Cisco White Paper

How to Configure Cisco's Core SIP Products

Introduction

The Session Initiation Protocol (SIP) is a signaling protocol used to negotiate, establish, and terminate multimedia sessions such as voice calls. It is a peer-to-peer technology, similar to H.323, where endpoints possess the capability to initiate and receive sessions without the assistance of a call-processing agent such as those used with the Media Gateway Control Protocol (MGCP) and Skinny Client Control Protocol (SCCP). SIP utilizes existing Internet protocols such as DNS, DHCP, TFTP, and Session Description Protocol (SDP), so it maps well to the World Wide Web (WWW) model. As such, SIP uses several different types of servers—including proxy, redirect, and registration servers—to route signaling information and locate endpoints.

This paper introduces the core components of a SIP network and explains how to configure them. The intent is to provide a quick reference to individuals who are just beginning to work with SIP and may need to set up a customer demonstration or add this equipment to their lab. The configurations provided should help users understand basic SIP functionality. This paper does not provide advanced configurations, extensive call-flow examples, and debugging output.

Definitions

The following definitions are taken from IETF draft, draft-ietf-sip-rfc2543bis-04.txt.

Call stateful: A proxy is call stateful if it retains state for a dialog from the initiating INVITE to the terminating BYE request. A call-stateful proxy is always transaction stateful, but the converse is not necessarily true.

Location service: Service that is used by a SIP redirect or proxy server to obtain information about a callee's possible locations. It contains a list of bindings of address-of-record keys to zero or more contact addresses. Bindings can be created and removed in many ways; this specification defines a REGISTER method that updates bindings.

Method: Primary function that a request is meant to invoke on a server. The method is carried in the request message itself. Examples are INVITE and BYE.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Proxy, proxy server: An intermediary entity that acts as both server and client for the purpose of making requests on behalf of other clients. A proxy server primarily handles routing, which means that its job is to ensure that a request is sent to another entity that is "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure that a user is allowed to make a call). A proxy interprets and, if necessary, rewrites specific parts of a request message before forwarding it.

Redirect server: A user-agent server that generates 3xx responses to requests that it receives, directing the client to contact an alternate set of URIs.

Registrar: A server that accepts REGISTER requests and places information in those requests into the location service for the domain that it handles.

Request: A SIP message that is sent from a client to a server, invoking a particular operation.

Response: A SIP message that is sent from a server to a client, indicating the status of a request sent from the client to the server.

Stateful proxy: A logical entity that maintains the client and server transaction-state machines defined by this specification during the processing of a request; also known as a transaction-stateful proxy. A (transaction-) stateful proxy is not the same as a call-stateful proxy.

Stateless proxy: A logical entity that does not maintain the client or server transaction-state machines defined in this specification when it processes requests. A stateless proxy forwards every request that it receives downstream and every response that it receives upstream.

User-agent client (UAC): A logical entity that creates a new request, and then uses the client transaction-state machinery to send it. The role of UAC lasts only for the duration of a transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of the transaction. If it receives a request later, it assumes the role of a user-agent server for the processing of that transaction.

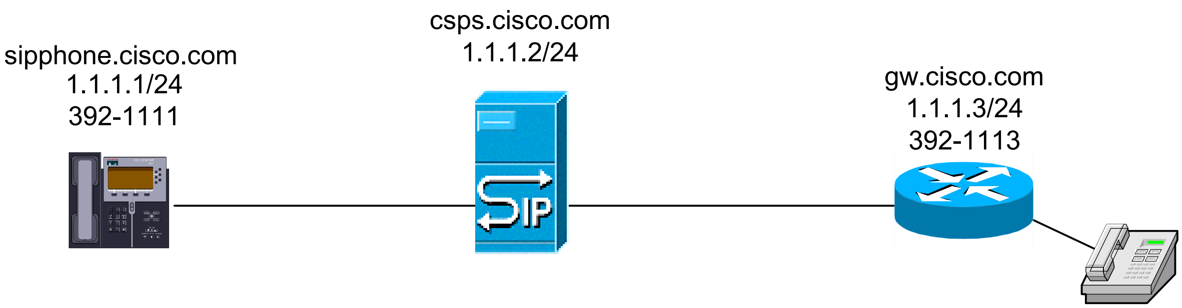
User-agent server (UAS): A logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of a transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of the transaction. If it generates a request later, it assumes the role of a user-agent client for the processing of that transaction.

SIP Components

Basic topology consists of one Cisco SIP proxy server, one Cisco 7960 SIP IP phone, and one Cisco IOS gateway with an analog phone connected to an FXS port. All components, with the exception of the analog phone, are connected via a Cisco 3524-XL-PWR switch. There are other servers that could be added, including DNS, TFTP, DHCP, and NTP servers; however, they are not required.

Cisco Confidential
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Topology



Cisco IOS and Firmware

Cisco IOS Gateway	Cisco SIP Proxy Server (Linux)	Cisco 7960 SIP IP Phone
12.2(13)T1	2.0	4.3

Device Configurations

This section contains basic configuration examples for the Cisco SPS, Cisco IOS gateway, and Cisco 7960 SIP IP phone. The information provided should enable you to configure the above topology and place basic calls between endpoints.

Cisco SIP Proxy Server

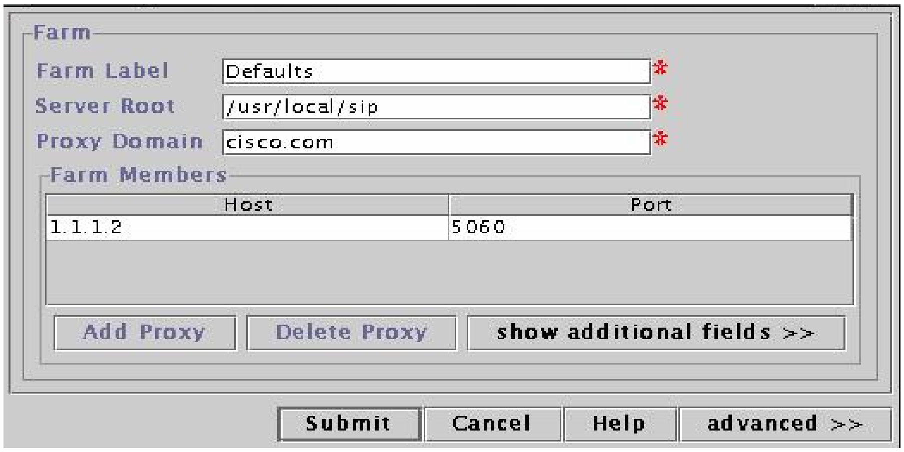
Before discussing how to configure Cisco SPS, it is important to understand some of the key steps regarding product installation. Before installation, the Linux or Solaris device should be properly configured with the correct networking and address-resolution parameters. If these parameters are not correct or are changed after installation, problems could arise. Once Cisco SPS is installed on the device, it is imperative that the csps_setup script be used to complete the installation properly.

With the release of 2.0, there are two ways to configure the Cisco SPS: 1) the sipd.conf file and 2) the provisioning GUI. You can use either method, but not a combination of both. If you use the provisioning GUI, a new sipd.conf file is written every time you change a configuration and click Commit, and put into service when you gracefully restart the system, restart it, or stop and then start it. Any changes that you made directly to the sipd.conf file beforehand are overwritten.

This section contains a basic configuration for the Cisco SPS (GUI version). Certain directives are not shown, including RAS, RPMS, Virtual Proxy Host, ENUM, GKTMP, and Accounting.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

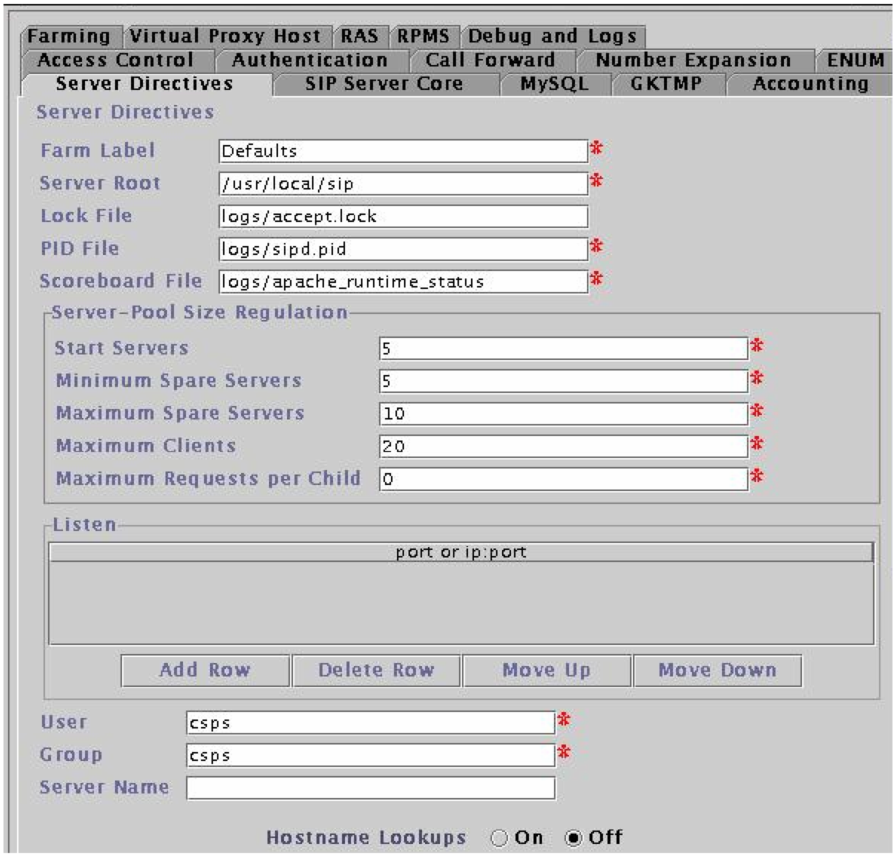
Farm Interface



The Farm Interface is the first interface that appears when you click on the Farm/Proxies option in the provisioning GUI menu. It contains the ***Proxy Domain*** directive that was configured during execution of the csps_setup script as well as the list of farm members.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

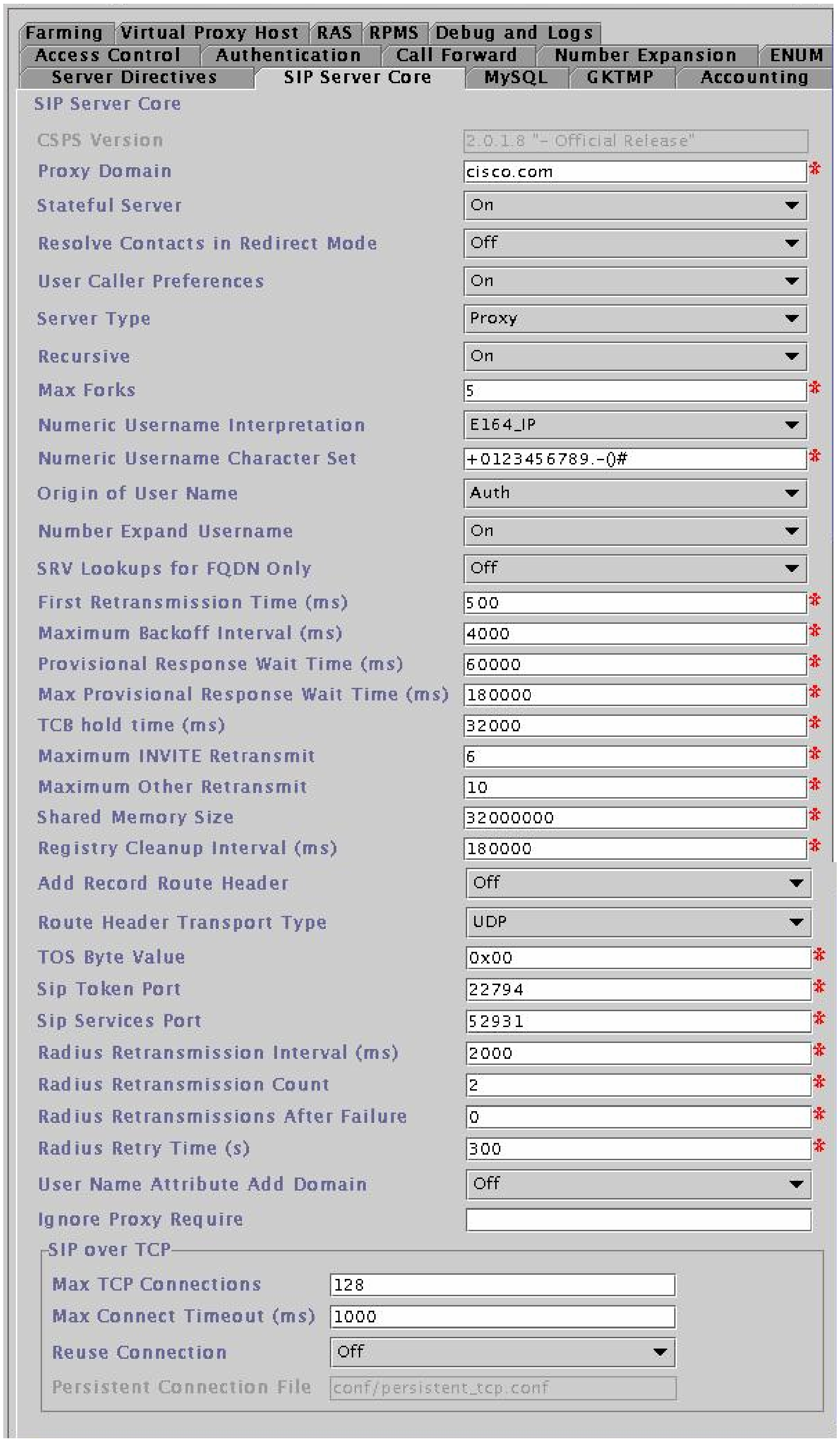
Server Directives Interface



The Server Directives interface contains standard apache directives such as ***Start Servers*** and ***Maximum Clients***. For normal operation, you need not change these directives. The ***User*** and ***Group*** directives were configured when Cisco SPS was first installed. The ***Server Name*** directive is needed only for a farm of multiple Cisco SPSs; it represents either the virtual IP (VIP) address of the farm if the farm resides behind a load balancer, or the DNS SRV record for the farm. For example, if proxy1.cisco.com and proxy2.cisco.com are members of the same farm, you can configure a server name such as farm.cisco.com to represent both proxies. For redundancy, endpoints can direct their requests and responses to farm.cisco.com so that either member of the farm can handle them during normal operation and in the event of a proxy failure.

Cisco Confidential
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

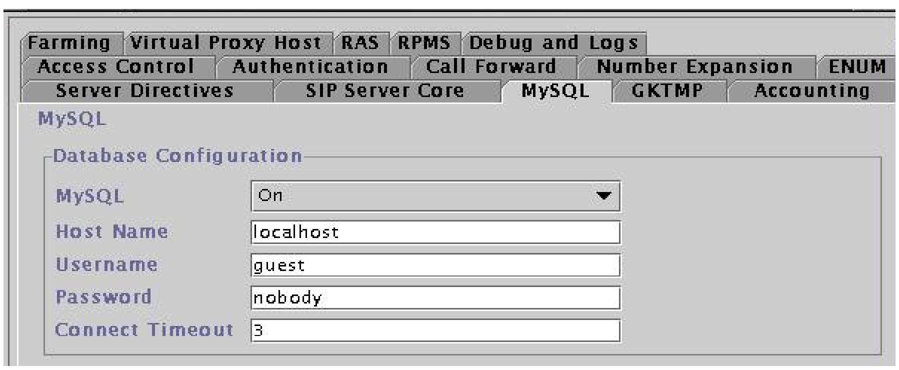
SIP Server Core Interface



Copyright © 2003 Cisco Systems, Inc. All rights reserved.

The SIP Server Core interface is where you configure core directives of the SIP server. The ***Proxy Domain*** directive was already configured during execution of the csps_setup script. The ***Stateful Server*** directive controls whether the server is transaction stateful or stateless by setting how long transaction-control blocks (TCB) are maintained for each transaction. For example, a transaction-stateless server maintains a TCB for only the length of time it takes to process an INVITE (approximately 20–30 ms); a transaction-stateful server maintains the TCB from the time an INVITE is received until 40 seconds after the 200 OK final response is processed. The ***Server Type*** directive can be set to either proxy, in which all session signaling flows through the proxy (similar to a Directed Mode Gatekeeper in H.323), or redirect, in which the server receives the request and replies to the client with one or more request-URIs, forcing the client to route the request (similar to a Routed Mode Gatekeeper in H.323). If the ***Add Record Route Header*** directive is set to on, then the server adds the Record Route header to the SIP signaling, forcing all requests and responses for a session to traverse that server; this is needed for billing and for certain security mechanisms such as IPSec. The ***Route Header Transport Type*** directive can be set to either UDP (default) or TCP; TCP should be used only if all of the devices that connect directly to Cisco SPS support it.

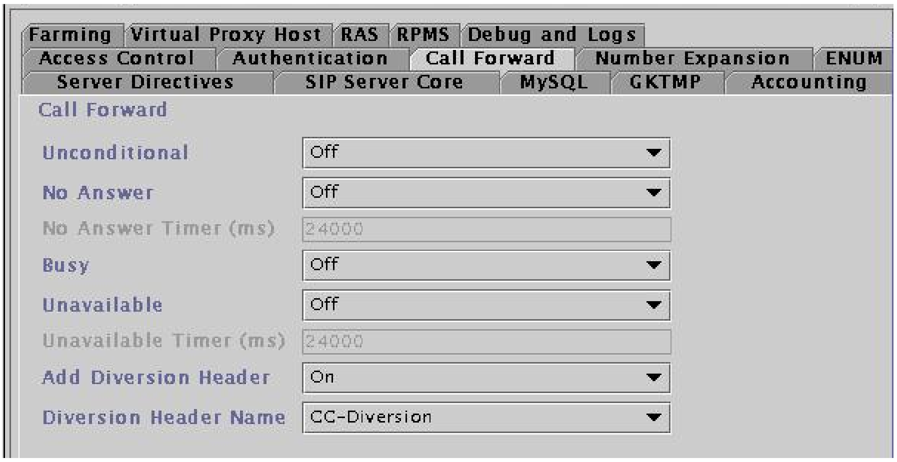
MySQL Interface



The MySQL interface contains directives regarding the database that Cisco SPS uses to store registered-user and configuration data. The directives are automatically set when MySQL is installed during execution of the csps_setup script. If the database resides on the same machine as Cisco SPS, the ***Host Name*** directive is localhost. If it resides on a separate machine, that host-name directive contains that machine's host name. The ***Username*** and ***Password*** directives are default and should not be changed; Cisco SPS uses them to access the MySQL database.

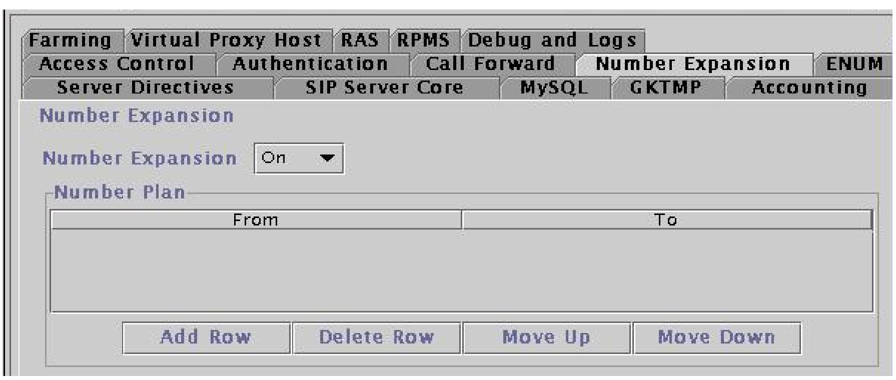
Cisco Confidential
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Call Forward Interface



The Call Forward interface contains the ***Call Forwarding Unconditional***, ***No Answer***, ***Busy,*** and ***Unavailable*** directives. These directives can be turned on or off (default) and are used for all registered endpoints that have call-forwarding information configured (refer to the Subscriber interface). If either the no-answer or unavailable directives are turned on, the associated timers are activated and become configurable. The default for these timers, 24000 ms, equals 4 rings.

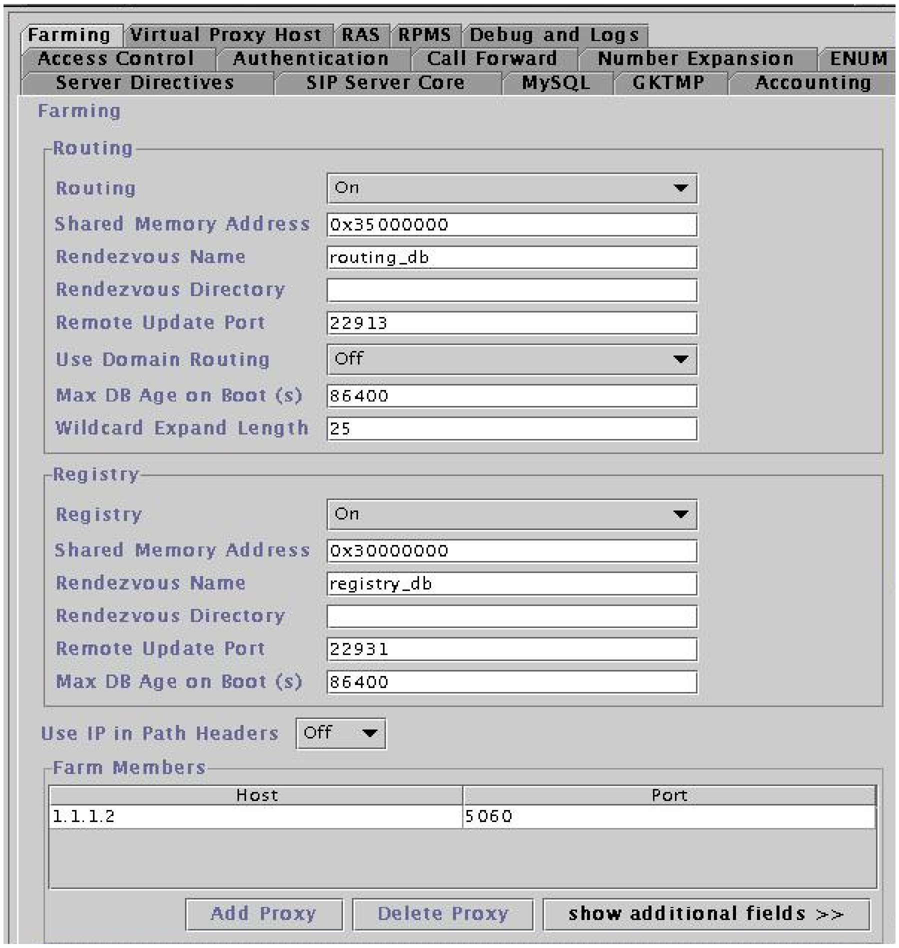
Number Expansion Interface



The Number Expansion interface contains the number plan. The user portion of the From, To, and Proxy-Authentication headers are expanded for internal processing only. The actual headers remain unchanged. Cisco SPS uses the expanded forms to perform MySQL, registry, and routing database searches.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

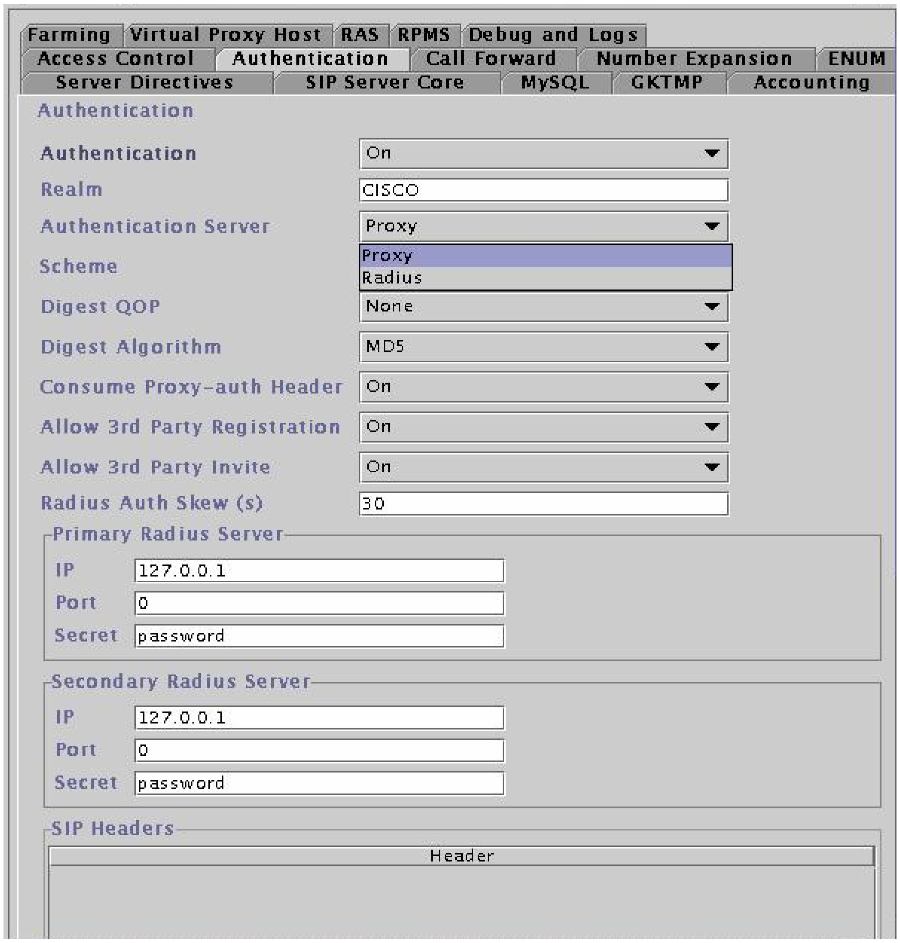
Farming Interface



The Farming interface contains the ***Routing*** and ***Registry*** directives. Both of these are on by default. Farm members are again listed on this interface. It is important to note that, when you configure farming, you need to set up an NTP source so that all servers in the farm can synch appropriately.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

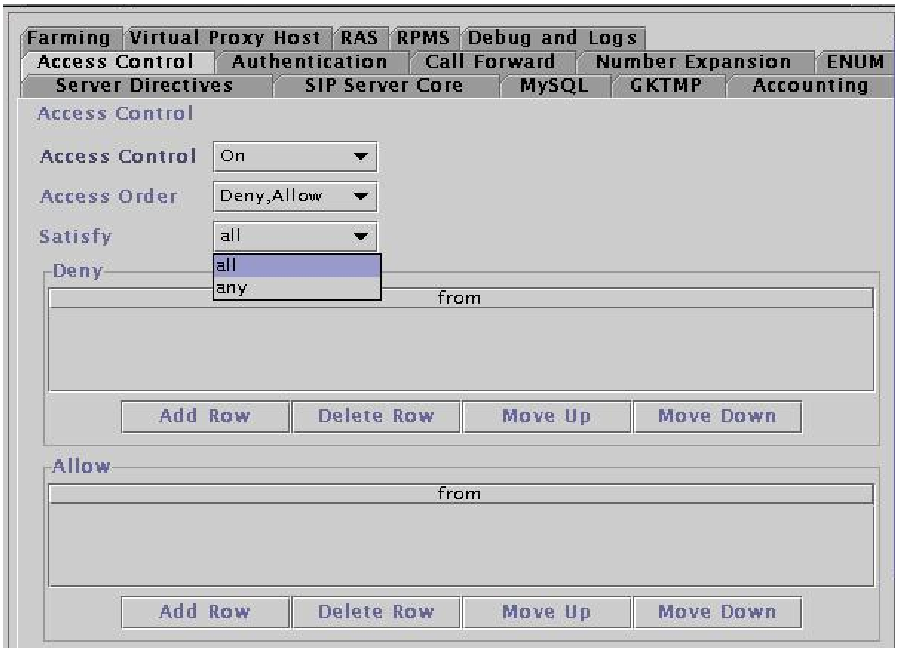
Authentication Interface



The Authentication interface contains the directives that are used to authenticate REGISTER and INVITE requests from endpoints. Authentication is off by default. You can configure the ***Authentication Server*** directive to use the Cisco SPS MySQL database (refer to the Subscriber interface) or a separate Radius server for authentication information. If you chose a separate Radius server, you can configure a primary and secondary server. Remember, Cisco gateways do not register nor do they authenticate with Cisco SPS, so you need to configure access-control lists to permit or deny their access to the Cisco SPS (refer to the Access Control interface).

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

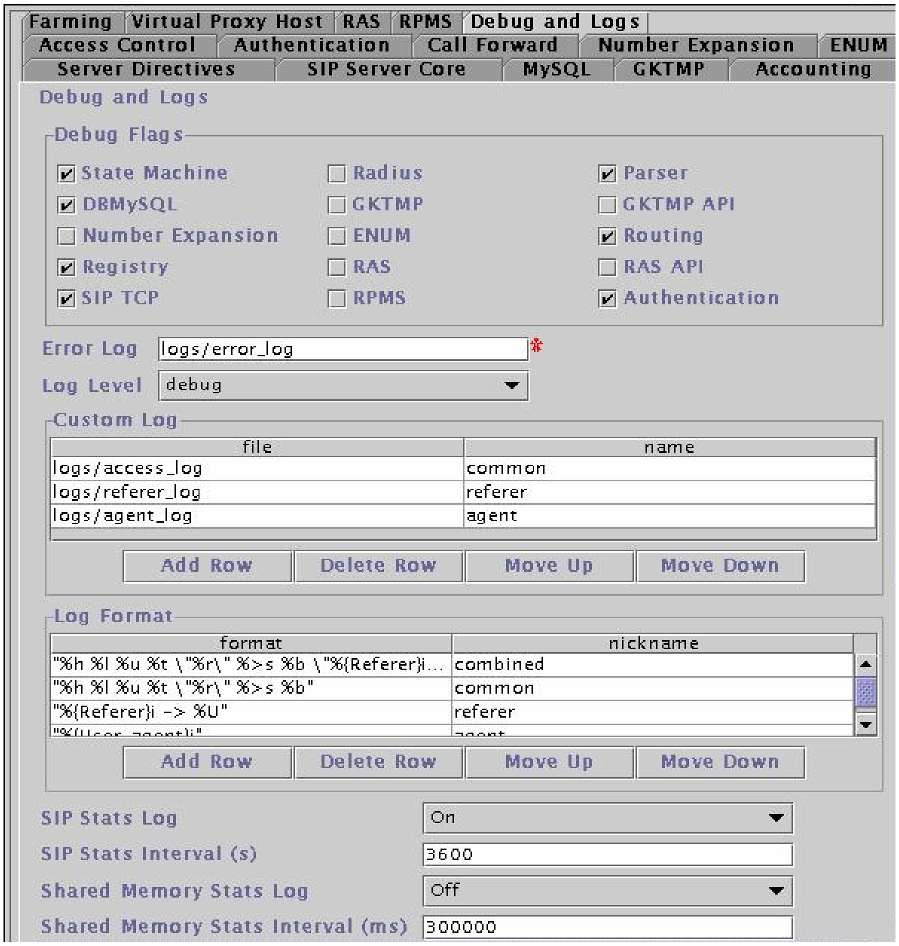
Access Control Interface



The Access Control interface contains directives that control access to the Cisco SPS. The ***Access Control*** directive is off by default. When it is turned on, you can add allow and deny statements to allow or deny access to certain devices within the SIP network. The functionality is similar to the basic ACLs that are configured in Cisco IOS gateways, with a couple of differences. First, there is the ***Access Order*** directive, which states the order in which ACL statements are evaluated. If you choose Deny, Allow, deny statements are evaluated first and access is allowed by default; therefore, an end user who does not match a deny statement or does match an allow statement is granted access. If you choose Allow, Deny, allow statements are evaluated first and access is denied by default; therefore, an end user who does not match an allow statement or does match a deny statement is denied access to the server. Second, there is the ***Satisfy*** directive, which has two options: 1) all, which means that end users must pass the authentication check and be allowed access; 2) any, which means that end users must either pass the authentication check or be allowed access. If authentication is turned off, the authentication check is considered successful.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Debug and Logs Interface



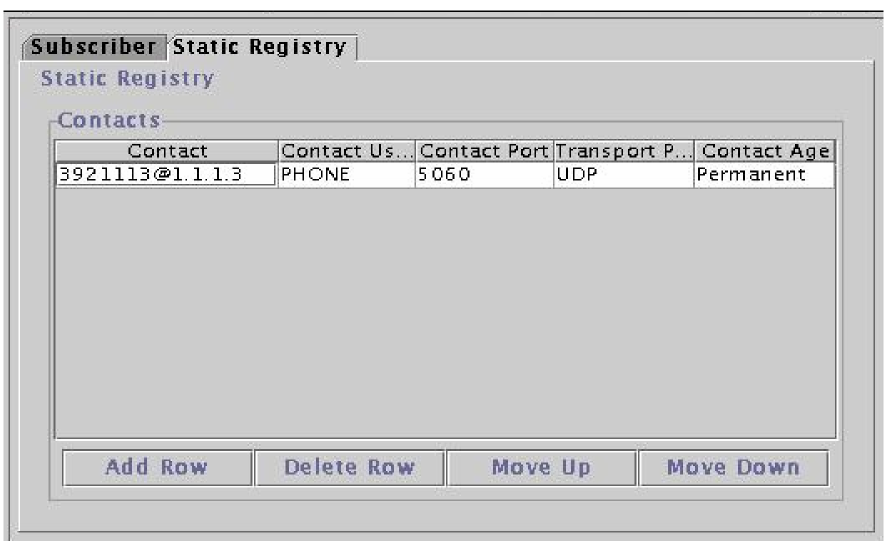
The Debug and Logs interface contains debug flags, log levels, and log-file location information. As a general rule, you should activate the State Machine ***Debug Flag*** as well as debug flags for any other functionality you are using. To obtain verbose troubleshooting information, it is recommended that you change the ***Log Level*** to debug. To view real-time debug information on the screen, use the **tail –f <log file name>** command, which is similar to activating debug commands on Cisco IOS gateways.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Subscriber Interface

The Subscriber interface contains information about registered (static or dynamic) users, including passwords for authentication and call-forwarding URLs.

Static Registry Interface



The Static Registry interface lists endpoints that do not support the REGISTER method but nevertheless need to receive calls from other endpoints. A good example is a Cisco IOS gateway connected to a PBX or a gateway that has analog phones connected via FXS ports. The gateway does not support the REGISTER method so it cannot dynamically register its endpoints with the Cisco SPS. Therefore, you must statically register the endpoints so that they can receive sessions from other endpoints. This also means that these gateway-connected endpoints cannot authenticate with the Cisco SPS so you need to configure access controls to allow or deny access.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Cisco IOS Gateway

This section contains a basic SIP configuration for a Cisco IOS gateway. Entries of particular interest are bold and shaded.

`version 12.2`	
`!`	
`hostname gw`	
`!`	
`ip domain name cisco.com`	
`ip name-server 1.1.1.2`	***IP address of DNS server**
`!`	
`interface FastEthernet0/0`	
`ip address 1.1.1.3 255.255.255.0`	
`duplex auto`	
`speed auto`	
`!`	
`voice-port 1/0/0`	
`!`	
`voice-port 1/0/1`	
`!`	
`dial-peer voice 1113 pots`	
`application session`	***configured for call transfer**
`destination-pattern 3921113`	
`port 1/0/0`	
`!`	
`dial-peer voice 1 voip`	
`application session`	***configured for call transfer**
`destination-pattern 3......`	
`session protocol sipv2`	***configures the dial peer to use IETF SIP**
`session target sip-server`	***configures the session target as the global SIP server; each dial peer could also be configured with different DNS names or IP addresses specifying different SIP servers or gateways**
`codec g711ulaw`	
`!`	
`sip-ua`	
`sip-server dns:csps1.cisco.com`	***configures the global sip server by specifying either a valid DNS name or IP address. Only one server can be configured, although it can be the name of the Cisco SPS farm**
`!`	
`end`	

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Cisco 7960 SIP IP Phone

This section describes the files that are required to configure and operate the Cisco 7960 SIP IP phone. Optional files that are not listed include RINGLIST.DAT, which lists audio files for custom ring type options, dialplan.xml, which contains a sample North American dial plan, and syncinfo.xml, which controls the image version and synchronization values for remote reboots.

It is assumed that the phone is provisioned, via DHCP or static configuration, with an IP address, subnet mask, TFTP server, default router, domain name, and DNS server.

Phone Files on TFTP Server

File	**Required/Optional**	**Description**
OS79XX.TXT	Required	Enables the phone to automatically determine and initialize for the correct VoIP environment (SIP, SCCP, etc.). If the firmware image listed in this file is different from the image currently running on the phone, the phone downloads the correct image from the TFTP server.
SIPDefault.cnf	Optional (recommended)	Contains configuration parameters common to all SIP phones. Cisco recommends using this generic file so that all global phone parameters can be stored and updated in one place.
SIP<Phone_MAC_Address>.cnf	Required	Contains configuration parameters specific to an individual phone.
P0S3xxyy.bin or P0S3-xx-y-zz.bin	Required	Contains the SIP IP phone firmware image. The P03xxyy.bin format represents images 2.3 and earlier. The P0S3-xx-y-zz.bin represents images 3.0 and later. Remember, phones running firmware version 2.1 and earlier require a different upgrade procedure from phones running firmware version 2.2 and later. Refer to the administrator guide for details.

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

OS79XX.TXT File

```
P0S3-04-3-00
```

SIPDefault.cnf

```
# SIP Default Generic Configuration File
#Image Version
```

image_version: P0S3-04-3-00	***indicates the firmware version on a global basis; once the phone is operating in a SIP environment, this parameter takes precedence over the version specified in the OS79XX.TXT file**

```
# Proxy Server
```

proxy1_address: 1.1.1.2	; Can be dotted IP or FQDN
proxy2_address: ""	; Can be dotted IP or FQDN
proxy3_address: ""	; Can be dotted IP or FQDN
proxy4_address: ""	; Can be dotted IP or FQDN
proxy5_address: ""	; Can be dotted IP or FQDN
proxy6_address: ""	; Can be dotted IP or FQDN

```
# Proxy Server Port (default - 5060)
proxy1_port: 5060
proxy2_port: 5060
proxy3_port: 5060
proxy4_port: 5060
proxy5_port: 5060
proxy6_port: 5060
# Proxy Registration (0-disable (default), 1-enable)
```

proxy_register: 1

```
# Phone Registration Expiration [1-3932100 sec] (Default - 3600)
timer_register_expires: 3600
# Codec for media stream (g711ulaw (default), g711alaw, g729a)
preferred_codec: g711ulaw
# TOS bits in media stream [0-5] (Default - 5)
tos_media: 5
# Inband DTMF Settings (0-disable, 1-enable (default))
dtmf_inband: 1
# Out of band DTMF Settings (none-disable, avt-avt enable (default), avt_always - always avt )
dtmf_outofband: avt
# DTMF dB Level Settings (1-6dB down, 2-3db down, 3-nominal (default), 4-3db up, 5-6dB up)
dtmf_db_level: 3
# SIP Timers
timer_t1: 500                              ; Default 500 msec
timer_t2: 4000                             ; Default 4 sec
sip_retx: 10                               ; Default 10
```


Copyright © 2003 Cisco Systems, Inc. All rights reserved.

```
sip_invite_retx: 6                             ; Default 6
timer_invite_expires: 180                      ; Default 180 sec
####### New Parameters added in Release 2.0 #######
# Dialplan template (.xml format file relative to the TFTP root directory)
```

dial_template: dialplan ***needed if using the optional dialplan.xml file**

```
# TFTP Phone Specific Configuration File Directory
```

tftp_cfg_dir: "" **; Example: ./sip_phone/**

***leave blank if files are located in the TFTP server root directory**

```
# Time Server (There are multiple values and configurations refer to Admin Guide for Specifics)
sntp_server: ""                                ; SNTP Server IP Address
sntp_mode: directedbroadcast                   ; unicast, multicast, anycast, or directedbroadcast
(default)
time_zone: GMT                                 ; Time Zone Phone is in
dst_offset: 1                                  ; Offset from Phone's time when DST is in effect
dst_start_month: April                         ; Month in which DST starts
dst_start_day: ""                              ; Day of month in which DST starts
dst_start_day_of_week: Sun                     ; Day of week in which DST starts
dst_start_week_of_month: 1                     ; Week of month in which DST starts
dst_start_time: 02                             ; Time of day in which DST starts
dst_stop_month: Oct                            ; Month in which DST stops
dst_stop_day: ""                               ; Day of month in which DST stops
dst_stop_day_of_week: Sunday                   ; Day of week in which DST stops
dst_stop_week_of_month: 8                      ; Week of month in which DST stops 8=last week of
month
dst_stop_time: 2                               ; Time of day in which DST stops
dst_auto_adjust: 1                             ; Enable(1-Default)/Disable(0) DST automatic
adjustment
time_format_24hr: 1                            ; Enable(1 - 24Hr Default)/Disable(0 - 12Hr)
# Do Not Disturb Control (0-off, 1-on, 2-off with no user control, 3-on with no user control)
dnd_control: 0                                 ; Default 0 (Do Not Disturb feature is off)
# Caller ID Blocking (0-disbaled, 1-enabled, 2-disabled no user control, 3-enabled no user
control)
callerid_blocking: 0                           ; Default 0 (Disable sending all calls as anonymous)
# Anonymous Call Blocking (0-disabled, 1-enabled, 2-disabled no user control, 3-enabled no user
control)
anonymous_call_block: 0                        ; Default 0 (Disable blocking of anonymous calls)
# DTMF AVT Payload (Dynamic payload range for AVT tones - 96-127)
dtmf_avt_payload: 101                          ; Default 101
# Sync value of the phone used for remote reset
```

sync: 1 **; Default 1**

***needed if using the syncinfo.xml file**

```
####### New Parameters added in Release 2.1 #######
```


Copyright © 2003 Cisco Systems, Inc. All rights reserved.

```
# Backup Proxy Support
proxy_backup: 1.1.1.2                      ; Dotted IP of Backup Proxy
```

***a value needs to be configured for the proxy_backup parameter even if no backup proxy server is used; this value will be used to support SIP-SRST in the future**

```
proxy_backup_port: 5060                    ; Backup Proxy port (default is 5060)
# Emergency Proxy Support
proxy_emergency                            ; Dotted IP of Emergency Proxy
proxy_emergency_port: 5060                 ; Emergency Proxy port (default is 5060)
# Configurable VAD option
enable_vad: 0                              ; VAD setting 0-disable (Default), 1-enable
####### New Parameters added in Release 2.2 ######
# NAT/Firewall Traversal
nat_enable: 0                               ; 0-Disabled (default), 1-Enabled
nat_address: ""                             ; WAN IP address of NAT box (dotted IP or DNS A
record only)
voip_control_port: 5060                    ; UDP port used for SIP messages (default - 5060)
start_media_port: 16384                    ; Start RTP range for media (default - 16384)
end_media_port: 32766                      ; End RTP range for media (default - 32766)
nat_received_processing: 0                 ; 0-Disabled (default), 1-Enabled
# Outbound Proxy Support
outbound_proxy: ""                         ; restricted to dotted IP or DNS A record only
outbound_proxy_port: 5060                  ; default is 5060
####### New Parameter added in Release 3.0 #######
# Allow for the bridge on a 3way call to join remaining parties upon hangup
cnf_join_enable : 1                        ; 0-Disabled, 1-Enabled (default)
####### New Parameters added in Release 3.1 #######
# Allow Transfer to be completed while target phone is still ringing
semi_attended_transfer: 1                  ; 0-Disabled, 1-Enabled (default)
# Telnet Level (enable or disable the ability to telnet into the phone)
telnet_level: 2                            ; 0-Disabled (default), 1-Enabled, 2-Privileged
####### New Parameters added in Release 4.0 #######
# XML URLs
services_url: ""                           ; URL for external Phone Services
directory_url: ""                          ; URL for external Directory location
logo_url: ""                               ; URL for branding logo to be used on phone display
# HTTP Proxy Support
http_proxy_addr: ""                        ; Address of HTTP Proxy server
http_proxy_port: 80                        ; Port of HTTP Proxy Server (80-default)
# Dynamic DNS/TFTP Support
dyn_dns_addr_1: ""                         ; restricted to dotted IP
dyn_dns_addr_2: ""                         ; restricted to dotted IP
dyn_tftp_addr: ""                          ; restricted to dotted IP
# Remote Party ID
```


Copyright © 2003 Cisco Systems, Inc. All rights reserved.

```
remote_party_id: 0                    ; 0-Disabled (default), 1-Enabled
```

SIP<Phone_MAC_Address>.cnf

```
# SIP Configuration Generic File
#Line 1 appearance
```

line1_name: 3921111	***number or e-mail address used when registering with the Cisco SPS; do not use dashes for number or host names for e-mail addresses (this is different from SCCP phones that are provisioned on the Cisco CallManager)**

```
# Line 1 Registration Authentication
```

line1_authname: sipphone	***authentication name used by the phone if the Cisco SPS is configured to authenticate REGISTER and INVITE methods**

```
# Line 1 Registration Password
```

line1_password: cisco	***authentication password used by the phone if the Cisco SPS is configured to authenticate REGISTER and INVITE methods**

```
# Line 2 appearance
line2_name:
# Line 2 Registration Authentication
line2_authname: "UNPROVISIONED"
# Line 2 Registration Password
line2_password: "UNPROVISIONED"
####### New Parameters added in Release 2.0 #######
# All user_parameters have been removed
# Phone Label (Text desired to be displayed in upper right corner)
phone_label:                          ; Has no effect on SIP messaging
# Line 1 Display Name (Display name to use for SIP messaging)
```

line1_displayname: 3921111	***used for caller-identification purposes; can be a number, name, or e-mail address**

```
# Line 2 Display Name (Display name to use for SIP messaging)
line2_displayname: ""
####### New Parameters added in Release 3.0 ######
# Phone Prompt (The prompt that will be displayed on console and telnet)
phone_prompt:   sipphone               ; Limited to 15 characters (Default - SIP Phone)
# Phone Password (Password to be used for console or telnet login)
phone_password:                       ; Limited to 31 characters (Default - cisco)
# User classification used when Registering [ none(default), phone, ip ]
user_info: phone
```

Cisco Confidential
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Troubleshooting & Verification

This section contains some basic verification and troubleshooting commands for the Cisco SPS, Cisco IOS gateways, and Cisco 7960 SIP IP phones.

Cisco SIP Proxy Server

1) Activate the appropriate debug flags and set the log level to debug on the Debug and Logs interface.

2) Use the **ps –ef | grep –i sip** command to ensure that all necessary processes are running for the Cisco SPS to operate.

3) Review the log files for information. The error_log file provides details regarding SIP signaling. You can also use the **tail –f <log_file>** command to view real-time information on the screen.

4) One of the most common issues with Cisco SPS relates to DNS. Before installing Cisco SPS and running the csps_setup script, make sure that the machine has not only an IP address, subnet mask, and default route, but also a valid DNS host name. You can accomplish this in two ways: 1) add the host name to a local DNS server or 2) if no DNS server is available, use the host file to resolve the name. In order to force the machine to search the host file before using DNS, create an additional file, called irs.conf, and add it to the /etc directory. The file needs to contain the following lines:

```
hosts local continue
hosts dns
```

5) Use the ./sysadmin_csps_regroute tool to verify dynamically registered users.

Cisco IOS Gateways

1) To verify functionality, use these commands:

    a. **show dial-peer voice <number> | summary |** <cr>

    b. **show sip-ua statistics**

    c. **show sip-ua status**

2) To troubleshoot issues, use these commands:

    a. **debug ccsip all**

    b. **debug ccsip messages**

    c. **debug voip ccapi inout**

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Cisco 7960 SIP IP Phones

1) To verify functionality, use these commands:

   a. **show register**

   b. **show status**

2) To troubleshoot issues, use the command:

   a. **show config**

   b. **debug error sip-messages sip-state**

References

- *Cisco SIP Proxy Server Administrator Guide*
  http://www.cisco.com/en/US/products/sw/voicesw/ps2157/prod_technical_documentation.html

- *Cisco SIP Proxy Server CD Installation Instructions*
  http://www.cisco.com/en/US/products/sw/voicesw/ps2157/prod_technical_documentation.html

- *Cisco SIP IP Phone 7940/7960 Administrator Guide*, Version 4.0
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/sip7960/sadmin31/index.htm

- *Configuring Session Initiation Protocol for Voice over IP*, IOS Version 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfsip.htm

- *SIP: Session Initiation Protocol*
  http://www.jdrosen.net/papers/draft-ietf-sip-rfc2543bis-04.txt

Copyright © 2003 Cisco Systems, Inc. All rights reserved.