proxy Server environment are standard Apache directives. If the default for an Apache directive has been changed for the Cisco SIP proxy Server usage, the new default is documented. For more detail on Apache directives, see www.apache.org.

To configure the host-specific directives, define values for the following located in the sipd.conf file:

- **Port**—Port on which the Cisco SIP Proxy Server listens. The default is the well-known SIP port 5060. If this directive is set to a value less than 1023, the Cisco SIP Proxy Server (sipd daemon) initially must be run as root. This is still true if you want sipd to run as a different user or group.
- **User**—Name or number of the user to run the sipd process as when sipd is started by the root user.
- **Group**—Name or number of the group to run the sipd process as when sipd is started by the root user.

  Note On SCO (ODT 3), use value "nouser" for User, and use value "nogroup" for Group. On HPUX, if you cannot use "shared memory" as "nobody," create a user "www" and use it. For kernels that refuse to "setgid(Group)" or "semctl(IPC_SET)" when the value of (unsigned)Group is above 60000, do not use Group#-1.

- **ServerName**—Hostname of the server used by clients in Request-URIs that is different than the standard name the server would recognize as its own.

  For example, sip-proxy.company.com. This must be a valid DNS name of your host. If this is not available, enter the host IP address. The server will deduce the name from the IP address.
- **HostnameLookups**—Whether client DNS host names or IP addresses are logged. Valid values are On (log host names) or Off (log IP addresses). Default is Off.
- **ErrorLog**—Location of the error log file to which the Cisco SIP Proxy Server will log debug and error messages. Default is *logs/error_log*.

  If you want to automatically rotate error/debug log without having to tear down the Cisco SIP Proxy Server (sipd daemon), use the following examples for Linux and Solaris respectively.

  ErrorLog "|/usr/local/sip
- **LogLevel**—Verbosity of messages recorded in the error logs. Valid values (in order of decreasing significance) are:
  - emerg—Emergencies; system is unusable.
  - alert—Action must be taken immediately.
  - crit—Critical conditions.
  - error—Error conditions.
  - warn—Warning conditions (default).
  - notice—Normal but significant condition.
  - Info—Informational.
  - debug—debug-level messages.

  Default is warn.
- **LogFormat**—Format nicknames of logfile. These are used with the CustomLog directive.
  - LogFormat "%h %l %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
  - LogFormat "%h %l %t \"%r\" %>s %b" common
  - LogFormat "%{Referer}i -> %U" referer
  - LogFormat "%{User-agent}i" agent
- **CustomLog**—Location and format of the access log file. The default is *logs/access_log common*. For an agent and referer logfiles, use the following directives by uncommenting them:

  - CustomLog logs/referer_log referer
  - CustomLog logs/agent_log agent

  For a single logfile with access, agent, and referer information (combined logfile format), use the following directive by uncommenting it:

  - CustomLog logs/access_log combined

- **TransferLog**—With what frequency (in seconds) to rotate Cisco SIP Proxy Server logs without having to tear down the Cisco SIP Proxy Server (sipd daemon). To specify a value for this directive, specify the full path of the log file to be rotated and the rotation time.

  You can specify a value similar to
  `/user/local/sip/bin/rotatelogs/usr/local/sip/logs/request_log 86400`
  in this directive to have access records such as a REGISTER request logged to both the access_log and request_log.0974732040 (number extension is calculated and added based on the current time stamp and the specified rotation frequency). If the CustomLog directive is commented out, access records are logged to the file specified in the TransferLog directive.

Configuring the Cisco SIP Module Core Directives

The Cisco SIP Proxy Server core module implements an RFC 2543-compliant SIP server that can function as a redirect, registrar, or proxy server. If configured to be a proxy, the Cisco SIP Proxy Server can be configured to function as a transaction stateful or stateless server.

To define the Cisco SIP Proxy Server core configuration, define values for the following directives in the Cisco SIP Proxy Server Core module (mod_sip):

- **ProxyDomain**—DNS domain of the Cisco SIP Proxy Server. The DNS domain suffix must be entered in a standard Fully Qualified Domain (FQDN) format “mydomain.com” or “company.mydomain.com.” There is no default for this directive.
- **StatefulServer**—Whether the Cisco SIP Proxy Server will be a transaction stateful or transaction stateless server.

  When configured to function as a stateful server, on receiving a SIP request, the Cisco SIP Proxy Server creates a TCB in which it maintains a transaction state.

  As a stateful proxy server, from the time a SIP request is received until the final response is one transaction. Stateful proxy servers do not originate any SIP requests except for the SIP CANCEL request or an ACK for a non-200 OK final response. When configured to function as stateless proxy server, the Cisco SIP Proxy Server forwards every request downstream and every response upstream.

  As a stateful redirect server, the Cisco SIP Proxy server looks up its registry database on receiving a SIP request and returns a 302 response upstream. As a stateless redirect server, the Cisco SIP Proxy Server returns a final response on receiving any request and does not forward any response or request.

  Valid values are On and Off. Default is On.

- **SipResolveLocalContactsInRedirectMode**—Whether to return next-hop routing information when the Cisco SIP Proxy Server is configured to function as a redirect server. A redirect server typically returns the contact location it knows about. However, if this directive is set to On, next-hop routing will occur and the contact information may be updated before returning the SIP 3xx response. Valid values are On and Off. Default is Off.
- **ServerType**—Whether the Cisco SIP Proxy Server will function as a proxy or redirect server. As a proxy server, the Cisco SIP Proxy Server will process and route SIP requests. As a redirect server, the Cisco SIP Proxy Server will provide contact information via SIP redirect responses (3xx). Possible values are Proxy and Redirect. Default is Proxy.

- **UseCallerPreferences**—Whether to use user-defined or administrator-defined preferences when handling requests. Request-handling preferences are controlled by a server administrator but can be overridden by a UAC. Preferences include decisions such as whether to proxy or redirect a request, whether to fork a request (sequential or parallel), whether to recursively search, and to which URI to proxy or redirect a request. Valid values are On (use user-defined preferences) or Off (ignore user-defined preferences). Default is On.
- **Recursive**—Whether the Cisco SIP Proxy Server will recursively try addresses returned in a SIP 3xx redirection response or use the lowest-numbered address. Valid values are On (the server will recursively try addresses on the contact list returned) or Off (the server will use the lowest-numbered response). Default is On.
- **RedirectMode**—Toggle for redirect mode. Default is Off.
- **MaxForks**—Maximum number of branches that can be forked when the Cisco SIP Proxy Server is configured to function as a stateful server. The range is 1 to 6. Default is 5.
- **NumericUsernameInterpretation**—Lookup order for numeric user information in the Request-URI header field when the ";user=usertype" parameter is missing.

  Valid values are:

  - IP_164—Process the Request-URI entries as URLs first and then as E.164 numbers.
  - E164_IP—Process the Request-URI entries as E.164 numbers first and then as URLs.
  - IP—Process the Request-URI entries as URLs only.
  - E164—Process the Request-URI entries as E.164 numbers.

  Default is E164_IP.
- **NumericUsernameCharacterSet**—Set of characters used to determine whether the user information portion of the Request-URI is in a category of users that will be applied to the "NumericUsernameInterpretation" processing step. This set does not apply to any user information parameters. Default is +0123456789.-() (global phone number combinations). For more information on this directive, see the sipd.conf file.
- **SrvForFqdnOnly**—Whether to perform DNS Server (SRV) lookups only for hosts that are FQDNs. If the host portion of the Request-URI header field does not contain an IP address but contains a period, the Cisco SIP Proxy Server determines the host to be an FQDN. Valid values are On (perform DNS SRV lookups only on FQDN hosts) or Off (perform DNS SRV lookups for any host that does not contain a target port). Default is Off.
- **SipT1InMs**—Amount of time (in milliseconds) after which a request is first retransmitted. Default is 500.
- **SipT2InMs**—Amount of time (in milliseconds) after which the backoff interval for non-INVITE requests does not increase exponentially. Default is 4000.
- **SipT3InMs**—Amount of time (in milliseconds) the Cisco SIP Proxy Server will wait after receiving a provisional response when processing an INVITE request. Default is 60000.
- **SipMaxT3InMs**—Maximum amount of time (in milliseconds) the Cisco SIP Proxy Server will wait after receiving a provisional response when processing an INVITE request. Default is 180000.
- **SipT4InMs**—Amount of time (in milliseconds) that the TCB will be maintained after a final response to a SIP INVITE is proxied. Default is 32000.
- **MaxInviteRetxCount**—Maximum number of times that a SIP INVITE request can be retransmitted by the Cisco SIP Proxy Server. The range is 0 to 6. Default is 6.
- **MaxNonInviteRetxCount**—Maximum number of times that a SIP request other than an INVITE request can be retransmitted. The range is 0 to 10. Default is 10.

- **SharedMemorySize**—Shared memory size to be allocated for transaction control block (TCB). The valid range is 1,024,000 to the maximum DRAM on the machine. Default is 32 MB.
- **RegistryCleanupRate**—Interval (in milliseconds) at which the entries are deleted from the registry. Default is 180000 milliseconds.
- **AddRecordRoute**—Whether the Cisco SIP Proxy Server will add the Record-Route header field to an initial SIP INVITE message. The Record-Route header field contains a globally reachable Request-URI that identifies that proxy server. When a proxy server adds the Request_URI to the Record-Route field in SIP messages, the proxy server will be kept in the path of subsequent requests for the same call leg. Valid values are On (add the Record-Route field) and Off (do not add the Record-Route field). Default is Off. The ServerType directive must be set to Proxy for this directive to be applied.
- **DiffServeValue**—THe value (in hex) to mark the Type of Service (TOS) byte of the IP header field of the transmitted SIP packets. This field is in 8 bits (1 byte). Default value is 0x00. DiffServ values and their meangs are specified in RFC2474, RFC2475, RFC2597, and RFC2598. Following are the DiffServ values:
  - Expedited Forwarding (EF) queue (RFC2598) value: 0xB8
  - Assured Forwarding (AF) queue (RFC2597) values:

	Class 1	Class 2	Class 3	Class 4
Low drop	0x28	0x48	0x68	0x88
Medium drop	0x30	0x50	0x70	0x90
High drop	0x38	0x58	0x78	0x98

Some networks may alternatively recognize the Tyoe of Service (RFC1349, RVD1812) bitmasks as follows:

- Minimize delay: 0x10
- Maximize throughput: 0x08
- Maximize reliability: 0x04
- Minimize cost: 0x02

Note This directive only marks IP packets to a specified value. Marked packets receive special treatment only if the network's IP routers and switches are configured to do so.

- **Sip_Token_Port**—Port that will be used by the sychronization server on the Cisco SIP Proxy Server. This port must be identical for all servers in a farm.Default is 22794.
- **Sip_Services_Port**—Port on the sychronization server. Default is 52931.
- **RadiusRetransmissionInterval**—Time (in milliseconds) between retransmissions to radius server.
- **RadiusRetransmissionCount**—Number of times to retransmit before deciding that the radius server is unreachable.
- **RadiusRetransmissionAfterFailure**—Number of retransmissions on requests to RADIUS requests subsequent to a fallure. Default is 0.
- **RadiusRetryTime**—Time (in seconds) before retrying the primary server, if primary RADIUS server is marked out-of-service. Default is 300 seconds (5 minutes).

- **AccessListFile**—Location and name of the access-list file that lists all proxies in the same trusted boundary.
- **UserIpAddrInPathHeaders**—Whether the server will use its IP address or FQDN in the Via and Record-Route header fields. Possible values are On (use the IP address) and Off (use the FQDN). Default is On.
- **IPAddrInPathHeaders**—Which IP address will be used in the Via and Record-Route header fields when the UserIpAddrInPathHeaders field is set to On. If an address is not defined in this directive, the first value returned via gethostbyname is used.
- **IgnoreProxyRequire**—Proxy-sensitive feature that can be ignored when servicing clients.
- **SIPStatsLog**—Whether the Cisco SIP Proxy Server will print statistics to the stats_log file. Default is On.
- **SIPStatsInterval**—Interval (in seconds) at which statistics are logged. Default is 3600.
- **DebugFlag**—Whether to enable the printing of mod_sip module debug messages to *logs/error_log*. Valid values are StateMachine On (print messages) or StateMachine Off (do not print messages). Default is StateMachine Off.
- **OrigUserNameSource**—Origin of the “User Name” attribute in the accounting-request message. Possible values are From and Auth. For From, the user part of the URL in the From SIP header is used to perform authentication and populate standard RADIUS accounting attribute #1 (User Name). For Auth, the user provided for authentication in the authorization or proxy-authorization header is used for authentication and billing. If no proxy-authorization header is present, the user is taken from the From header in the billing records. Default is Auth.
- **NumExpandAuthUserName**—Apply number-expansion rules to the UserName received in the Authorization or Proxy-Authorization header [On | Off]. Default is On.

Configuring Cisco SIP Module Standard Directives

The Cisco SIP Proxy Server contains eight additional modules that can be used to configure a variety of inerfaces and additional features. The following describes the interfaces and services that you can configure on your Cisco SIP Proxy Server via modules.

Configuring MySQL Database Subscriber Table Interface

The Cisco SIP Proxy Server MySQL module (mod_sip_db_mysql) allows you to configure an interface to a MySQL-database subscriber table to maintain subscriber records for user authentication, authorization, and accounting purposes.

If a MySQL-database subscriber table exists in your network, you can use directives in the MySQL module to map the field names used by the Cisco SIP Proxy Server to those used in the MySQL database subscriber table. If a MySQL subscriber table does not already exist in your network, you must create one useing the “install_mysql_db” script or cut and paste the subscriber.sql into an existing MySQL database, then start the Csico SIP Proxy Server with the MySQL interface enabled.

Note For terminating features such as the Call Forwarding features, the “user” portion of the Request-URI is the key to query the MySQL database. For originating features such as Authentication, the UserName from the Authorization, Proxy-Authorization header, or From header is the key. In either case, the key may be expanded to a fully expanded E164 number before the MySQL query, depending on the relative configuration directives.

To configure the interface to the MySQL-database subscriber table and map field names used by the Cisco SIP Proxy Server to an existing MySQL-subscriber table, specify values for the following directives in the mod_sip_db_mysql module:

- **DB_MySQL**—Enable or disable the interface to the MySQL database. Enabling the interface will establish a TCP connection with the database. Valid values are On (enable the interface) or Off (disable the interface). Default is Off.
- **DB_MySQL_HostName**—Host name or IP address of the machine on which the MySQL database resides.
- **DB_MySQL_DB**—Name of the database in which the subscriber table is stored and maintained.
- **DB_MySQL_Username**—Login username to the database account.
- **DB_MySQL_Password**—Login password to the database account.
- **DB_MySQL_SubscriberTable**—Name of the table in which the subscriber entries will be stored.
- **DB_MySQL_*XXX*_Field**—Name equivalent in an existing MySQL-database subscriber table. Use these directives as necessary to map the field names being used by the Cisco SIP Proxy Server to the equivalent entry in an existing MySQL subscriber table.
- **DB_MySQL_COnnect_Timeout**—The timeout value (in seconds) when attempt to connect to the MySQL-database server. When it expires, the Cisco SIP Proxy Server marks the connection “bad” to prevent more child processes from blocking on the connect attempt. The Cisco SIP Proxy Server resets the connection flag as soon as the MySQL server comes back online. Default is 3 seconds.

  Note Adjust this value according to the server’s traffic load. If the timeout value is too large, more child processes can be blocked.

- **DebugFlag**—Whether to enable the printing of all mod-sip-db-mysql debug messages to *logs/error_log*. Valid values are DBMySQL On (print messages) or DBMySQL Off (do not print messages). Default is DBMySQL Off.

  Note For information on working with MySQL databases, see www.mysql.com.

- Number Expansion (mod_sip_numexpand)
  - **Cisco_Numexpand**—Whether to use number expansion on the Cisco SIP Proxy Server. Valid values are On (use number expansion) or Off (do not use number expansion). Default is Off.
  - **Cisco_Numexpand_DEBUG**—Whether to enable the printing of all number expansion-related debug messages. Valid values are On (print messages) or Off (do not print messages). Default is Off.
  - Define the number plan as follows:

    ```
    <NumberPlan mycompany.com>
        NumExp    2....    +1919555....
        NumExp    6....    +1408554....
        NumExp    7....    +1408553....
        NumExp    4....    +1978555....
        NumExp    3....    408556
    </NumberPlan>
    ```

- Authentication and Authorization (mod_sip_authen)
  - **Authentication**—Whether the proxy server will require users be authenticated before servicing their transactions. Valid values are On (user must be authenticated) or Off (user does not have to be authenticated). Default is Off.
  - **AuthRealm**—Realm used in authentication response headers. Default is Cisco.

  - **AuthScheme**—Type of authentication method to be used when users are required to obtain authentication before receiving service from the Cisco SIP Proxy Server. Possible values are HTTP_Digest or HTTP_CHAP. Default is HTTP_Digest.
  - **RadiusAuthSkew**—Amount of time (in seconds) that a challenge is valid. Default is 30.
  - **PrimaryRadiusAuthIp**—IP address or host name of the primary RADIUS server to be used for user authentication.
  - **PrimaryRadiusAuthPort**—Destination port number of the primary RADIUS server to be used for user authentication.
  - **PrimaryRadiusAuthSecret**—Secret text string shared between the Cisco SIP Proxy Server and the primary RADIUS authentication server.
  - **SecondaryRadiusAuthIp**—IP address or host name of the backup RADIUS server to be used for user authentication.
  - **SecondaryRadiusAuthPort**—Destination port number of the backup RADIUS server to be used for user authentication.
  - **SecondaryRadiusAuthSecret**—Secret text string shared between the Cisco SIP Proxy Server and the backup RADIUS authentication server.

- Call Forwarding Unconditional (mod_sip_call_forward)
  - **CallForwardUnconditional**—Whether to forward calls unconditionally. Possible values are On (forward calls unconditionally) or Off (do not forward calls unconditionally).
  - **CallForwardNoAnswer**—Whether to forward calls when a call is not answered. Possible values are On (forward calls when a call is not answered) or Off (do not forward calls when a call is not answered).
  - **CallForwardBusy**—Whether to forward calls when a SIP 486 Busy Here response is received. Possible values are On (forward calls) or Off (do not forward calls).
  - **CallForwardUnavailable**—Whether to forward calls when a UAC is unavailable. Possible values are On (forward calls) or Off (do not forward calls).
  - **CallForwardNoAnswerTimer**—Time (in milliseconds) after which to forward a call when a call goes unanswered. Default is 24000. The setting for this directive is valid only when the CallForwardNoAnswer directive is set to On.
  - **CallForwardUnavailableTimer**—Time (in milliseconds) after which to forward a call when a UAC is unavailable. Default is 24000. The setting for this directive is valid only when the CallForwardUnavailable directive is enabled.
  - **AddDiversionHeader**—Whether the CC-Diversion header will be included in the SIP messages. Inclusion of the CC-Diversion header enables conveying call-redirection information during a call setup phase. Possible values are On (include the CC-Diversion header) and Off (exclude the CC-Diversion header). Default is On if call forwarding is enabled.

- Registry Services (mod_sip_registry)
  - **Cisco_Registry**—Whether registry services are enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (function as a registrar server) or Off (do not function as a registrar server).
  - **Cisco_Registry_Shared_Memory_Address**—Memory location of the registration table. Default is the platform address.
  - **Cisco_Registry_Rendezvous_Name**—Rendezvous name of the database containing registration information. Default is a null value.
  - **Cisco_Registry_Rendezvous_Directory**—Location of the registration database.

  - **Cisco_Registry_Remote_Update_Port**—Port number of the registration database server for all members of a farm of servers. The value for this directive must be identical for all members of the farm. Default is 22913.
  - **Cisco_Registry_Farm_Members**—Names of the Cisco SIP Proxy Servers that you wish to be members of the farm of Cisco SIP Proxy Servers. This list must be defined identically on all the Cisco SIP Proxy Servers identified as part of a farm.
  - **Cisco_Registry_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. Default is 86400. The value specified in this directive must be greater than that specified in the RegistryCleanupRate core directive.
  - **DebugFlag**—Whether to enable the printing of mod_sip_registry module debug messages to *logs/error_log*. Valid values are Registry On (print messages) or Registry Off (do not print messages). Default is Registry Off.
  - Define the static registry contact entries as follows:

```
<StaticRegistry 10.1>
Static_Registry_User_Type           IP
Static_Registry_User                jdoe
Static_Registry_Contact             0015155551212@mycompany.com
Static_Registry_Contact_User_Type   PHONE
Static_Registry_ContactPort         5060
Static_Registry_TransportProtocol   UDP
Static_Registry_ContactAge          Permanent
Static_Registry_Delete_or_Add       ADD
</StaticRegistry>
```

- E.164 to Request-URI Address Translation (mod_sip_enum)
  - **Cisco_Enum**—Whether E.164 to Request-URI translation is enabled. Possible values are On (translate) or Off (do not translate). Default is On.
  - **Cisco_Enum_Domain**—Private search domain for a private ENUM number plan. If a Request-URI user begins with the plus (+) character, this directive is not used because the plus character indicates that the number is part of a global ENUM number plan, which is e164.arpa.
  - **Cisco_Enum_Global_Domain**—Domain to use when the Request-URI user begins with a plus (+) character (indicating a global domain) or to use when a value is not specified for the Cisco_Enum_Domain directive. Default is to use e164.arpa.
  - **DebugFlag**—Whether to enable the printing of mod_sip_enum API debug messages to *logs/error_log*. Valid values are Enum On (print messages) or Enum Off (do not print messages). Default is Enum Off.
- GKTMP Interface (mod_sip_gktmp)
  - **GktmpConnection**—Whether the GKTMP interface is enabled or disabled. Possible values are On (interface is enabled) or Off (interface is disabled). Default is Off.
  - **MasterServerHostname**—Hostname of the primary NAM server.
  - **MasterServerIpAddress**—IP address of the primary NAM server.
  - **MasterServerPort**—Destination port number of the primary NAM server to be used for 800/900 and LNP lookup services.
  - **SecondaryServerHostname**—Hostname of the secondary NAM server.
  - **SecondaryServerIpAddress**—IP address of the secondary NAM server.
  - **SecondaryServerPort**—Destination port number of the secondary NAM server.

  - **Debug Flag**—Whether to enable the printing of mod_sip_gktmp module debug messages to *logs/error_log*. Valid values are Gktmp On (print messages) or Gktmp Off (do not print messages). Default is Gktmp Off.
  - **DebugFlag**—Whether to enable the printing of mod_sip_gktmp API debug messages to *logs/error_log*. Valid values are Gktmp API On (print messages) or GktmpAPI Off (do not print messages). Default is GktmpAPI Off.
- Next Hop Routing (mod_sip_routing)
  - **Cisco_Routing**—Whether next hop routing is enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (next hop routing is enabled) or Off (next hop routing is disabled). Default is On.
  - **Cisco_Routing_Shared_Memory_Address**—Memory location of the routing table. If the value of this directive is a null value, the default address of the platform will be used.
  - **Cisco_Routing_Rendezvous_Name**—Rendezvous name of the database containing routing information. Default is a null value.
  - **Cisco_Routing_Rendezvous_Directory**—Location of the routing database.
  - **Cisco_Routing_Remote_Update_Port**—Port number of the routing database server for all members of a farm of servers. The value for this directive must be identical for all members of the farm. Default is 22913.
  - **Cisco_Routing_Use_Domain_Routing**—Whether to use domain next hop routing. Domain next hop routing uses the host portion of the Request-URI as the key in obtaining the next hop or hops for a request. Valid values are On (use domain routing) or Off (do not use domain routing). Default is Off.
  - **Cisco_Routing_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. Default is 0.
  - **DebugFlag**—Whether to enable the printing of all mod-sip-routing module debug messages to *logs/error_log*. Valid values are Routing On (print messages) or Routing Off (do not print messages). Default is Routing Off.
  - Define the static route entries as follows:

```
<StaticRoute 1>
Static_Route_Destination Pattern          001555666
Static_Route_Type                         PHONE
Static_Route_NextHop                      sip_gw1.mycompany.com
Static_Route_NextHopPort                  5060
Static_Route_TransportProtocol            UDP
Static_Route_Priority                     0
Static_Route_Delete_or_Add                Add
</StaticRoute>
```

- Number Services (sip_numserv)
  - **Cisco_Number_Services**—Whether or not numbering services is enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (enabled) or Off (disabled).
  - **Cisco_Number_Services_Shared_Memory_Address**—Memory location of the number services table. Default is the platform address.
  - **Cisco_Number_Services_Rendezvous_Name**—Rendezvous name of the number services database. Default is numserv_db.
  - **Cisco_Number_Services_Rendezvous_Directory**—Location of the number services database.

- **Cisco_Number_Services_Remote_Update_Port**—TCP port number of the number services for all members of a farm of servers. The value for this directive must be identical for all members of the farm. Default is 22913.
- **Cisco_Number_Services_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. Default is 0.
- **DebugFlag**—Whether to enable the printing of all mod_sip_numserv module debug messages to *logs/error_log*. Valid values are Numserv On (print messages) or Numserv Off (do not print messages). Default is Numserv Off.
- Define the static number service entries as follows:

```
<Number_Services 1>
Number_Services_Contact                          911
Number_Services_Priority                         EMERGENCY
<Number_Services_Route 10>
Static_Number_Services_Route_Target              proxyserver@company.com
Static_Number_Services_Route_OriginationPattern  515555
Static_Number_Services_TransportPortocol         UDP
Static_Number_Services_ContactPort               5060
</Number_Services_Route>
</Number_Services>
```

Note For complete information about creating and modifying the sipd.conf file, see the *Cisco SIP Proxy Server Administration Guide.*

Configuring the Cisco uOne Messaging System

There are multiple components that make up the uOne Messaging System. Configuration of the system requires configuration of each of its components.

When implementing the uOne SIP system, be aware of the following:

- A uOne SIP system supports the following payloads:
  - G.711 mu-law
  - G.729
  - Dynamic AVT tones payload: 97—127
  - Cisco RTP DTMF relay payload: 121
- A uOne SIP system does not support CODEC switching within a call.
- The uOne SIP system does not support Single Number Reach (SNR) services.
- The SIP uOne implementation supports Netscape messaging and directory servers for Internet Message Access Protocol (IMAP) / Lightweight Directory Access Protocol (LDAP) servers.

Note For complete information about configuring the Cisco uOne Messaging System, see the *uOne BackEnd Servers Reference Manual, Release 4.2(2)s*, the *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*, and the *Installing and Configuring uOne 4.2(2)s, SIP Edition* document.

To configure the uOne system, perform the following tasks:

	Task	References
Step 1	Run the Quick Config tool to perform the initial uOne configuration tasks on the gateserver: • Configure the uOne system for calls • Setup the uOne Subscriber Administration tool • Setup the uOne Manager and/or the uOne database	*Installing and Configuring uOne 4.2(2)s, SIP Edition* *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*
Step 2	Make any configuration changes on the gateserver necessary for your operating environment.	*Installing and Configuring uOne 4.2(2)s, SIP Edition* *SIP Compliance and Call Flows for uOne 4.2(2)s* *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s* *uOne Administration Manual, Release 4.2(2)s*
Step 3	Configure the directory server for uOne.	*uOne Back End Servers Reference Manual, Release 4.2(2)s*
Step 4	Configure the messaging server for uOne.	
Step 5	Configure the paging server for uOne.	
Step 6	If desired, set up communities of interest.	*uOne Administration Manual, Release 4.2(2)s* *uOne Back End Servers Reference Manual, Release 4.2(2)s*
Step 7	Set up classes of service.	
Step 8	Provision subscribers.	
Step 9	Create broadcast lists	
Step 10	If necessary, set up additional greeting and/or fax administrators.	

Configuring the Cisco Secure PIX Firewall

To configure the Cisco Secure PIX Firewall, perform the following tasks:

	Task	References
Step 1	Obtain a console terminal, download the most current software, and configure network routing.	*Configuration Guide for the Cisco Secure PIX Firewall Version 6.0*
Step 2	Start the PIX Firewall configuration mode.	
Step 3	Identify each interface.	
Step 4	Create a default route outside.	
Step 5	Permit ping access.	
Step 6	Store image in Flash memory and reboot.	

In addition, perform the following tasks:

- Enable the SIP protocol on the appropriate interface or interfaces (via the **fixup protocol sip 5060** command)
- If necessary, customize the SIP inactivity timer (via the **timeout sip** ***hh:mm:ss*** command) and the SIP media timer used for SIP RTP/RTCP with SIP UDP media packets instead of the UDP inactivity timeout (via the **timeout sip_media** ***hh:mm:ss*** command).
- Create a list of "allowed" external devices for all outside devices you wish to be able to call inside the firewall (outside callers cannot make calls to inside the firewall unless they have been defined as an allowed device).

Configuring the Cisco SS7 Interconnect for VoIP Gateways Solution

There are numerous components that make up the Cisco SS7 Interconnect for VoIP Gateways Solution. The configuration tasks for each component in the solution are briefly described in the following sections:

- Configuring the Signaling Controller, page 4-23
- Configuring the Cisco AS5300 Universal Access Server, page 4-27

Note For complete information about configuring the Cisco SS7 Interconnect for VoIP Gateways Solution, see the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*, the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*, and the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*.

Configuring the Signaling Controller

Configuring the signaling controller software consists of three tasks:

- Configuring the Signaling Controller
- Configuring the Cisco SLT
- Configuring the LAN Switch (Optional)

⚠ **Caution** Always use the Cisco signaling controller CMM tool or MML commands to create, modify, manage, and deploy your configuration files on the signaling controller. We do not recommend modifying the configuration files directly on the signaling controller.

Configuring the Signaling Controller

To configure the signaling controller, perform the following tasks:

	Task	Reference
Step 1	Prepare the following: • Bearer routes to other switches • Signaling point links (the connection between an MGC and a SIP server) • Network access server control links • Trunks, trunk groups, and routes (for incoming SIP calls) • Dial plans	*Cisco Media Gateway Controller Software Release 9 Provisioning Guide* *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 2	Configure the SS7 signaling routes to external switches by completing the following tasks: • Add the OPC in your network. • Add the DPC to identify the destination switch. • Add the APCs to identify the STPs with which the signaling controller communicates signaling information. • Add linksets to connect the Cisco SLTs to the STPs. • Add the SS7 subsystem to identify the mated STPs. • Add the SS7 routes for each signaling path from the signaling controller to the destination switch. • Add the SS7 signaling service from the signaling controller to the destination switch.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*

	Task	Reference
Step 3	Provision the signaling links by completing the following tasks: • Add the Ethernet adapters (cards) in the SC host that carry signaling to and from the Cisco SLTs. • Add Ethernet interfaces for the cards in the host. • Add C7 IP links for each SS7 link from the signaling controller to the SS7network (through the Cisco SLT).	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 4	Configure the access gateway control links by completing the following tasks: • Add external nodes for the access gateways in your network. • Add NAS signaling services for each access gateway. • Add IP links for each access gateway to each Ethernet card in the SC host.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 5	Configure trunks, trunk groups, and routes.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 6	Provision black and white trunk screening.	
Step 7	Build and deploy the configuration.	

Configuring the Cisco SLT

To configure the Cisco SLTs, perform the following tasks:

	Task	Reference
Step 1	Identify the serial WAN interface card on your Cisco SLT and connect cable to card.	*Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 1	Install the Cisco SLT image software.	
Step 2	Configure the basic parameters and SS7 links for the Cisco SLT.	
Step 3	Configure Session Manager and RUDP.	
Step 4	Save the new configuration as the startup configuration, and then reload the Cisco SLT.	

Configuring the LAN Switch (Optional)

This section describes the task of configuring LAN switches (Cisco Catalyst Switch family) for your solution. The LAN switch connects the SC hosts to the access gateways or the Cisco SLTs. The LAN switch is used in the SC node to extend VLANs across platforms through backbone Fast Ethernet, Gigabit, or ATM connections, when necessary. The LAN switch is not provided with the SC host.

To configure the LAN switch, complete the following tasks:

	Task	Reference
Step 1	Make sure that you have virtual LAN assignments and IP address assignments for solution devices.	*Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 2	Configure basic system information.	
Step 3	Configure the logical interface.	
Step 4	Configure SNMP information.	
Step 5	Configure the virtual LANs (VLANs).	
Step 6	Configure module and port parameters.	
Step 7	Configure spanning-tree parameters.	
Step 8	Configure the standby ports.	
Step 9	Configure the ISL connections between switches.	
Step 10	Configure the switch port analyzer.	
Step 11	Configure the route switch module.	

Configuring the Cisco AS5300 Universal Access Server

The Cisco AS5300 Universal Access Server is a required Cisco SIP Gateway when implementing the VoIP Infrastructure Solution for SIP with the Cisco SS7 Interconnect for Voice Gateways Solution.

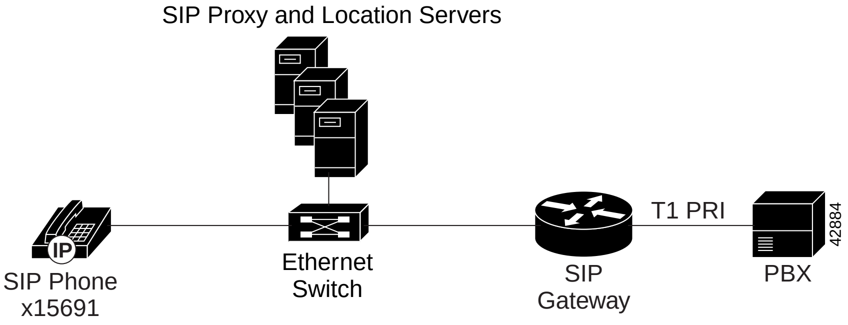
In addition to the configuration prerequisites described in the "Configuring the Routers" section on page 4-1, for each AS5300 access server installed in your solution that will connect to the Cisco SS7 Interconnect for Voice Gateway Solution, configure the access gateway by performing the following tasks:

	Task	Reference
Step 1	Configure the switch type to NI2, using the **isdn switch-type primary-ni** command. (This command enables the connection between the access gateway and the virtual switch controller.)	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
Step 2	Configure the access server for channelized T1 or E1 lines.	
Step 3	Enable POTS and VoIP dial peers.	
Step 4	Enable VoIP functionality.	"Configuring VoIP Support" section on page 4-2.
Step 5	Configure the SIP support on the gateway.	"Configuring the Cisco SIP Gateway" section on page 4-2.

Configuration Example

Figure 4-1 illustrates an example of a simple implementation of the Cisco VoIP Infrastructure Solution for SIP. The example configurations in this section pertain to this illustration.

Figure 4-1 Simple Implementation Example



Example Cisco SIP Gateway Configuration

To configure the Cisco router or access server as a VoIP SIP gateway as shown in Figure 4-1, we must perform the following tasks:

Task	Command
Configure the serial interface used for voice data and enter interface configuration mode.	**interface serial** *slot*/*port*
Specify the central office switch type on the ISDN interface.	**isdn switch-type** *switch_type*

Task	Command
Specify how incoming voice calls are to be handled.	For the Cisco 2600 and 3600: **isdn incoming-voice voice** For the Cisco AS5300: **isdn incoming-voice modem** [**56** | **64**]
Exit interface configuration mode.	**exit**
Configure the parameters of the T1 or E1 line that is connected to the PBX and enter controller configuration mode.	**controller** {**t1** | **e1**} *slot*/*port*

Select the frame type for the T1 or E1 data line.	For a T1 line:
	framing {**sf** | **esf**}
	For an E1 line:
	framing {**crc4** | **no-crc4**}

Configure the line coding for T1 lines.	**linecoding** { **b8zs** | **ami** }
Configure the ISDN PRI.	**pri-group timeslots** *range*
Exit controller configuration mode.	**exit**
Configure the VoIP dial-peers, which are used to handle outgoing calls from the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **voip**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that the dial-peer is to use SIP for all call signaling.	**session protocol sipv2**
Specify that all outbound calls are to be routed to the SIP proxy.	**session target sip-server**
Specify the codec to be used for outbound calls. This information is included in the SDP body of the INVITE.	**codec** {**g711alaw** | **g711ulaw** | **g723r63** | **g726r16** | **g728** | **g729r8**}
Exit VoIP dial-peer configuration mode.	**exit**
Configure the POTS dial-peers, which are used to handle incoming calls to the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **pots**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that direct inward dialing is to be used (there is no secondary dial tone).	**direct-inward-dial**
Specify that all calls that match the destination pattern should be routed to the specified voice port.	**port** *slot*/*port*:*ds0-group-no*

Task	Command
Specify the prefix of the dialed digits for this dial peer.	**prefix** *string*
Exit POTS dial-peer configuration mode.	**exit**
Specify the digits to use to expand an extension number into a destination pattern.	**num-exp** *extension-number expanded-number*
Enable SIP on the router and enter SIP user agent configuration mode.	**sip-ua**
Specify the retry values for SIP messages.	**retry** {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}
Specify the network address (IP address or host name) of the SIP proxy or redirect server.	**sip-server** { **dns**:[*host-name*] | **ipv4**:*ipaddr*[:*port-num*] }
Exit the SIP user-agent configuration mode.	**exit**

Example 4-1 shows the resulting configuration of a Cisco router as a SIP gateway for the Cisco VoIP Infrastructure Solution for SIP.

Example 4-1 Cisco SIP Gateway Running Configuration

```
router-sip-gw#show running
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtp-sip-gw
!
enable secret 5 $1$JipI$QyBzbLd44Y4k6yXqND3iR.
!
!
!
!
!
voice-card 1
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 161.44.11.21
!
isdn switch-type primary-5ess
isdn alert-end-to-end
!
!
!
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
```

```
!
controller T1 1/1
!
!
!
interface FastEthernet0/0
 ip address 172.17.207.91 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 no ip mroute-cache
 shutdown
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.207.1
no ip http server
ip pim ssm
!
!
voice-port 1/0:23
!
dial-peer voice 15690 voip
 application session
 destination-pattern 1569.
 session protocol sipv2
 session target sip-server
 codec g711ulaw
!
dial-peer voice 20000 pots
 application session
 destination-pattern 919392....
 direct-inward-dial
 port 1/0:23
 prefix 919392
!
dial-peer voice 30000 pots
 application session
 destination-pattern 408853....
 direct-inward-dial
 port 1/0:23
 prefix 408853
!
dial-peer voice 40000 pots
 application session
 destination-pattern 978244....
 direct-inward-dial
 port 1/0:23
 prefix 978244
!
dial-peer voice 50000 pots
 application session
 destination-pattern 408525....
 direct-inward-dial
 port 1/0:23
 prefix 408525
!
dial-peer voice 60000 pots
 application session
 destination-pattern 408526....
 direct-inward-dial
 port 1/0:23
 prefix 408526
!
dial-peer voice 70000 pots
 application session
 destination-pattern 408527....
 direct-inward-dial
 port 1/0:23
 prefix 408527
!
dial-peer voice 9 pots
 application session
 destination-pattern 9.......
 no digit-strip
 direct-inward-dial
 port 1/0:23
!
dial-peer voice 10 pots
 application session
 destination-pattern 91..........
 no digit-strip
 direct-inward-dial
 port 1/0:23
!
num-exp 991569. 1569.
num-exp 2.... 919392....
num-exp 3.... 408853....
num-exp 4.... 978244....
num-exp 5.... 408525....
num-exp 6.... 408526....
num-exp 7.... 408527....
sip-ua
retry invite 4
retry response 3
retry bye 2
retry cancel 2
sip-server ipv4:172.18.192.232
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password sip
 login
!
end
```

Example Cisco SIP IP Phone Configuration Files

To configure the Cisco SIP IP phone as shown in Figure 4-1, we created the default configuration file show in Example 4-2 and the phone-specific phone file shown in Example 4-3.

Example 4-2 Example Cisco SIP IP Phone Default Configuration File

```
# SIP Default Configuration File

# Proxy Server Address
proxy1_address : 172.18.192.232

# Image Version
image_version : P0S3Z313
```

Example 4-3 Example Cisco SIP IP Phone-Specific Configuration File

```
# SIP Configuration File - 003094C25D66

# Proxy Register (0-disable, 1-enable)
proxy_register : 1 ;

# Preferred Codec (g711ulaw, g711alaw, g729)
preferred_codec : g711ulaw ;

# Line 1 Name
line1_name :15691;

# Line 1 Authentication Name
line1_authname: ;

# Line 1 Password
line1_password: ;
```