



Supplementary Services Features Roadmap

First Published: August 1, 2008

This roadmap lists the features covered in this document and provides links to specific configuration information. To reach links to specific feature documentation and to see a list of the releases in which each feature is supported, see the following tables:

- [Table 1](#) lists features by the Cisco IOS Release in which they were introduced.
- [Table 2](#) lists features alphabetically by feature name.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.



Note

[Table 1](#) lists only the Cisco IOS software releases that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 *Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Cisco IOS Release*

Releases	Feature Name	Feature Information	Where Documented
15.1(3)T	CallBack on No Answer for Analog Phones	Provides CallBack notification when a called phone becomes available. This feature is supported on analog SCCP endpoints in Cisco Unified CM only.	Configuring CallBack on No Answer for Analog Phones
15.1(3)T	cBarge for Shared Lines	Allows idle IP or analog phones that are connected to the same FXS ports on a Cisco VG2nn Analog Gateway to automatically join already active calls on the same shared lines by simply going offhook. This feature is supported in Cisco Unified CM only.	Configuring cBarge and Privacy for Shared Lines
15.1(3)T	Configurable AMWI and VMWI	Allows users to configure AMWI only, VMWI only, or both.	Configuring AMWI and VMWI
15.1(3)T	Configurable Call Waiting Tone Cadence	Allows the call waiting tone to continuously play when the called party has not switched to the new call and the new caller has not hung up.	Configuring Call Waiting Tone Cadence

Table 1 *Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Cisco IOS Release (continued)*

Releases	Feature Name	Feature Information	Where Documented
15.1(3)T	Enhanced Serviceability	Provides line measurement and connectivity check support for analog voice ports.	Implementing Enhanced Serviceability
15.1(3)T	Media Renegotiation	Enhances the STCAPP state machine to support any of the most possible sequences of the media setup messages.	Media Renegotiation
15.1(3)T	Privacy for Shared Line Phones	Disallows other users to cBarge into active calls on the same FXS ports on a Cisco VG2nn Analog Gateway. This feature is supported in Cisco Unified CM only.	Configuring cBarge and Privacy for Shared Lines
15.1(3)T	Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager	Enhances STCAPP FXS security analog endpoints through secure signaling and media encryption using TLS. This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified CM only.	Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager
15.1(3)T	Single Number Reach for Analog Phones	Enables incoming calls to analog phones connected to Cisco gateway FXS ports to be received on predefined alternate telephone numbers.	Configuring Single Number Reach for Analog Phones
15.1(1)T 15.0(1)XA	MLPP Support for Supplementary Services on SCCP Controlled Analog Endpoints	<p>Adds Multilevel Priority and Preemption (MLPP) support of supplementary services such as Call Hold, Call Forwarding, Call Transfer, Call Pickup, Conferencing, Call Waiting, and Cancel Call Waiting.</p> <p>MLPP service allows validated users to place priority calls and, if necessary, to preempt lower-priority calls.</p>	<p>See the documentation for your call-control system:</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager Maintain and Operate Guides • Cisco Unified CME System Administrator Guide
15.1(1)T 15.0(1)XA	Cancel Call Waiting	Adds FAC for Cancel Call Waiting feature.	Cancel Call Waiting
15.0(1)M	Flexible FACs in Feature Mode	Allows you to configure 1 to 4-character feature access codes (FACs) for accessing supplementary features that are supported in feature mode.	Configuring Feature Mode
12.4(20)YA	CallBack on Busy for Analog Phones	Provides callback notification when a busy called line becomes free. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.	Configuring CallBack on Busy

Table 1 Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Cisco IOS Release (continued)

Releases	Feature Name	Feature Information	Where Documented
12.4(20)YA	Call Hold/Resume for Shared Lines for SCCP Analog Ports	Enables an analog phone on a shared line to use hookflash to hold and resume an active call. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.	Configuring Call Hold/Resume for Shared Lines
	DC Voltage Based VMWI for SCCP Controlled Analog Ports	Notifies user on certain analog phones that support a DC voltage-controlled MWI lamp that there are messages waiting.	Configuring DC Voltage Based VMWI for SCCP Controlled Analog Ports
	Flexible Feature Access Codes	Allows you to configure 2 to 4-character feature codes for Feature Access Codes (FACs) and the speed-dial code for Redial so that phone users are not required to dial the prefix before dialing a feature code.	Flexible Feature Access Codes
	SCCP Meet-Me Conference	User on an analog SCCP phone can start or join a meet-me conference call.	SCCP Meet-Me Conference
	SIP Supplementary Features	Enables SIP supplementary features on analog FXS ports on a Cisco ISR or Cisco VG224 and under the control of Cisco Unified Communications Manager, including: <ul style="list-style-type: none"> • Call Hold/Resume • Three Way Calling • Call Transfer • Call Waiting. 	“Configuring SIP Support for Hookflash” module of the Cisco IOS SIP Configuration Guide, Release 12.4T
12.4(20)T 12.4(11)XW	Media Encryption (SRTP) on Cisco Unified CME	Provides secure voice call capabilities including secure Cisco VG224.	Configuring Secure Signaling and Media Encryption for the Cisco VG224

Table 1 *Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Cisco IOS Release (continued)*

Releases	Feature Name	Feature Information	Where Documented
12.4(11)T 12.4(6)XE	Feature Mode for SCCP FXS Ports in Cisco IOS	Enables feature mode call control on analog FXS ports on Cisco voice gateways and under the control of Cisco Unified Communications Manager or Cisco Unified CME.	Configuring Feature Mode
	DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS	Enhances the transmission of DTMF digits, faxes and modems between SCCP FXS ports on Cisco voice gateways. DTMF digit transmission is supported by using RFC 2833. Cisco Fax Relay, Cisco T.38 Fax Relay, and Cisco Modem Relay are supported using Names Signaling Events (NSE).	Configuring DTMF Relay, Fax Relay, and Modem Relay
	SCCP Gateway Dial Tone Generation After Remote Onhook	Provides PBX interoperability by enabling configurable automatic dial tone capability after remote call disconnect.	Configuring SCCP Gateway Dial Tone Generation After Remote Onhook
	Hookflash Duration	Enables modification of the upper limit of the hookflash duration range for an analog FXS port.	Hookflash Duration
	SCCP Gateway Ground Start FXS Ports	Converts loop-start FXS ports to ground start to support power denial-based supervisory disconnect capability.	Ground Start FXS Ports as SCCP Analog Endpoints
12.4(9)T	SCCP PLAR with DTMF Out-Pulse Digits for FXS Analog Phones	Adds private line automatic ring-down (PLAR) support and enhanced speed-dial capabilities for SCCP analog ports on a Cisco voice gateway.	PLAR with DTMF Out-Pulse Digits
	Supervisory Disconnect	Provides a disconnect indication to the remote party in a two-party call after one side disconnects and enables external applications connected to the Cisco voice gateway to promptly clear a call after receiving the disconnect indication.	Configuring Supplementary Features
12.4(6)T	Enhanced Speed Dial on SCCP Analog Phones	Allows you to define two-digit speed-dial codes for accessing up to 99 local speed-dial numbers configured on the call-control device.	Enhanced Speed Dial on SCCP Analog Phones
12.4(2)T	SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways	Enables supplementary features on SCCP-controlled analog FXS ports on a Cisco ISR or Cisco VG224.	Configuring Supplementary Features

Table 2 Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Feature Name

Feature Name	Releases	Feature Information	Where Documented
CallBack on Busy for Analog Phones	12.4(20)YA	Provides callback notification when a busy called line becomes free. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.	Configuring CallBack on Busy
CallBack on No Answer for Analog Phones	15.1(3)T	Provides CallBack notification when a called phone becomes available. This feature is supported on analog SCCP endpoints in Cisco Unified CM only.	Configuring CallBack on No Answer for Analog Phones
Call Hold/Resume for Shared Lines for SCCP Analog Ports	12.4(20)YA	Enables an analog phone on a shared line to use hookflash to hold and resume an active call. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.	Configuring Call Hold/Resume for Shared Lines
Cancel Call Waiting	15.1(1)T 15.0(1)XA	Adds FAC for Cancel Call Waiting feature.	Cancel Call Waiting
cBarge for Shared Lines	15.1(3)T	Allows idle IP or analog phones that are connected to the same FXS ports on a Cisco VG2nn Analog Gateway to automatically join already active calls on the same shared lines by simply going offhook. This feature is supported in Cisco Unified CM only.	Configuring cBarge and Privacy for Shared Lines
Configurable AMWI and VMWI	15.1(3)T	Allows users to configure AMWI only, VMWI only, or both.	Configuring AMWI and VMWI
Configurable Call Waiting Tone Cadence	15.1(3)T	Allows the call waiting tone to continuously play when the called party has not switched to the new call and the new caller has not hung up.	Configuring Call Waiting Tone Cadence
DC Voltage Based VMWI for SCCP Controlled Analog Ports	12.4(20)YA	Notifies user on certain analog phones that support a DC voltage-controlled MWI lamp that there are messages waiting.	Configuring DC Voltage Based VMWI for SCCP Controlled Analog Ports
DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS	12.4(11)T 12.4(6)XE	Enhances the transmission of DTMF digits, faxes and modems between SCCP FXS ports on Cisco voice gateways. DTMF digit transmission is supported by using RFC 2833. Cisco Fax Relay, Cisco T.38 Fax Relay, and Cisco Modem Relay are supported using Names Signaling Events (NSE).	Configuring DTMF Relay, Fax Relay, and Modem Relay
Enhanced Serviceability	15.1(3)T	Provides line measurement and connectivity check support for analog voice ports.	Implementing Enhanced Serviceability
Enhanced Speed Dial on SCCP Analog Phones	12.4(6)T	Allows you to define two-digit speed-dial codes for accessing up to 99 local speed-dial numbers configured on the call-control device.	Enhanced Speed Dial on SCCP Analog Phones
Feature Mode for SCCP FXS Ports in Cisco IOS	12.4(11)T 12.4(6)XE	Enables feature mode call control on analog FXS ports on Cisco voice gateways and under the control of Cisco Unified Communications Manager or Cisco Unified CME.	Configuring Feature Mode
Flexible FACs in Feature Mode	15.0(1)M	Allows you to configure 1 to 4-character feature access codes for accessing supplementary features that are supported in feature mode.	Configuring Feature Mode

Table 2 *Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Feature Name (continued)*

Feature Name	Releases	Feature Information	Where Documented
Flexible Feature Access Codes	12.4(20)YA	Allows you to configure 2 to 4-character feature codes for Feature Access Codes (FACs) and the speed-dial code for Redial so that phone users are not required to dial the prefix before dialing a feature code.	Flexible Feature Access Codes
Hookflash Duration	12.4(11)T 12.4(6)XE	Enables modification of the upper limit of the hookflash duration range for an analog FXS port.	Hookflash Duration
Media Encryption (SRTP) on Cisco Unified CME	12.4(20)T 12.4(11)XW	Provides secure voice call capabilities including secure Cisco VG224.	Configuring Secure Signaling and Media Encryption for the Cisco VG224
Media Renegotiation	15.1(3)T	Enhances the STCAPP state machine to support any of the most possible sequences of the media setup messages.	Media Renegotiation
MLPP Support for Supplementary Services on SCCP Controlled Analog Endpoints	15.1(1)T 15.0(1)XA	Adds Multilevel Priority and Preemption (MLPP) support of supplementary services such as Call Hold, Call Forwarding, Call Transfer, Call Pickup, Conferencing, Call Waiting, and Cancel Call Waiting. MLPP service allows validated users to place priority calls and, if necessary, to preempt lower-priority calls.	See the documentation for your call-control system: <ul style="list-style-type: none"> • Cisco Unified Communications Manager Maintain and Operate Guides • Cisco Unified CME System Administrator Guide
Privacy for Shared Line Phones	15.1(3)T	Disallows other users to cBarge into active calls on the same FXS ports on a Cisco VG2nn Analog Gateway. This feature is supported in Cisco Unified CM only.	Configuring cBarge and Privacy for Shared Lines
SCCP Gateway Dial Tone Generation After Remote Onhook	12.4(11)T 12.4(6)XE	Provides PBX interoperability by enabling configurable automatic dial tone capability after remote call disconnect.	Dial Tone Generation after Remote Onhook
SCCP Gateway Ground Start FXS Ports	12.4(11)T 12.4(6)XE	Converts loop-start FXS ports to ground start to support power denial-based supervisory disconnect capability.	Ground Start FXS Ports as SCCP Analog Endpoints
Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager	15.1(3)T	Enhances STCAPP FXS security analog endpoints through secure signaling and media encryption using TLS. This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified CM only.	Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager
Single Number Reach for Analog Phones	15.1(3)T	Enables incoming calls to analog phones connected to Cisco gateway FXS ports to be received on predefined alternate telephone numbers.	Configuring Single Number Reach for Analog Phones

Table 2 Feature Information for Supplementary Services Features for Analog FXS Ports on Cisco Voice Gateways, by Feature Name (continued)

Feature Name	Releases	Feature Information	Where Documented
SIP Supplementary Features	12.4(20)YA	Enables SIP supplementary features on analog FXS ports on a Cisco ISR or Cisco VG224 and under the control of Cisco Unified Communications Manager, including: <ul style="list-style-type: none"> • Call Hold/Resume • Three Way Calling • Call Transfer • Call Waiting. 	“Configuring SIP Support for Hookflash” chapter of the Cisco IOS SIP Configuration Guide, Release 12.4T
SCCP Meet-Me Conference	12.4(20)YA	User on an analog SCCP phone can start or join a meet-me conference call.	SCCP Meet-Me Conference
SCCP PLAR with DTMF Out-Pulse Digits for FXS Analog Phones	12.4(9)T	Adds private line automatic ring-down (PLAR) support and enhanced speed-dial capabilities for SCCP analog ports on a Cisco voice gateway.	PLAR with DTMF Out-Pulse Digits
Supervisory Disconnect	12.4(9)T	Provides a disconnect indication to the remote party in a two-party call after one side disconnects and enables external applications connected to the Cisco voice gateway to promptly clear a call after receiving the disconnect indication.	Configuring Supplementary Features

Additional References

The following sections provide references related to supplementary features for analog phones connected to FXS ports on a Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library

Related Topic	Document Title
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateways • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Integrated Services Routers • Cisco 3800 Series Integrated Services Routers • Cisco Unified 500 Series for Small Business
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport



Overview of Supplementary Services Features for FXS Ports on Cisco Voice Gateways

First Published: June 27, 2005

Last Updated: November 19, 2010

This guide contains information and tasks for configuring supplementary service feature capabilities for analog phones connected to Foreign Exchange Station (FXS) ports on Cisco Integrated Services Routers (ISRs) or Cisco VG224 Analog Phone Gateways, including call transfer and forward, conferencing, caller ID, speed dial and redial, and more.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Notices, page 9](#)
- [Information About Supplementary Services Features for FXS Ports on Cisco Voice Gateways, page 11](#)
- [Additional References, page 14](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 15](#)

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Information About Supplementary Services Features for FXS Ports on Cisco Voice Gateways

To enable supplementary services feature capabilities for analog phones connected to FXS ports on Cisco voice gateways, you should understand the following concepts:

- [Cisco Voice Gateway Interoperability with Cisco Unified Communications Manager or Cisco Unified CME, page 12](#)
- [Supported Gateways, Modules, and Voice Interface Cards, page 13](#)

Cisco Voice Gateway Interoperability with Cisco Unified Communications Manager or Cisco Unified CME

A standard telephone can be directly connected to an FXS port, which supplies the ring feature, voltage, and the dial tone. Cisco IOS Release 12.4(2)T and later releases provide supplementary feature capabilities for analog phones connected to FXS ports on a Cisco ISR or Cisco VG224.

Calls through analog FXS ports are controlled by a Cisco call-control system, such as Cisco Unified Communications Manager or Cisco Unified CME. The SCCP telephony control (STC) application on the Cisco voice gateway functions as a proxy to translate call-control messages between the Cisco call-control system and the Cisco voice gateway.

The STC application identifies locally attached analog telephones as individual endpoints to the call-control system, which allows the analog phones to be controlled in the same way as IP phones. With this capability, organizations such as retailers are able to connect traditional analog telephones to a Cisco voice gateway and share the same telephony features that are available on IP phones directly connected to Cisco Unified CME.

Figure 1 shows analog phones connected through the Cisco voice gateway to a remote Cisco Unified Communications Manager system. Figure 2 shows analog phones connected through the voice gateway to a local Cisco Unified CME router.

Figure 1 Analog Endpoints Managed by Cisco Unified Communications Manager

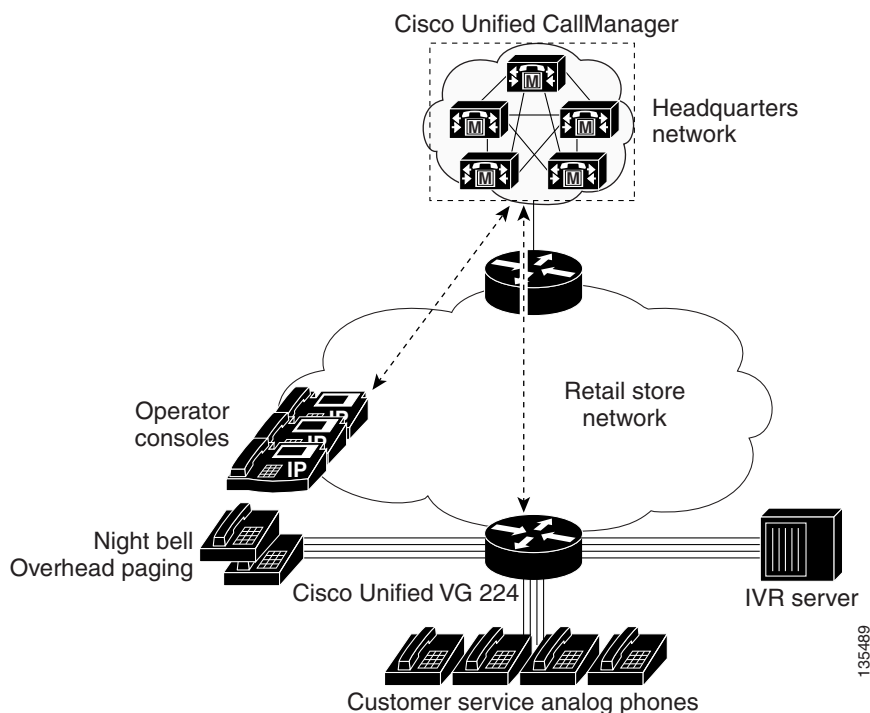
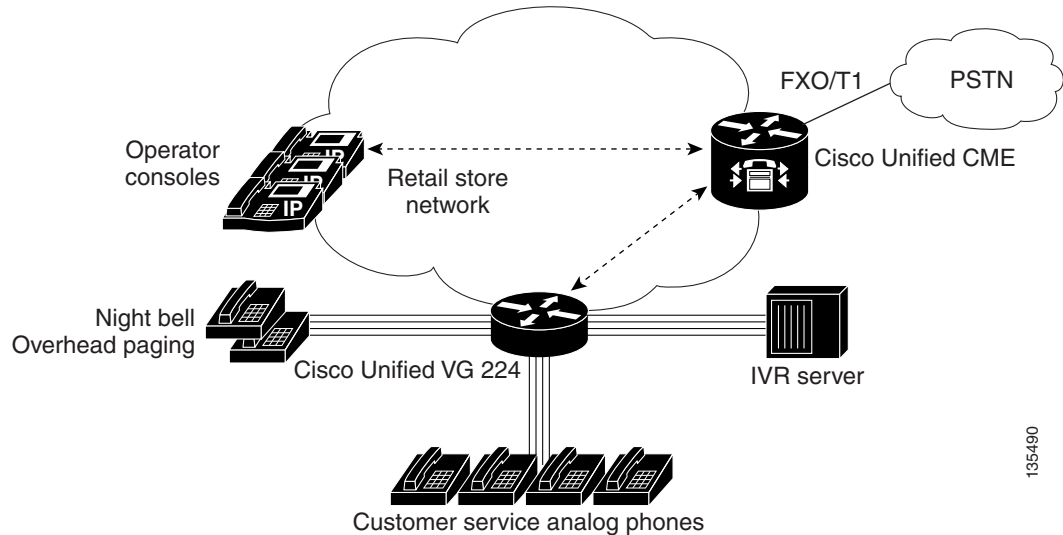


Figure 2 Analog Endpoints Managed by Cisco Unified CME



135490

Supported Gateways, Modules, and Voice Interface Cards

Table 1 lists Cisco voice gateways, modules, and voice interface cards (VICs) on which supplementary services for FXS ports are supported.



Note

Not all supplementary feature capabilities for FXS ports are supported on all gateways, modules, and VICs. If a feature is not supported on a certain hardware configuration, it is specified in the module for that feature.

Table 1 Supported Gateways, Modules, and VICs

Supported Gateways	Supported Extension Modules	Supported Network Modules and Expansion Modules	Supported VICs
<ul style="list-style-type: none"> • Cisco 1861 	—	<ul style="list-style-type: none"> • HWIC-1T1/E1 	—
<ul style="list-style-type: none"> • Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845 	—	<ul style="list-style-type: none"> • NM-HD-1V • NM-HD-2V • NM-HD-2VE 	<ul style="list-style-type: none"> • VIC2-2FXS • VIC-4FXS/DID • VIC2-2BRI-NT/TE

Table 1 Supported Gateways, Modules, and VICs

Supported Gateways	Supported Extension Modules	Supported Network Modules and Expansion Modules	Supported VICs
<ul style="list-style-type: none"> • Cisco 2801 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845 	<ul style="list-style-type: none"> • EVM-HD 	<ul style="list-style-type: none"> • EVM-HD-8FXS/DID • EM-3FXS/4FXO • EM-HDA-8FXS • EM-4BRI-NT/TE 	—
<ul style="list-style-type: none"> • Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845 	—	<ul style="list-style-type: none"> • NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1 	<ul style="list-style-type: none"> • VIC2-2FXS • VIC-4FXS/DID • VIC2-2BRI-NT/TE
<ul style="list-style-type: none"> • Cisco Unified 500 Series 	—	—	<ul style="list-style-type: none"> • VIC3-2FXS/DID* • VIC-4FXS/DID* • VIC3-4FXS/DID* • VIC2-2BRI-NT/TE*
<ul style="list-style-type: none"> • Cisco VG202 • Cisco VG204 • Cisco VG224 	—	—	—

* Factory option. Only one optional VIC can be factory-installed in a Cisco Unified 500 Series.

Additional References

The following sections provide references related to support for supplementary services on FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library

Related Topic	Document Title
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateways • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Integrated Services Routers • Cisco 3800 Series Integrated Services Routers • Cisco Unified 500 Series for Small Business
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.



Configuring FXS Ports for Basic Calls

First Published: October 2, 2008
Last updated: September 4, 2015

This module describes how to configure analog Foreign Exchange Station (FXS) ports on a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway for basic calls.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation and to see a list of the releases in which each feature is supported, see the “[Feature Information for Configuring FXS Ports for Basic Calls](#)” section on page 45.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring FXS Ports for Basic Calls, page 17](#)
- [Information About FXS Ports for Basic Calls, page 18](#)
- [How to Configure FXS Ports for Basic Calls, page 21](#)
- [Configuration Examples for Configuring FXS Ports for Basic Calls, page 39](#)
- [Additional References, page 44](#)

Prerequisites for Configuring FXS Ports for Basic Calls

Cisco IOS Gateway

- The Cisco voice gateway must be set up and configured for operation. For a list of supported Cisco voice gateways, see the “[Overview of Supplementary Services Features for FXS Ports on Cisco Voice Gateways](#)” section on page 9. For configuration information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the [Cisco IOS Voice Port Configuration Guide](#).

Analog Endpoints in Cisco Unified Communications Manager

- Cisco Unified Communications Manager 4.2 or a later version.
- Cisco voice gateway analog Foreign Exchange Station (FXS) ports are added in Cisco Unified Communications Manager. Each analog FXS port on which SCCP is enabled counts as a single IP phone for licensing purposes. For example, to register all 24 ports on a Cisco VG224 Analog Phone Gateway, the 24 ports count toward the 2500 limit if you purchase a Cisco Unified Communications Manager license for 2500 devices.

Analog Endpoints in Cisco Unified CME

- Basic feature license and phone user licenses are purchased. For licensing purposes, each analog FXS port on which SCCP is enabled counts as a single phone.

Information About FXS Ports for Basic Calls

To configure FXS ports for basic calls, you should understand the following concepts:

- [Hookflash Duration, page 18](#)
- [PLAR with DTMF Out-Pulse Digits, page 19](#)
- [Dial Tone Generation after Remote Onhook, page 19](#)
- [Ground Start FXS Ports as SCCP Analog Endpoints, page 20](#)
- [Supervisory Disconnect, page 20](#)

Hookflash Duration

Analog phones use hookflash to access a second dial tone to initiate certain SCCP phone features such as transfer and conference. Hookflash is an on-hook condition of short duration that is usually generated when a phone user presses the Flash button on a phone. The duration of an on-hook condition generated by a Flash button varies for different phone makes and models. Cisco voice gateways measure the duration of detected on-hook conditions to determine whether they should be interpreted as hookflash or not. The duration of a detected on-hook condition is interpreted by Cisco IOS software as follows:

- An on-hook condition that lasts for a time period that falls inside the hookflash duration range is considered a hookflash.
- An on-hook condition that lasts for a shorter period than the lower limit of the range is ignored.
- An on-hook condition that lasts for a longer period than the higher limit of the range is considered a disconnect.

The hookflash duration range for FXS ports is defined as follows:

- The lower limit of the range is set in software at 150 ms, although there is also a hardware-imposed lower limit that is typically about 20 ms, depending on platform type. An on-hook condition that lasts for a shorter time than this hardware-imposed lower limit is not reported to the Cisco IOS software.
- The upper limit of the range is set in software at 1000 ms by default, although this value can be changed on the voice gateway. The upper limit can be set to any value from 50 to 1550 ms.

- If the upper limit of the hookflash duration range is X, a value greater than 150, then any on-hook duration between 150 and X is interpreted as a hookflash. For example, if X is 1550, the hookflash duration range is 150 to 1550 ms. An on-hook signal that lasts for 1250 ms is interpreted as a hookflash, and an on-hook signal of 55 ms is ignored.
- If the upper limit of the hookflash duration range is X, a value less than 150, then any on-hook duration between Y, the hardware lower limit, and X is interpreted as a hookflash. For example, if X is 65, the hookflash duration range is Y to 65 ms (assume Y is 20 ms). An on-hook signal that lasts for 1250 ms is interpreted as a disconnect, and an on-hook signal of 55 ms is interpreted as a hookflash. An on-hook signal of less than Y is ignored.

For information about modifying the upper limit of the hookflash duration range, see the [“Modifying Hookflash” section on page 27](#).

PLAR with DTMF Out-Pulse Digits

A private line automatic ring-down (PLAR) connection allows an analog phone user to make a call without dialing any digits. When the user goes off-hook on the phone, the Cisco voice gateway automatically rings a predefined extension or PSTN number. The PLAR number is configured on the analog FXS port to which the corresponding analog phone is connected.

The PLAR with DTMF out-pulse digits feature in Cisco IOS Release 12.4(9)T is an enhancement that enables the voice gateway to out-pulse additional DTMF digits after the PLAR connection is up. These DTMF digits are configurable and can include 0 to 9, A to D, a comma (,) for a one-second pause, an asterisk (*), and number sign (#). If an analog phone user presses a string of digits (0-9, *, #) after taking a PLAR phone off-hook, the voice gateway buffers the digit string until the DTMF digits are done being out-pulsed. After the voice gateway sends all the DTMF digits, it sends the buffered digits to the destination port.

Although users do not hear a dial tone when taking a PLAR phone off-hook, PLAR phones support the same features as other analog phones. PLAR phones can receive incoming calls and support hookflash for basic supplementary features such as call transfer, call waiting, and conference. Feature access codes (FACs) and speed-dial codes are not valid immediately after taking a PLAR phone off-hook, but after connecting to the destination port, a user can press hookflash to get a dial tone and then dial an access code for features such as speed dial, redial, and call transfer.

For configuration information, see the [“Configuring PLAR with DTMF Out-Pulse Digits” section on page 28](#).

Dial Tone Generation after Remote Onhook

The Dial Tone Generation after Remote Onhook feature provides PBX interoperability by enabling configurable automatic dial tone capability after remote call disconnect. Dial tone is automatically generated to the remaining party in a basic A-B call scenario once one party disconnects, in the same way that a PBX user gets immediate dial tone after remote party disconnect. This allows the user to make a new call without hookflash or going onhook, then off hook. If automatic dial tone generation is disabled, the user is required to go onhook then off-hook, or perform a hookflash, in order to make a new call.

After remote onhook there are two ways for an SCCP analog phone to redial, either by the user pressing a redial button or entering a feature access code (FAC). Some phone model redial buttons do not function with the dial tone after remote onhook feature enabled, resulting in redial digits not being sent. For this reason, the dial tone generation after remote onhook feature supports redial only when activated by FAC.

Dial tone generation immediately after the remote party goes onhook is configurable on a per port basis and is enabled by default. Automatic dial tone is supported only on STC application-controlled loop start FXS ports. For devices such as interactive voice response (IVR) systems that require power denial to disconnect properly, power denial is triggered prior to dial tone generation after one party disconnects. For a PLAR port, dial tone is played instead of triggering another PLAR after remote party disconnect. You cannot configure the dial tone generation after remote onhook feature using the Cisco Unified Communications Manager auto configuration capability.

For configuration information, see the [“Configuring SCCP Gateway Dial Tone Generation After Remote Onhook” section on page 32.](#)

Ground Start FXS Ports as SCCP Analog Endpoints

SCCP enhanced supplementary features provide support on the SCCP analog gateway for ground start FXS ports, used for PBX and key system connections, enabling disconnect supervision and Cisco Unified Communications Manager registration. The ground start FXS port feature is supported for basic calls only and supports PBX interoperability by providing supervisory disconnect to FXS ports and analog endpoints. Prior to ground start FXS support, there was no disconnect supervision to signal the end of a call. The ground start FXS ports feature provides power denial-based supervisory disconnect to indicate remote party disconnect using the loop current feed open (LCFO) mechanism.

For configuration information, see the [“Configuring SCCP Gateway Ground Start FXS Ports” section on page 34.](#)

Supervisory Disconnect

The Supervisory Disconnect feature provides a disconnect indication to the remote party in a two-party call after one side disconnects. This enables external applications connected to the Cisco voice gateway to promptly clear a call after receiving the disconnect indication. This feature triggers a power denial on FXS ports with loop-start signaling when a voice call disconnects. The power denial is only generated in a two-party call scenario when one party disconnects. Power denial is not generated if a call is on hold and either the active party or the on-hold party hangs up. Power denial is also not generated for a three-way conference call when one party hangs up. This feature is enabled and disabled on a voice port basis. The remote party receives the power denial signal for the duration that is set on the analog FXS port.

Because the Cisco voice gateway cannot distinguish the type of device connected to the analog FXS port, a power denial signal is sent to all FXS ports that have the power denial feature enabled. This can result in analog phones also receiving a power denial signal after one party disconnects in a two-party call. The remaining party hears a brief click sound. To prevent this behavior on analog phones, you can disable the power denial feature on the analog FSX voice port. For configuration information, see the [“Configuring Supervisory Disconnect” section on page 36.](#)

How to Configure FXS Ports for Basic Calls

**Note**

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

This section contains the following tasks for setting up SCCP analog phone support:

- [Enabling SCCP on the Voice Gateway, page 21](#) (required)
- [Enabling the STC Application for Analog FXS Ports, page 24](#) (required)
- [Modifying Hookflash, page 27](#) (optional)
- [Configuring PLAR with DTMF Out-Pulse Digits, page 28](#) (optional)
- [Configuring SCCP Gateway Dial Tone Generation After Remote Onhook, page 32](#) (optional)
- [Configuring SCCP Gateway Ground Start FXS Ports, page 34](#) (optional)
- [Configuring Supervisory Disconnect, page 36](#) (optional)
- [Verifying and Troubleshooting the Configuration, page 38](#) (optional)

Enabling SCCP on the Voice Gateway

To enable SCCP on the local interface that communicates with your Cisco call-control system and identify priority levels to Cisco Unified Communications Manager servers or Cisco Unified CME routers, perform the following steps.

**Note**

If more than 72 end points are configured with SCCP in a single voice gateway, we recommend you to increase the hold-queue size on the interface of the gateway to 300.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number* [**port** *port-number*]
4. **sccp ccm** {*ip-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] [**version** *version-number*]
5. **sccp**
6. **sccp ccm group** *group-number*
7. **associate ccm** *identifier-number* **priority** *priority-number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>sccp local interface-type interface-number [port port-number]</p> <p>Example: Router(config)# sccp local FastEthernet0/0</p>	<p>Selects the local interface that SCCP applications (transcoding and conference) use to register with Cisco Unified Communications Manager and Cisco Unified CME.</p> <ul style="list-style-type: none"> <i>port-number</i>—(Optional) TCP or UDP port number used by the selected interface. Range: 1025 to 65535. Default: 2000.
Step 4	<p>sccp ccm {ip-address dns} identifier <i>identifier-number</i> [port port-number] [version version-number]</p> <p>Example: Router(config)# sccp ccm 10.8.1.2 identifier 10 version 4.1</p>	<p>Adds a Cisco Unified Communications Manager server or Cisco Unified CME router to the list of available call-control systems.</p> <ul style="list-style-type: none"> Repeat this step to add a backup system.
Step 5	<p>sccp</p> <p>Example: Router(config)# sccp</p>	<p>Enables SCCP and its related applications (transcoding and conferencing).</p>
Step 6	<p>sccp ccm group group-number</p> <p>Example: Router(config)# sccp ccm group 1</p>	<p>Creates a group of Cisco Unified Communications Manager or Cisco Unified CME systems and enters SCCP ccm configuration mode.</p> <ul style="list-style-type: none"> <i>group-number</i>—Number that identifies the group. Range: 1 to 50. Repeat this step to add a backup system.

	Command or Action	Purpose
Step 7	<p>associate ccm <i>identifier-number</i> priority <i>priority-number</i></p> <p>Example: Router(config-sccp-ccm)# associate ccm 1 priority 1</p>	<p>Adds a Cisco Unified Communications Manager server or Cisco Unified CME router to the group and establishes its priority within the group.</p> <ul style="list-style-type: none"> • <i>identifier-number</i>—Identifier that was defined in the sccp ccm command in Step 4. • priority <i>priority-number</i>—Number that indicates the priority of this Cisco Unified Communications Manager server or Cisco Unified CME router. Range: 1 to 4, where 1 is the highest priority. <p>Note A second Cisco Unified Communications Manager or Cisco Unified CME with a lower priority number becomes a backup system.</p> <p>Note The priority must match the order of the call manager group associated with this device within call manager.</p>
Step 8	<p>registration timeout <i>timeout-value</i></p> <p>Example: Router(config-sccp-ccm)# registration timeout 3</p>	<p>(Optional) Sets the length of time between registration messages sent from SCCP to the Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> • Time, in seconds, between registration messages. Range is 1 to 180. Default is 3.
Step 9	<p>keepalive timeout <i>seconds</i></p> <p>Example: Router(config-sccp-ccm)# keepalive timeout 3</p>	<p>(Optional) Sets the length of time between keepalive messages from Skinny Client Control Protocol (SCCP) to Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> • Time between keepalive messages. Range is 1 to 180. Default is 30.
Step 10	<p>connect interval <i>seconds</i></p> <p>Example: Router(config-sccp-ccm)# connect interval 3</p>	<p>(Optional) Specifies the amount of time that a given digital signal processor (DSP) farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.</p> <ul style="list-style-type: none"> • Timer value, in seconds. Range is 1 to 3600. Default is 60.
Step 11	<p>switchback method graceful</p> <p>Example: Router(config-sccp-ccm)# switchback method graceful</p>	<p>(Optional) Sets the Cisco Unified Communications Manager switchback method.</p> <ul style="list-style-type: none"> • graceful—The Cisco Unified Communications Manager switchback happens only after all the active sessions are terminated gracefully.
Step 12	<p>end</p> <p>Example: Router(config-sccp-ccm)# end</p>	<p>Exits SCCP ccm configuration mode and returns to privileged EXEC mode.</p>

Examples

The following example shows the configuration for SCCP communication on Cisco VG224 Fast Ethernet interface 0/0 to two Cisco Unified Communications Manager servers.

```
Router# show running-config
.
.
.
sccp local FastEthernet0/0
sccp ccm 10.4.13.20 identifier 10
sccp ccm 10.4.13.70 identifier 12
sccp
!
sccp ccm group 1
  associate ccm 10 priority 1
  associate ccm 12 priority 2
!
```

Enabling the STC Application for Analog FXS Ports

To enable the SCCP telephony control (STC) application and configure analog voice ports on the voice gateway for control by the STC application, perform the following steps.

Prerequisites

- SCCP is enabled on the Cisco voice gateway. For configuration information, see the [“Enabling SCCP on the Voice Gateway”](#) section on page 21.
- To enable the STC application for analog ports on a voice gateway on which the **station-id number** command is configured, remove the configuration for the **station-id number** command before performing this task.



Note

Only for FXS voice ports on a Cisco VG224 that is used with Cisco Unified CME or for FXS voice ports that are on a *different* router from Cisco Unified CME: To retain the station-id number configuration on your voice gateway, configure the **answer-address** command and do not remove the configuration for the **station-id number** command before performing this task.

Restrictions

- If Cisco Unified CME and the FXS voice ports to be controlled by the STC application are on the *same* voice gateway and the **station-id number** and **destination-pattern** commands are already configured on that gateway, the dial-peer matches the wrong entry and cannot access the STC application. To enable the STC application for FXS ports on a voice gateway on which Cisco Unified CME is configured, *remove* the configuration for the **station-id number** command before performing this task.
- If Cisco Unified CME and the FXS voice ports to be controlled by the STC application are on the *same* voice gateway and the **station-id number** command is configured for a voice-port which is controlled by the STC application with FACs, any feature code or speed dial code with ** will drop the call immediately. To use FACs that include **, *remove* the configuration for the **station-id number** command before performing this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp ccm-group** *group-number*
4. **stcapp**
5. **dial-peer voice** *tag* **pots**
6. **service stcapp**
7. **port** *slot-number/port-number*
8. **exit**
9. **voice-port** *slot-number/port-number*
10. **caller-id enable**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp ccm-group group-id Example: Router(config)# stcapp ccm-group 1	Associates the STC application with a specific Cisco Unified Communications Manager group that controls calls and features. <ul style="list-style-type: none"> <i>group-id</i>—Number that identifies the group. Use the number that was assigned with the scp ccm group command in the “Enabling SCCP on the Voice Gateway” section on page 21.
Step 4	stcapp Example: Router(config)# stcapp	Enables the STC application.
Step 5	dial-peer voice tag pots Example: Router(config)# dial-peer voice 102 pots	Defines a specific dial peer and enters dial-peer configuration mode. <ul style="list-style-type: none"> <i>tag</i>—Number that identifies the dial peer. Range: 1 to 2147483647.
Step 6	service stcapp Example: Router(config-dial-peer)# service stcapp	Enables the STC application on the dial peer.
Step 7	port slot-number/port-number or port slot-number/subunit-number/port Example: Router(config-dial-peer)# port 2/2 or Router(config-dial-peer)# port 0/1/0	Assigns an analog voice port to the dial peer. <ul style="list-style-type: none"> Format and values for analog FXS voice port number is platform-dependent. Type ? for values.
Step 8	exit Example: Router(config-dial-peer)# exit	Exits dial-peer configuration mode.
Step 9	voice-port slot-number/port-number Example: Router(config)# voice-port 2/0	Enters voice-port configuration mode. <ul style="list-style-type: none"> <i>slot-number/port-number</i>—Analog FXS voice port number. Range: 2/0 to 2/23.

	Command or Action	Purpose
Step 10	caller-id enable Example: Router(config-voiceport)# caller-id enable	(Optional) Enables caller ID for this voice port. Note Other parameters, such as caller-ID name and number, must be configured on the Cisco call-control system.
Step 11	end Example: Router(config-voiceport)# end	Exits voice-port configuration mode and returns to privileged EXEC mode.

Examples

The following example enables the STC application for Cisco Unified Communications Manager group 1 and associates the STC application with dial peer 102, to which the Cisco VG224 analog FXS port 2/2 has been assigned. This configuration also enables caller ID on voice port 2/2.

```
Router# show running-config
.
.
.
stcapp ccm-group 1
stcapp
!
dial-peer voice 102 pots
  service stcapp
  port 2/2
!
voice-port 2/2
  caller-id enable
.
.
.
```

Modifying Hookflash

To change the upper limit of the hookflash duration range for an analog FXS port, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port-number*
4. **timing hookflash-input** *milliseconds*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-port <i>slot-number/port-number</i> OR voice-port <i>slot-number/subunit-number/port</i> Example: Router(config)# voice-port 2/1	Enters voice-port configuration mode. <ul style="list-style-type: none"> Format and values for analog FXS voice port number is platform-dependent. Type ? for values.
Step 4	timing hookflash-input <i>milliseconds</i> Example: Router(config-voiceport)# timing hookflash-input 175	Specifies the maximum duration of an on-hook condition that will be interpreted as a hookflash. <ul style="list-style-type: none"> <i>milliseconds</i>—Range: 50 to 1550. Default: 1000.
Step 5	end Example: Router(config-voiceport)# end	Exits voice-port configuration mode and returns to privileged EXEC mode.

Configuring PLAR with DTMF Out-Pulse Digits

To configure an analog foreign exchange station (FXS) port to support PLAR, perform the following steps.

Prerequisites

- Cisco IOS Release 12.4(6)T or a later release for Cisco VG224 Analog Phone Gateways.
- Cisco IOS Release 12.4(9)T or a later release for Cisco ISRs.

SUMMARY STEPS

- enable**
- configure terminal**
- dial-peer voice** *tag pots*
- service stapp**
- port** *slot-number/port*
- exit**

7. **secp plar**
8. **voiceport** *port-number* **dial** *dial-string* [**digit** *dtmf-digits* [**wait-connect** *wait-msecs*] [**interval** *inter-digit-msecs*]]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag pots Example: Router(config)# dial-peer voice 102 pots	Defines a specific dial peer and enters dial-peer configuration mode. <ul style="list-style-type: none"> <i>tag</i>—Number that identifies the dial peer. Range: 1 to 2147483647.
Step 4	service stcapp Example: Router(config-dial-peer)# service stcapp	Enables the STC application for the dial peer.
Step 5	port slot-number/port Example: Router(config-dial-peer)# port 2/2	Assigns a voice port to the dial peer.
Step 6	exit Example: Router(config-dial-peer)# exit	Exits dial-peer configuration mode.
Step 7	sccp plar Example: Router(config)# sccp plar	Enters SCCP PLAR configuration mode.

	Command or Action	Purpose
Step 8	<p>voiceport <i>port-number</i> dial <i>dial-string</i> [digit <i>dtmf-digits</i> [wait-connect <i>wait-msecs</i>] [interval <i>inter-digit-msecs</i>]]</p> <p>Example: Router(config-sccp-plar)# voiceport 2/1 dial 3660 digit 1234 wait-connect 100 interval 100</p>	<p>Enables PLAR on analog FXS ports that use SCCP for call control.</p> <ul style="list-style-type: none"> • <i>port-number</i>—Analog FXS voice port number. Range is 2/0 to 2/23. • dial <i>dial-string</i>—Up to 16 characters that can be dialed on a telephone keypad (0 to 9, A to D, *, #). The voice gateway sends this string to the call-control system when the analog phone goes off hook. • digit <i>dtmf-digits</i>—Up to 16 characters (0 to 9, A to D, *, #, and a comma (,) for a one-second pause). The voice gateway sends this string to the call-control system after the <i>wait-msecs</i> expires. • wait-connect <i>wait-msecs</i>—Number of milliseconds that the voice gateway waits after voice cut-through before out-pulsing the DTMF digits. Range: 0 to 30000, in multiples of 50. Default: 50. If 0, DTMF digits are sent automatically by the voice gateway after the call is connected. • interval <i>inter-digit-msecs</i>—Number of milliseconds between the DTMF digits. Range: 50 to 500, in multiples of 50. Default: 50.
Step 9	<p>end</p> <p>Example: Router(config-sccp-plar)# end</p>	<p>Exits SCCP PLAR configuration mode and returns to privileged EXEC mode.</p>

Examples

The following example shows PLAR enabled on voice port 2/0 and 2/1.

```
Router# show running-config
.
.
.
sccp plar
  voiceport 2/0 dial 3660 digit 1234 wait-connect 100 interval 100
  voiceport 2/1 dial 3660 digit 6789 interval 100
!
!
!
dial-peer voice 500 pots
  service stcapp
  port 2/0
!
dial-peer voice 501 pots
  service stcapp
  port 2/1
!
```

Configuring SCCP Gateway Dial Tone Generation After Remote Onhook

This task configures dial tone generation after remote onhook. This feature enables the SCCP gateway to generate dial tone to the remaining party in basic call mode once the remote party disconnects. Perform this task to allow PBX interoperability by enabling configurable automatic dial tone capability after remote call disconnect.

Prerequisites

- Cisco IOS Release 12.(6)XE or a later release.

Restrictions

- The SCCP Gateway Dial Tone Generation After Remote Onhook feature is supported only on SCCP loop-start FXS ports that are registered with Cisco Unified Communications Manager and Cisco Unified CME.
- You cannot configure the SCCP Gateway Dial Tone Generation After Remote Onhook feature using Cisco Unified Communications Manager automatic download capability.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* pots**

4. `tone dialtone remote-onhook`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice tag pots</code> Example: Router(config)# <code>dial-peer voice 101 pots</code>	Defines a particular dial peer and enters dial peer voice configuration mode. <ul style="list-style-type: none"><code>tag</code>—Number that identifies the dial peer range: 1 to 2147483647.
Step 4	<code>tone dialtone remote-onhook</code> Example: Router(config-dial-peer)# <code>tone dialtone remote-onhook</code>	Enables dial tone generation after remote onhook.
Step 5	<code>end</code> Example: Router(config-dial-peer)# <code>end</code>	Exits dial-peer configuration mode and returns to privileged EXEC mode.

Examples

The following examples show the dial tone generation after the remote onhook feature is enabled. Because the dial tone generation after remote onhook feature is enabled by default, it does not display in the `show running-config` output.

```
Router# show running-config

service stcapp
 dial-peer voice 3001 pots
 port 1/1/1

Router# show dial-peer voice 3001

VoiceEncapPeer3001
 peer type = voice, system default peer = FALSE, information type = voice,
 !
 !
 !
 in bound application associated: 'stcapp'
 dial tone generation after remote-onhook = enabled

Router# show stcapp device voice-port 1/1/1
```

```
Port Identifier: 1/1/1
!
Dialtone after remote-onhook feature: activated
```

The following examples show the dial tone generation after the remote onhook feature disabled.

```
Router# show running-config

no tone dialtone remote-onhook
dial-peer voice 3002 pots
  service stcapp
  port 1/1/0

Router# show dial-peer voice 3002

VoiceEncapPeer3002
!
dial tone generation after remote-onhook = disabled

Router# show stcapp device voice-port 1/1/0

Port Identifier: 1/1/0
!
Dialtone after remote-onhook feature: not activated
```

Troubleshooting Tips

The following commands can help troubleshoot the dial tone after remote onhook feature:

- **debug voip application stcapp all**
- **debug voip application stcapp port *port-number***

Configuring SCCP Gateway Ground Start FXS Ports

To configure ground-start FXS ports, perform the following steps.

Prerequisites

- Cisco IOS Release 12.4(6)XE or a later release.

Restrictions

- Supports for basic calls only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** [*slot-number/subunit-number/port*]
4. **signal ground-start**

- 5. **shutdown**
- 6. **no shutdown**
- 7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-port [slot-number/subunit-number/port] Example: Router(config)# voice-port 1/1/1	Enters voice-port configuration mode.
Step 4	signal ground-start Example: Router(config-voiceport)# signal ground-start	Configures ground-start signaling as the signaling type for the voice port.
Step 5	shutdown Example: Router(config-voiceport)# shutdown	Takes the specified voice port offline and triggers deregistration of the device with Cisco Unified Communications Manager.
Step 6	no shutdown Example: Router(config-voiceport)# no shutdown	Puts the specified voice port back online and triggers reregistration of the device with Cisco Unified Communications Manager.
Step 7	end Example: Router(config-voiceport)# end	Exits voice-port configuration mode and returns to privileged EXEC mode.

Examples

The following example shows the ground start FXS port feature enabled and verifies the port type:

```
Router# show voice port 1/1/1

Foreign Exchange Station 1/1/1 Slot is 1, Sub-unit is 1, Port is 1
Type of VoicePort is FXS VIC2-2FXS
Operation State is DORMANT
Administrative State is UP
!
Voice card specific Info Follows:
Signal Type is groundStart
```

Troubleshooting Tips Ground Start FXS Ports

The following command can help troubleshoot ground start FXS ports:

- **debug vpm signal**—Use this command to collect debugging information for signaling events.

Configuring Supervisory Disconnect

To configure the Supervisory Disconnect feature on an analog FXS voice port, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port-number*
4. **supervisory disconnect lcfo**
5. **timeouts power-denial** *ms*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>voice-port port-number</code></p> <p>Example: Router(config)# voiceport 2/1</p>	<p>Enters voice port configuration mode.</p> <ul style="list-style-type: none"> <i>port-number</i>—Format and values for analog FXS voice port number is platform-dependent. Type ? for values.
Step 4	<p><code>supervisory disconnect lcfo</code></p> <p>Example: Router(config-voiceport)# supervisory disconnect lcfo</p>	<p>Sends a loop current feed open (LCFO) signal to indicate a disconnect on an FXS loop-start port.</p> <p>Note This command is enabled by default.</p>
Step 5	<p><code>timeouts power-denial ms</code></p> <p>Example: Router(config-voiceport)# timeouts power-denial 500</p>	<p>Sets the duration of the power denial timeout on the specified FXS voice port.</p> <ul style="list-style-type: none"> <i>ms</i>—Number of milliseconds that the power-denial is invoked. Range: 0 to 2500. Default: 750.
Step 6	<p><code>end</code></p> <p>Example: Router(config-voiceport)# end</p>	<p>Exits voice-port configuration mode and returns to privileged EXEC mode.</p>

Examples

The following example shows that the duration of the power denial is 500 ms on port 2/0 (which has supervisory disconnect enabled by default) and supervisory disconnect on port 2/1 is disabled.

```
Router# show running-config
.
.
.
voice-port 2/0
  timeouts power-denial 500
!
voice-port 2/1
  no supervisory disconnect
.
.
.
```


Verifying and Troubleshooting the Configuration

Use the following commands on the voice gateway to verify the configuration and status of the STC application and SCCP:

- **show call application voice summary**—Displays whether the STC application is running.
- **show call application voice stcapp**—Displays detailed application state and statistics.
- **show call active voice**—Displays the number of calls that are currently active. Call legs associated with this feature are included in the “Call agent controlled call-legs” listing.
- **show sccp [all | connections | statistics]**—Displays SCCP information such as administrative and operational status.
- **show stcapp device summary**—Displays a summary of endpoints associated with the STC application, and their states, types, and directory numbers.
- **show stcapp device [name *device-name* | voice-port *port*]**—Displays information for a single endpoint associated with the STC application. If an active call is in progress, the output will display additional call-related information.
- **show stcapp statistics [all | voice-port *port*]**—Displays call statistics for endpoints associated with the STC application.
- **show running-config**—Displays running configuration nondefault values.

Use the following commands on the voice gateway to troubleshoot the STC application and SCCP:

- **debug [voip | voice] application stcapp all**—Displays detailed debugging for all ports.
- **debug [voip | voice] application stcapp error**—Displays error debugging for all ports.
- **debug [voip | voice] application stcapp events**—Displays call flow event debugging for all ports.
- **debug [voip | voice] application stcapp functions**—Displays function debugging for all ports.
- **debug [voip | voice] application stcapp port *port***—Displays detailed debugging only for the specified port.
- **debug sccp all**—Displays detailed debugging for all SCCP debug trace information.
- **debug sccp config**—Displays SCCP auto-configuration/download debugging.
- **debug sccp errors**—Displays SCCP error debugging.
- **debug sccp events**—Displays SCCP events debugging.
- **debug sccp packets**—Displays SCCP packets debugging.
- **debug sccp parser**—Displays SCCP parser and builder debugging.

Use the following commands on the voice gateway to capture and view a log of STCAPP events:

- **debug voip application stcapp buffer-history**—Enables event logging for STCAPP ports.
- **show stcapp buffer-history**—Displays call flow and device events saved to the event log.

Use the following command on the voice gateway to filter output for debug commands based on the individual voice port:

- **debug condition voice-port *port***

Configuration Examples for Configuring FXS Ports for Basic Calls

This section contains the following examples:

- [Example: Cisco IOS Gateway SCCP Analog Ports Configuration, page 39](#)
- [Example: PLAR with DTMF Out-Pulse Digits, page 41](#)

Example: Cisco IOS Gateway SCCP Analog Ports Configuration

The following example shows a configuration for a Cisco VG224 Analog Phone Gateway in Cisco IOS Release 12.4(2)T:

```
Router# show running-config

Building configuration...

Current configuration : 3442 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource manager
!
ip subnet-zero
no ip dhcp use vrf connected
!
!
no ftp-server write-enable
!
stcapp ccm-group 1
stcapp
!
stcapp feature access-code
  prefix *#
  call forward all 2
  call forward cancel 9
!
stcapp feature speed-dial
  prefix ##
  redial 9
  voicemail 8
  speed dial from 3 to 7
!
!
template address
!
voice-card 0
```

```

!
!
!
!
!
interface FastEthernet0/0
 ip address 10.4.138.5 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
 ip default-gateway 10.4.0.1
 ip classless
 ip route 223.255.254.0 255.255.255.0 10.4.0.1
!
 ip http server
!
!
!
 control-plane
!
!
 voice-port 2/0
  caller-id enable
!
 voice-port 2/1
  caller-id enable
!
 voice-port 2/2
  caller-id enable
!
 voice-port 2/3
  caller-id enable
!
 voice-port 2/4
!
.
.
.
!
 voice-port 2/23
!
!
!
 sccp local FastEthernet0/0
 sccp ccm 10.4.131.200 identifier 7815
 sccp ccm 10.4.138.77 identifier 7825
 sccp
!
 sccp ccm group 1
  associate ccm 7815 priority 1
  associate ccm 7825 priority 2
!
!
 dial-peer voice 500 pots
  service stcapp
  port 2/0
!
 dial-peer voice 501 pots

```

```

service stcapp
port 2/1
!
dial-peer voice 502 pots
service stcapp
port 2/2
!
dial-peer voice 503 pots
service stcapp
port 2/3
!
dial-peer voice 504 pots
service stcapp
port 2/4
!
.
.
.
!
dial-peer voice 523 pots
service stcapp
port 2/23
!
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
line aux 0
transport preferred all
transport output all
line vty 0 4
login
transport preferred all
transport input all
transport output all
!
end

```

Example: PLAR with DTMF Out-Pulse Digits

The following example shows PLAR with DTMF Out-Pulse Digits configured on a Cisco VG224 voice gateway:

```

Router# show running-config

Building configuration...

Current configuration : 3442 bytes
.
.
.
!
stcapp ccm-group 1
stcapp
!
stcapp feature access-code
prefix *#
call forward all 2
call forward cancel 9
!
stcapp feature speed-dial

```

```

digit 2
voicemail 55
speed dial from 11 to 17
!
!
template address
!
voice-card 0
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 10.4.138.5 255.255.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip default-gateway 10.4.0.1
ip classless
ip route 223.255.254.0 255.255.255.0 10.4.0.1
!
ip http server
!
!
!
control-plane
!
!
voice-port 2/0
caller-id enable
!
voice-port 2/1
caller-id enable
!
voice-port 2/2
caller-id enable
!
voice-port 2/3
caller-id enable
!
voice-port 2/4
!
.
.
.
!
voice-port 2/23
!
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.131.200 identifier 7815
sccp ccm 10.4.138.77 identifier 7825
sccp ccm 172.16.18.4 identifier 37454
sccp

```

```
!
sccp ccm group 1
  associate ccm 7815 priority 1
  associate ccm 7825 priority 2
  associate ccm 37454 priority 3
  registration timeout 3
  keepalive retries 1
  keepalive timeout 3
  switchback method graceful
!
sccp plar
  voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
  voiceport 2/1 dial 3264 digit 678,,9*0,,#123 interval 100
  voiceport 2/3 dial 3478 digit 34567 wait-connect 500
!
!
dial-peer voice 500 pots
  service stcapp
  port 2/0
!
dial-peer voice 501 pots
  service stcapp
  port 2/1
!
dial-peer voice 502 pots
  service stcapp
  port 2/2
!
dial-peer voice 503 pots
  service stcapp
  port 2/3
!
dial-peer voice 504 pots
  service stcapp
  port 2/4
!
.
.
.
!
dial-peer voice 523 pots
  service stcapp
  port 2/23
!
!
line con 0
  exec-timeout 0 0
  transport preferred all
  transport output all
line aux 0
  transport preferred all
  transport output all
line vty 0 4
  login
  transport preferred all
  transport input all
  transport output all
!
end
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager documentation
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express documentation
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series documentation • Cisco 1800 Series Integrated Services Routers documentation • Cisco 2800 Integrated Services Routers documentation • Cisco 3800 Series Integrated services Routers documentation • Cisco Unified 500 Series documentation
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Configuring FXS Ports for Basic Calls

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(6)XE or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Configuring FXS Ports for Basic Calls

Feature Name	Releases	Feature Information
Hookflash Duration	12.4(6)XE 12.4(11)T	<p>Enables modification of the upper limit of the hookflash duration range for an analog FXS port.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Hookflash Duration, page 18. • Modifying Hookflash, page 27. <p>No new commands were introduced by this feature.</p>

Table 1 Feature Information for Configuring FXS Ports for Basic Calls (continued)

Feature Name	Releases	Feature Information
SCCP Dial Tone Generation After Remote On-Hook	12.4(6)XE 12.4(11)T	<p>Enables the SCCP gateway to generate dial tone to the remaining party in basic call mode once the remote party disconnects.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Dial Tone Generation after Remote Onhook, page 19. • Configuring SCCP Gateway Dial Tone Generation After Remote Onhook, page 32. <p>The following commands were introduced or modified by this feature: tone dialtone remote-onhook</p>
SCCP Gateway Ground Start FXS Ports		<p>Supports ground-start FXS ports for disconnect supervision and Cisco Communications Manager registration of PBX and key system connections.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Ground Start FXS Ports as SCCP Analog Endpoints, page 20 • Configuring SCCP Gateway Ground Start FXS Ports, page 34 <p>No new commands were introduced by this feature.</p>
SCCP PLAR with DTMF Out-Pulse Digits for FXS Analog Phones	12.4(6)T	<p>Adds private line automatic ring-down (PLAR) support for SCCP analog ports on a Cisco VG224 Analog phone gateway.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PLAR with DTMF Out-Pulse Digits, page 19 • Configuring PLAR with DTMF Out-Pulse Digits, page 28 <p>The following commands were introduced or modified by this feature: sccp plar, voiceport.</p>
	12.4(9)	Adds supports for FXS ports on Cisco ISRs.

Table 1 *Feature Information for Configuring FXS Ports for Basic Calls (continued)*

Feature Name	Releases	Feature Information
Supervisory Disconnect	12.4(6)T	<p>Provides a disconnect indication to the remote party in a two-party call after one side disconnects and enables external applications connected to the Cisco voice gateway to promptly clear a call after receiving the disconnect indication.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supervisory Disconnect, page 20 • Configuring Supervisory Disconnect, page 36. <p>The following commands were introduced or modified by this feature: supervisory disconnect, timeouts power-denial.</p>
	12.4(9)T	Adds supports for FXS ports on Cisco ISRs.



Enabling Fallback to Cisco Unified SRST for Call Control on Analog (FXS) Ports

First Published: June 27, 2005

Last Updated: November 26, 2012

This chapter describes how to enable remote Cisco Unified Communications Manager servers and the local Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) router for determining the order in which the systems assume call control for analog endpoints connected to analog Foreign Exchange Station (FXS) ports on a Cisco voice gateway. Cisco Unified SRST provides fallback for analog endpoints in Cisco Unified Communications Manager only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this chapter. To reach links to specific feature documentation and to see a list of the releases in which each feature is supported, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Enabling Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports, page 50](#)
- [Restrictions for Enabling Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports, page 51](#)
- [How to Enable Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports, page 51](#)
- [Additional References, page 54](#)

Prerequisites for Enabling Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports

Cisco IOS Gateway

- The Cisco voice gateway must be set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- SCCP is enabled on the Cisco voice gateway. For configuration information, see the “[Enabling SCCP on the Voice Gateway](#)” section on page 21.
- Before Cisco IOS 15.0(1)M: To ensure that the analog phones can register in Cisco Unified SRST when required, such as when the Cisco VG224 is rebooted while Cisco Unified Communications Manager is in fallback mode, the DN for analog phones connected to FXS ports on the Cisco voice gateway and registered in Cisco Unified Communications Manager must be explicitly configured on the Cisco VG224 using the **station-id number** command in voice-port configuration mode. For information, see the [Cisco IOS Voice Command Reference](#).



Note

In Cisco IOS Release 15.0(1)M and later releases: When a directory number for an analog phone is added or changed in Cisco Unified Communications Manager, the **station-id number** command in voice-port configuration mode is automatically added for the new or modified directory number. Every time the Cisco VG224 receives DNs from Cisco Unified Communications Manager during registration, it checks the new DNs against the already-saved DNs. If at least one DN is different, then a background save is triggered and the DN is saved in the station-id number configuration. If the Cisco VG224 must register to Cisco Unified SRST after rebooting, it uses the saved DN to register the corresponding analog phone in Cisco Unified SRST.

Cisco Unified SRST

- For Cisco SRST 3.3: Cisco IOS Release 12.3(14)T or a later release.
- For Cisco SRST 3.4 and Cisco Unified SRST 4.0: Cisco IOS Release 12.4(2)T or a later release.

Cisco Unified Communications Manager

- This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

Restrictions for Enabling Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports

- Switchover and switchback are supported using the graceful method only. Other switchover and switchback methods are not supported.
- Cisco Unified SRST supports basic calls only; it does not support supplementary features.
- Cisco Unified SRST does not provide fallback for analog endpoints in Cisco Unified Communications Manager Express (Cisco Unified CME).
- In an actual Cisco Unified SRST scenario, when a Cisco Unified IP phone registers with a Cisco Unified CM, the Cisco Unified CM pushes Cisco Unified SRST information (using the selected device pool) to the Cisco Unified IP phone and the phone stores the information. However, in the case of an analog phone connected to Cisco IOS SCCP voice gateways, like the VG224, that provision is not available. These voice gateways do not perform autoconfiguration through the TFTP download of XML configuration files. The ports of these voice gateways do not receive or store any Cisco Unified SRST information from Cisco Unified CM so selective fallback is not possible with VG224 and similar voice gateway ports.

How to Enable Fallback to Cisco Unified SRST for Call Control on Analog FXS Ports

To assign priority levels to remote Cisco Unified Communications Manager servers and the local Cisco Unified SRST router for determining the order in which the systems assume call control if one becomes unavailable, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **scp ccm group** *group-number*
4. **associate ccm** *identifier-number* **priority** *priority-number*
5. **switchover method** {**graceful** | **immediate**}
6. **switchback method** {**graceful** | **guard** [*guard-timeout*] | **immediate** | **uptime** *uptime-timeout*}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>sccp ccm group <i>group-number</i></p> <p>Example: Router(config)# sccp ccm group 1</p>	<p>Creates a Cisco Unified Communications Manager and Cisco Unified SRST group and enters SCCP ccm configuration mode.</p> <ul style="list-style-type: none"> <i>group-number</i>—Number that identifies the group. Range: 1 to 65535.
Step 4	<p>associate ccm <i>identifier-number</i> priority <i>priority-number</i></p> <p>Example: Router(config-sccp-ccm)# associate ccm 10 priority 1</p>	<p>Adds a Cisco Unified Communications Manager server or Cisco Unified SRST router to the group and establishes its priority within the group.</p> <ul style="list-style-type: none"> <i>identifier-number</i>—Number that identifies the Cisco Unified Communications Manager server or Cisco Unified SRST router. This is the number that was assigned with the sccp ccm command. See the “Enabling SCCP on the Voice Gateway” section on page 21. priority <i>priority-number</i>—Number that indicates the priority of this Cisco Unified Communications Manager server or Cisco Unified SRST router. Range: 1 to 4, where 1 is the highest priority. Assign the lowest priority to Cisco Unified SRST. <p>Note A second Cisco Unified Communications Manager server that is entered with a lower priority number becomes a backup system.</p>
Step 5	<p>switchover method {graceful immediate}</p> <p>Example: Router(config-sccp-ccm)# switchover method graceful</p>	<p>(Optional) Sets the switchover method that the voice gateway uses if connectivity to the primary Cisco Unified Communications Manager fails.</p> <ul style="list-style-type: none"> graceful—Switchover happens only after all active sessions are terminated gracefully. This is the only supported method. immediate—Switchover to a secondary call-control system happens immediately regardless of whether or not there are active connections. <p>Note The switchover method graceful command is enabled by default. Other switchover methods are not supported.</p>

	Command or Action	Purpose
Step 6	<pre>switchback method {graceful guard [guard-timeout] immediate uptime uptime-timeout}</pre> <p>Example: Router(config-sccp-ccm)# switchback method graceful</p>	<p>Sets the switchback method that the voice gateway uses when the primary or higher priority Cisco Unified Communications Manager becomes available again.</p> <ul style="list-style-type: none"> graceful—Switchback happens only after all active sessions are terminated gracefully. This is the only supported method. <p>Note The switchback method graceful command must be enabled. Other switchback methods are not supported.</p>
Step 7	<pre>end</pre> <p>Example: Router(config-sccp-ccm)# end</p>	<p>Exits SCCP ccm configuration mode and returns to privileged EXEC mode.</p>

Configuration Examples for SCCP and the STC Application

The following example enables SCCP communication on Fast Ethernet interface 0/0 to two Cisco Unified Communications Manager servers and a Cisco Unified SRST router. In SCCP group 1, the Cisco Unified Communications Manager server at IP address 10.4.13.20 is assigned priority 1, making it the primary call-control system. If connectivity to the primary fails, call control reverts to the backup Cisco Unified Communications Manager server at 10.4.13.70. If connectivity to both Cisco Unified Communications Manager servers fails, call control reverts to the Cisco Unified SRST router at 10.4.18.40.

```
Gateway# show running-config
.
.
.
sccp local FastEthernet0/0
sccp ccm 10.4.13.20 identifier 10
sccp ccm 10.4.13.70 identifier 12
sccp ccm 172.16.10.40 identifier 30
sccp
!
sccp ccm group 1
  associate ccm 10 priority 1
  associate ccm 12 priority 2
  associate ccm 30 priority 3
  switchback method graceful
!
!
```


Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager documentation
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express documentation
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series documentation • Cisco 1800 Series Integrated Services Routers documentation • Cisco 2800 Integrated Services Routers documentation • Cisco 3800 Series Integrated services Routers documentation • Cisco Unified 500 Series documentation
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport



Configuring Supplementary Features

First Published: June 27, 2005

Last Updated: June 3, 2016

This module describes how to enable Skinny Client Control Protocol (SCCP) supplementary features for analog Foreign Exchange Station (FXS) ports on a Cisco voice gateway, such as a Cisco Integrated Services Router (Cisco ISR) or Cisco VG224 Analog Phone Gateway, under the control of Cisco Unified Communications Manager or Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways](#)” section on page 88.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways, page 56](#)
- [Restrictions for SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways, page 57](#)
- [Information About SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways, page 57](#)
- [How to Configure SCCP Analog FXS Ports with Supplementary Features in Cisco IOS Gateways, page 71](#)
- [Configuration Examples for SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways, page 84](#)
- [Additional References, page 87](#)
- [Feature Information for SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways, page 88](#)

Prerequisites for SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways

Cisco IOS Gateway

- Cisco IOS Release 12.3(11)T or a later release.
- The Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the [Cisco IOS Voice Port Configuration Guide](#).
- SCCP and the SCCP telephony control (STC) application is enabled on the Cisco voice gateway. For configuration information, see the [“Configuring FXS Ports for Basic Calls” section on page 17](#).

Analog Endpoints in Cisco Unified Communications Manager

- Cisco Unified Communications Manager 4.2 or a later version.
- Phones are added and configured in Cisco Unified Communications Manager. See the “Directory Number Configuration” chapter under “Call Routing Configuration” and the “Gateway Configuration” chapter under “Device Configuration” in the appropriate [Cisco Unified Communications Manager Administration Guide](#).

Analog Endpoints in Cisco Unified CME

- Cisco CME 3.2 or a later version.
- Ephone configurations and feature parameters for analog endpoints are configured in Cisco Unified CME. For information, see the *Cisco Unified CME Administration Guide*.
- To use call transfer on analog endpoints, set the **transfer-system** command to full-blind or full-consult on Cisco router. Neither of these settings is the default for this command, so one of these settings must be manually configured. For configuration information, see the “[Configuring Call Transfer and Forwarding](#)” module in the *Cisco Unified CME Administration Guide*.

The following example shows how to configure full consultation as the call transfer method:

```
Router(config)# telephony-service
Router(config-telephony)# transfer-system full-consult
```

Restrictions for SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways

- Maximum number of participants in a software-based ad hoc conference is three. Conference chaining, the ability of a conference participant to add another party to an existing three-party conference, is not supported.

Analog Endpoints in Cisco Unified Communications Manager

- Local group pickup and external group pickup are supported for Cisco Unified Communications Manager only if the AutoCallPickupEnabled service parameter is set to True.
- Directed call park and directed call pickup are not supported for Cisco Unified Communications Manager.

Information About SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Summary of SCCP Supplementary Features for FXS ports, page 58](#)
- [Flexible Feature Access Codes, page 66](#)
- [Enhanced Speed Dial on SCCP Analog Phones, page 68](#)
- [Cancel Call Waiting, page 69](#)
- [SCCP Meet-Me Conference, page 69](#)



Note

In Cisco IOS Release 15.1(2)T5 and later, Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints. Cisco IOS Release 15.1(2)T5 also adds support for the STCAPP functionality for Cisco IAD2430.

Summary of SCCP Supplementary Features for FXS ports

Table 1 contains a list of SCCP supplementary features that are supported on analog phones connected to FXS ports, along with descriptions and information about how to configure support for each feature in your Cisco call-control system.



Note For information about individual commands in Cisco Unified CME, see the [Cisco Unified CME Command Reference](#).

Table 1 *SCCP Supplementary Features for Analog FXS Ports*

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
Audible Message-Waiting Indication (AMWI) Notifies user of new voice mail.	User picks up handset and hears message waiting indication (MWI) tone whenever a new voice message is waiting to be heard.	Cisco Unified Communications Manager To configure, see the “Message Waiting Configuration” chapter under “Voice Mail Configuration” in the appropriate Cisco Unified Communications Manager Administration Guide . Cisco Unified CME To configure, see “ Integrating Voice Mail ” in the Cisco Unified CME Administration Guide .
Call Forward Busy (CFB) Forwards calls to a target number when the called number is busy.	User activates by using the Cisco Unified CME GUI or administrator activates by configuring this feature in the Cisco call-control system.	Cisco Unified Communications Manager For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and protocols” in the appropriate Cisco Unified Communications Manager System Guide . To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate Cisco Unified Communications Manager Administration Guide . Cisco Unified CME To configure, see “ Configuring Call Transfer and Forwarding ” in the Cisco Unified CME Administration Guide .

Table 1 *SCCP Supplementary Features for Analog FXS Ports (continued)*

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Call Forward No Answer (CFNA)</p> <p>Forwards calls to a target number when there is no answer at the called number.</p>	<p>User activates by using the Cisco Unified CME GUI or an administrator activates by configuring this feature in the Cisco call-control system.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Call Transfer and Forwarding” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Call Transfer</p> <p>Connects call to a third party that the phone user dials.</p>	<p>During an active call, user presses hookflash and receives dial tone. User dials number for transfer and either stays online to announce (consultive transfer) or hangs up (blind transfer). When user hangs up, the call is transferred.</p> <p>Note When blind transfer is configured in Cisco Unified CME, the phone user does not have to hang up; the call is transferred when Cisco Unified CME receives the dialed number.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see “Making and Receiving Multiple Calls Per Directory Number” section of the “Understanding Directory Numbers” chapter under “Dial Plan Architecture” in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Call Transfer and Forwarding” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Call Waiting</p> <p>Announces a second call during an active call.</p>	<p>During an active call, user hears a tone and can press hookflash to toggle between the active call and the incoming call.</p> <p>For analog endpoints in Cisco Unified Communications Manager: The call waiting tone depends on the ring setting for the active station and the tone does not play repeatedly, it plays only once.</p> <p>For analog endpoints in Cisco Unified CME: The call waiting tone is played continuously.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Understanding Directory Numbers” section of the “Understanding Route Plans” chapter under “Dial Plan Architecture” in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>Cisco Unified CME</p> <p>No configuration task are required in Cisco Unified CME.</p>

Table 1 SCCP Supplementary Features for Analog FXS Ports (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Caller ID</p> <p>Displays calling number, caller name, and time of call.</p>	<p>Administrator activates on the Cisco call-control system. Time stamp is from the Cisco voice gateway.</p> <p>Note To display the caller ID when caller ID is supported by the local telco provider, an administrator must use the caller id enable command on the appropriate Cisco voice gateway port.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Caller Identification and Restriction” section of the “Understanding Route Plans” chapter under “Dial Plan Architecture” in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>Cisco Unified CME</p> <p>For caller-ID display on local calls (calls between FXS ports and IP phones registered to the same Cisco Unified CME router):</p> <ul style="list-style-type: none"> To configure, see “SCCP: Configuring Phones on SCCP Controlled Analog (FXS) Ports” in the <i>Cisco Unified CME Administration Guide</i>. <p>For restricting or blocking caller-ID display:</p> <ul style="list-style-type: none"> To configure, see “How to Configure Caller-Id Blocking” in the <i>Cisco Unified CME Administration Guide</i>.
<p>Conference Call</p> <p>Initiates a three-party conference.</p>	<p>User in basic call mode presses hookflash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, user presses hookflash to get feature tone and then dials #3 to initiate a three-party conference.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Initiating an Ad Hoc Conference Bridge” section of the “Conference Bridges” chapter under “Media Resources” in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see the “Configuring Conferencing” section of the “Adding Features” chapter in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Distinctive Ringing on Cisco IOS SCCP Voice Gateways</p> <p>Enables distinct ring tone to alert user whether incoming call is from an internal or external phone.</p>	<p>System administrator configures the ring patterns for both internal and external calls on the voice gateway port.</p>	<p>To configure, see the ring cadence command in the <i>Cisco IOS Voice Command Reference</i>.</p>

Table 1 **SCCP Supplementary Features for Analog FXS Ports (continued)**

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Feature Access Codes (FACs) Access features using an abbreviated code.</p> <p>Flexible FACs Allows you to configure feature codes for FACs so that phone users are not required to dial the prefix before dialing the feature code to access an SCCP feature.</p> <p>Enhanced Flexible Facs Allows you to configure feature codes for FACs so that phone users are not required to dial the prefix or special characters to access an SCCP feature.</p>	<p>User accesses features by dialing a FAC, typically consisting of a prefix plus a feature code.</p> <p>For a list of STC application call features that can be accessed by dialing a FAC, see Table 2.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>For feature and configuration information for individual STC application call features for which you can configure a FAC, see Table 2.</p>
<p>Redial Dials again the last number dialed from this phone.</p>	<p>User dials the feature speed dial (FSD) prefix and the redial code. Default prefix and code is *#.</p> <p>Note The stcapp feature speed-dial command must be enabled on the Cisco voice gateway.</p>	<p>No configuration tasks required on your Cisco call-control system.</p>

Table 1 SCCP Supplementary Features for Analog FXS Ports (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Speed Dial</p> <p>Dials a telephone number using an abbreviated code.</p>	<p>Up to 99 Speed Dials (Local Phone)</p> <p>User dials the FSD prefix and desired speed-dial code. The digit command determines the number of digits used for FSD codes on the Cisco voice gateway.</p> <p>Default prefix and code range is:</p> <ul style="list-style-type: none"> • *1 to *9 for one-digit codes • *01 to *99 for two-digit codes <p>User stores speed-dial destinations by using the Cisco Unified CME GUI or an administrator stores destinations on the Cisco call-control system.</p> <p>Note The stcapp feature speed-dial command must be enabled on the Cisco voice gateway.</p> <p>Up to 9,999 Speed Dials (System-wide)</p> <p>User dials access code and speed-dial number. Administrator activates on the Cisco call-control system.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Phone Features” section of the “Cisco Unified IP Phones” chapter under “Devices and protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Configuring Speed-Dial Buttons” section in the “Cisco Unified Phone Configuration” chapter under “Device Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Speed Dial” in the <i>Cisco Unified CME Administration Guide</i>.</p> <p>Cisco Unified Communications Manager</p> <p>To configure, see the “Translation Pattern Configuration” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Speed Dial” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Speed Dial to Voice Mail</p> <p>Dials the voice-mail number using an abbreviated code.</p>	<p>User dials the FSD prefix and speed dial to voice mail code. The digit command determines the number of digits used for FSD codes.</p> <p>Default prefix and code is:</p> <ul style="list-style-type: none"> • *0 for one-digit codes • *00 for two-digit codes. <p>Note The stcapp feature speed-dial command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>To configure, see the “Cisco Voice-Mail Pilot Configuration” chapter under “Voice Mail Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Integrating Voice Mail” in the <i>Cisco Unified CME Administration Guide</i>.</p>

Table 2 **FACs for SCCP Supplementary Features for Analog FXS Ports**

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Call Forward All (CFA)</p> <p>Forwards all calls to a target number.</p>	<p>User dials feature access code (FAC) prefix and call-forward-all code, and then following the confirmation tone, the target number. Default prefix and code is **1.</p> <p>After CFA is activated, user hears a stutter tone when the handset is picked up to indicate that all incoming calls are being forwarded.</p> <p>If a phone user tries to activate CFA after it is already activated, a fast busy tone is generated.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and Protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <ul style="list-style-type: none"> • To configure, see “How to Configure Call Transfer and Forwarding” in the <i>Cisco Unified CME System Administrator Guide</i>. • Use the call-forward max-length command in Cisco Unified CME to limit the number of digits that can be dialed for the target forwarding number. • The target destination for diverted calls can be specified in the router configuration or on the phone by using a FAC. The most recently entered destination is recognized by Cisco Unified CME, regardless of how it was entered.

Table 2 FACs for SCCP Supplementary Features for Analog FXS Ports (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Call Forward All Cancel Cancels an active CFA condition.</p>	<p>User dials FAC prefix and call-forward-cancel code. Default prefix and code is **2.</p> <p>After CFA is canceled, user hears a confirmation tone when the handset is picked up to indicate incoming calls are no longer being forwarded.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and Protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <ul style="list-style-type: none"> To configure, see “Configuring Call Transfer and Forwarding” in the <i>Cisco Unified CME Administration Guide</i>. Can also be activated using the no call-forward all command.
<p>Call Park Directed Call Pickup Directed Puts a call on hold at a designated extension so that it can be retrieved by anyone.</p>	<p>During an active call, user presses hookflash for dial tone, and then dials the call-park slot number configured on the call-control system.</p> <p>User retrieves the call by dialing the FAC prefix, the directed pickup code, and the call-park slot number where the call was parked, and pressing hookflash. Default prefix and code is **6. For example, if the call is parked at slot 1211, user dials **61211.</p> <p>Users can also retrieve the last call parked by their own extensions by dialing the FAC prefix, the directed pickup code, and an asterisk (*), and pressing hookflash. Default prefix and code is **6*.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>This feature is not supported for Cisco Unified Communications Manager.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Call Coverage Features” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Call Pickup of Ringing Extension, Directed Allows incoming calls to be picked up by phones other than the ringing phone.</p>	<p>User picks up a ringing extension by dialing the FAC prefix, the directed pickup code, and the ringing extension number. Default prefix and code is **6.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>This feature is not supported for analog endpoints in Cisco Unified Communications Manager.</p> <p>Cisco Unified CME</p> <p>No configuration tasks are required In Cisco Unified CME.</p>

Table 2 FACs for SCCP Supplementary Features for Analog FXS Ports (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Call Pickup Group</p> <p>Allows incoming calls in a different pickup group than the user to be picked up.</p>	<p>User picks up a ringing extension by dialing the FAC prefix, the group pickup code, and the number of the pickup group. Default prefix and code is **4.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>AutoCallPickupEnabled service parameter must be set to True.</p> <p>For feature information, see the “Call Pickup” section of the “Translation Pattern Configuration” chapter under “Call Configuration” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Pick Up Phone Configuration” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Call Coverage Features” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Call Pickup Local</p> <p>Allows incoming calls in the same pickup group as the user to be picked up.</p>	<p>User picks up a ringing extension by dialing the FAC prefix and the local pickup code. Default prefix and code is **3.</p> <p>Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>AutoCallPickupEnabled service parameter must be set to True.</p> <p>To configure, see the “Pick Up Phone Configuration” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>To configure, see “Configuring Call Coverage Features” in the <i>Cisco Unified CME Administration Guide</i>.</p>
<p>Cancel Call Waiting</p> <p>Cancels the call waiting service during a call.</p>	<p>User dials the cancel call waiting FAC, receives recall dial-tone, and places a call. Default prefix and code is **8.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and Protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>Cisco Unified CME</p> <p>No configuration tasks are required in Cisco Unified CME.</p>

Table 2 FACs for SCCP Supplementary Features for Analog FXS Ports (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
Forward to Voice Mail Forwards calls to voice mail.	User dials FAC prefix and voice-mail code. Default prefix and code is **7. Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.	Cisco Unified Communications Manager For feature information, see the “Phone Features” section of the “Cisco Unified IP Phone” chapter under “Devices and Protocols” in the appropriate <i>Cisco Unified Communications Manager System Guide</i> . To configure, see the “Configuring Directory Numbers” chapter under “Call Routing Configuration” in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i> .
SCCP Meet-Me Conference Enables user on an analog SCCP phone to start or join a meet-me conference call.	To start a meet-me conference, user dials FAC prefix and meet-me conference code, and following the confirmation tone, the meet-me conference number. Default prefix and code is **5. Participants can join the conference by dialing the meet-me conference number. Participants hear a busy tone if they call the conference number before the conference controller has joined. In this case, participants must call back. To end a meet-me conference, all participants must hang up. The conference does not automatically end when the conference controller disconnects. Before a conference controller can start a meet-me conference, meet-me conference numbers must be configured in your Cisco call-control system by the system administrator. Note The stcapp feature access-code command must be enabled on the Cisco voice gateway.	Cisco Unified Communications Manager To configure: <ul style="list-style-type: none"> • See the “Conference Bridge Configuration” section of the “Media Resource Configuration” chapter in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>. • See the “Meet-Me Number/Pattern Configuration” section of the “Call Routing” chapter in the appropriate <i>Cisco Unified Communications Manager Administration Guide</i>. Cisco Unified CME To configure meet-me conferencing and meet-me conference numbers, see “SCCP: Configuring Conferencing” in the <i>Cisco Unified CME Administration Guide</i> .

Flexible Feature Access Codes

To access certain STC application call features on analog phones connected to a voice gateway, phone users must dial a FAC consisting of a prefix plus a feature code, for example **1.

The prefix for FACs is a one to five-character string beginning with an asterisk (*) or number sign (#). The default value is **.

Before Cisco IOS Release 12.4(20)YA, feature codes for FACs were limited to a single character (0-9, *, or #). In Cisco IOS Release 12.4(20)YA and later releases, the Flexible FAC feature allows you to configure feature codes as follows:

- For feature codes to be dialed after dialing the prefix, you can configure one character (0-9, *, or #) or two digits (00-99) that can be dialed on phone keypad.
- For feature codes that do not require the prefix to be dialed to access the feature, you can configure two to four characters that can be dialed on phone keypad and the leading or ending character must be an asterisk (*) or number sign (#).
- The default values for specific FACs are listed in [Table 2](#).

Flexible FACs allow you to configure feature codes for FACs so that phone users are not required to dial the prefix before dialing the feature code to access an SCCP feature on an analog phone. If you configure a feature code that is at least two characters and the leading or ending character is an asterisk (*) or number sign (#), no prefix is required to access the feature. For example, if you configure a feature code of 78# for Call Forward Cancel, the phone user dials just the feature code (78#) to access that feature. If you configure a feature code of 78 for Call Forward Cancel, the phone user must dial the prefix, whatever it is, plus the feature code (78) to access that feature.

If you attempt to set a feature code to a value that is already configured for another feature code, a speed-dial code, or the Redial FSD, you receive a warning message. If you configure a duplicate code, the system implements the first feature it matches in the order shown in the output of the `show stcpp feature codes` command. Precedence is determined by the value for each feature code.

If you attempt to set a feature code to a value that precludes or is precluded by another feature code, a speed-dial code, or the Redial FSD, you receive a warning message. For example, if you attempt to set a feature code of #123 and #12 is already configured for another feature, such as Call Forward Cancel, the following message appears:

```
#123 is precluded by call forward cancel(#12)
```

Or if you attempt to configure #1 and #12 is already configured for another feature, such as Call Forward Cancel, the following message appears:

```
#1 precludes call forward cancel(#12)
```

These messages will not prevent you from configuring the feature code.

After a phone user dials the FAC or FSD, the system matches the dialed string with configured FACs, Redial, and speed-dial codes in the following order and executes the first complete match, ignoring the longer feature code:

- Malicious call ID (MCID)
- Call forward all
- Call forward cancel
- Pickup local group
- Pickup different group
- Pickup direct
- Redial
- Speeddial1
- Speeddial2
- Speeddial3
- and so on...

For example, assume that Call Forward All is #123, Call forward Cancel is #12, and Pickup Local Group and Redial are both #1. After the phone user dials #1, the system matches the dialed characters to the configured codes in the order listed and because it is the first exact match, executes Pickup Local Group. If the phone user dials #12, the digit 2 will be ignored because #1 is an exact match and the system executes Pickup Local Group again. In this configuration, the phone user is unable to access Call Forward All (#123), Call Forward Cancel (#12), or Redial (#1) because all are precluded by #1 for Pickup Local Group. You must configure a new value for a precluded feature code in order to enable a FAC for that feature.

To enable and configure FACs on an analog FXS port, see the [“Configuring Feature Access Codes” section on page 71](#).

Enhanced Flexible Feature Access Code

In Cisco IOS 15.0(1)M and later releases, you can configure an all-numeric three or four-digit feature codes so that users are not required to dial a prefix or special characters. For example, if you configure a feature code of 788 for Call Forward Cancel, the phone user dials just the feature code (788) to access that feature.

Flexible Feature Access Code Support for Redial

Flexible feature access codes includes support for Redial. To access Redial using an FSD, analog phone users must dial a prefix and speed-dial code. The default prefix and speed-dial code for Redial is *#.

In Cisco IOS Release 12.4(20)YA and later releases, if you configure a speed-dial code for Redial of one or two characters that can be dialed on a phone keypad, the phone user must dial the FSD prefix before dialing the speed-dial code. If you configure a speed-dial code for Redial of two to four characters and the leading or ending character is an asterisk (*) or a number sign (#), the phone user is not required to dial the FSD prefix before dialing the speed-dial code for Redial.

In Cisco IOS 15.0(1)M and later releases, you can configure a speed-dial code of three or four digits for Redial so that the phone user is not required to dial the FSD prefix or any special character to dial the speed-dial code for Redial.

For configuration information, see the [“Enabling and Changing Feature Speed-Dial Codes” section on page 78](#).

Enhanced Speed Dial on SCCP Analog Phones

To access predefined speed-dial numbers used with the STC application, analog phone users must dial a FSD consisting of a prefix and speed-dial code, for example *9. The FSD prefix and speed-dial codes are set on the Cisco voice gateway; the telephone numbers that are speed dialed must be configured on your Cisco call-control system.

The speed-dial codes on the Cisco voice gateway are mapped to speed-dial positions on the call-control device, starting with position 1. For example, if you configure speed-dial codes 00 to 20 on the Cisco voice gateway, the system maps code 00 to speed-dial 1 on the call-control device, code 01 to speed-dial 2, code 02 to speed-dial 3, and so on. Dialing 00 on the analog phone dials the telephone number associated with speed-dial 1.

Prior to Cisco IOS Release 12.4(6)T, speed-dial codes for FSDs were limited to a single digit, 0 to 9. In Cisco IOS Release 12.4(6)T and later releases, you can define two-digit speed-dial codes to access up to 99 local speed-dial numbers configured on the call-control device.

In Cisco IOS 15.0(1)M and later releases, for speed-dial to voice mail, you can dial a three or four digit FAC without a prefix. For example:

```
VG224(config)#stcapp feature speed-dial
VG224(config-stcapp-fsd)#voicemail 777
do not use prefix. voicemail is 777
```

Flexible FACs supports only the FSD for Redial. In Cisco IOS Release 12.4(20)YA and later releases, if you configure a speed-dial code for Redial of two to four characters that can be dialed on a phone keypad and the leading or ending character is an asterisk (*) or a number sign (#), the phone user is not required to dial the FSD prefix before dialing the speed-dial code for Redial. For information about Flexible FACs, see the [“Flexible Feature Access Codes” section on page 66](#).

To enable FSDs on an analog FXS port, see the [“Enabling and Changing Feature Speed-Dial Codes” section on page 78](#).

To use bulk speed-dial codes up to 9,999, no specific configuration is required on the Cisco voice gateway. Analog phone users do not need to use an FSD prefix or speed-dial codes to access bulk speed-dial numbers. See the documentation for your Cisco call-control system for information about configuring up to 9,999 speed dials.

Cancel Call Waiting

In Cisco IOS Release 15.1(1)T and later releases, the Cancel Call Waiting feature allows a phone user with Call Waiting service to disable the Call Waiting feature for one call. The user dials the cancel call waiting FAC, receives recall dial-tone, and places a call normally. The Call Waiting service is inactive during this call. Anyone calling the user receives the normal busy treatment and no call waiting tone interrupts the user’s active call. Cancel Call Waiting automatically deactivates when the user disconnects from the call.

For configuration information, see the [“Configuring Feature Access Codes” section on page 71](#).

SCCP Meet-Me Conference

In Cisco IOS Release 12.4(20)YA and later releases, hardware-based meet-me conferencing is supported on analog phones connected to the FXS port of Cisco voice gateways. Hardware-based conferencing uses digital signal processors (DSPs) to allow more parties than the three-party limit allowed by software-based ad hoc conferencing. Meet-me conferencing requires a range of meet-me conference numbers that are created in the Cisco call-control system and allocated for exclusive use of the conference.

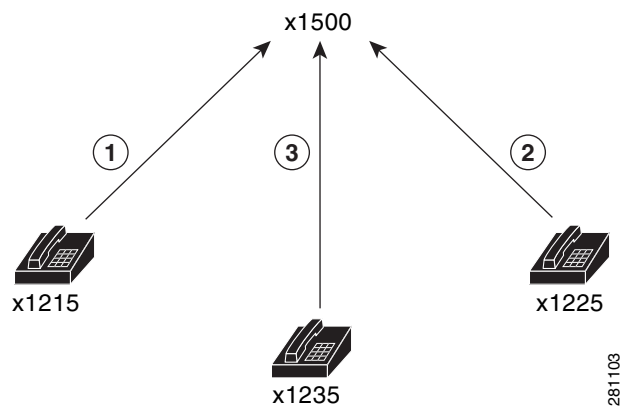
To start an SCCP Meet-Me Conference on an analog phone connected to a voice gateway, you must dial a FAC consisting of a prefix plus a feature code. The default FAC for SCCP Meet-Me Conference is **5.

When you start a meet-me conference, the Cisco call-control system considers you the conference controller. When a meet-me conference is set up, you choose a meet-me conference number and advertise it to conference participants. Participants call the number to join the conference. Anyone who calls the number while the conference is active joins the conference if the number of participants does not exceed the maximum number of parties specified for the conference type and sufficient streams are available on the conference device.

In [Figure 1](#), extensions 1215, 1225, and 1235 are all parties in a meet-me conference on extension number 1500. The conference is created as follows:

1. The conference controller at extension 1215 presses the FAC for SCCP Meet-Me Conference, hears a confirmation tone, and then dials the meet-me conference number 1500.
2. Extension 1225 and extension 1235 joins the meet-me conference by dialing 1500.
3. Extension 1235 joins the meet-me conference by dialing 1500.

Figure 1 Simple Meet-Me Conference



If other phone users press the meet-me FAC and then dial the same meet-me conference number, the Cisco call-control system ignores the signal.

A meet-me conference continues even if the conference controller hangs up.

If only one participant remains in the meet-me conference, for example, if one participant forgets to hang up, the conference call is disconnected after five minutes to free system resources.

If the conference controller is waiting for participants to join the conference and is the only party on the conference, the conference is not disconnected because significant resources are not being used.

For configuration information, see the [“Configuring Feature Access Codes”](#) section on page 71.

How to Configure SCCP Analog FXS Ports with Supplementary Features in Cisco IOS Gateways

**Note**

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

This section contains the following tasks for setting up SCCP analog phone support:

- [Configuring Feature Access Codes, page 71](#) (optional)
- [Enabling and Changing Feature Speed-Dial Codes, page 78](#) (optional)

Configuring Feature Access Codes

To enable FACs and enter STC application feature access-code configuration mode for defining a prefix other than the default (**) or a feature code other than the default for a particular feature, perform the following steps.

**Note**

The Flexible Feature Access Code feature also affects only the FSD for redial. If you want the phone user to just dial the speed-dial code to access the Redial feature, configure a redial speed-dial code that begins or ends with an asterisk (*) or number sign (#) by using the **redial** command. For configuration information, see the [“Enabling and Changing Feature Speed-Dial Codes”](#) section on page 78.

**Note**

In Cisco IOS 15.0(1)M and later releases, a user can dial a three or four digit FAC without a prefix, for all the features under scapp FACs and for voice mail under scapp feature speed-dial.

Prerequisites

- Cisco IOS Release 12.4(2) or a later release.
- To configure a FAC that does not require the user to dial a prefix, Cisco IOS Release 12.4(20)YA or a later release.
- To configure an all-numeric feature code, Cisco IOS Release 15.0(1)M or a later release.

For SCCP Meet-Me Conference and Analog Endpoints in Cisco Unified Communications Manager

- A hardware conference bridge is configured in Cisco Unified Communications Manager. Configure the same bridge name for the hardware conference bridge and for the Cisco IOS bridge. Security mode can be encrypted, authenticated or non-secure. See the “Conference Bridge Configuration” section of the “Media Resource Configuration” chapter in the appropriate [Cisco Unified Communications Manager Administration Guide](#).
- Meet-Me page and conference numbers are configured in Cisco Unified Communications Manager. See the “Meet-Me Number/Pattern Configuration” section of the “Call Routing” chapter in the appropriate [Cisco Unified Communications Manager Administration Guide](#).

For SCCP Meet-Me Conference and Analog Endpoints in Cisco Unified CME

- Meet-Me Conferencing and meet-me conference numbers are configured in Cisco Unified CME. For configuration information, see [“How to Configure Conferencing”](#) in the *Cisco Unified CME System Administrator Guide*.

Restrictions

- In Cisco IOS Release 12.4(20)YA and later releases, if you configure the same value for more than one feature code or speed-dial code, or for the Redial FSD, the system implements the first feature it matches in the order of precedence shown in the output of the **show stcapp feature codes** command.
- In Cisco IOS Release 12.4(20)YA and later releases, if you configure feature codes for FACs or speed-dial codes for FSDs, including the Redial FSD, to a value that precludes or is precluded by another code, the system implements the feature with the shortest feature code first. The precluded codes cannot be implemented.

For SCCP Meet-Me Conference

- Maximum number of simultaneous meet-me conferences for each Cisco Unified Communications Manager server is 100.
- The maximum number of meet-me conference parties in Cisco Unified CME is 32 for one DSP using the G.711 codec and 16 for a DSP using the G.729 codec.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp feature access-code**
4. **prefix** *prefix-string*
5. **call forward all** *keypad-character*
6. **call forward cancel** *keypad-character*
7. **cancel-call-waiting** *keypad-character*
8. **meetme-conference** *keypad-character*
9. **pickup local** *keypad-character*
10. **pickup group** *keypad-character*
11. **pickup direct** *keypad-character*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>stcapp feature access-code</code> Example: Router(config)# stcapp feature access-code	Enables FACs and enters STC application feature access-code configuration mode.
Step 4	<code>prefix prefix-string</code> Example: Router(config-stcapp-fac)# prefix *#	(Optional) Sets a prefix string to indicate that the following keypad character is a feature access code. <ul style="list-style-type: none"> <i>prefix-string</i>—One to five characters that can be dialed on a telephone keypad. The leading character must be an asterisk (*) or a number sign (#). Default is **. Configuring the prefix command changes the prefix for all FACs.
Step 5	<code>call forward all keypad-character</code> Example: Router(config-stcapp-fac)# call forward all 2	(Optional) Sets the code to use for enabling call-forward-all on FXS ports. <ul style="list-style-type: none"> <i>keypad-character</i>—String that can be dialed on a phone keypad. Default is 1. In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. In Cisco IOS Release 12.4(20)YA and later releases, the length of <i>keypad-character</i> is a single character or 2 digits (00-99). or <ul style="list-style-type: none"> To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <i>keypad-character</i> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <i>keypad-character</i> must be 3 or 4 digits (000-9999).

Command or Action	Purpose
<p>Step 6</p> <p><code>call forward cancel keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# call forward cancel 3</p>	<p>(Optional) Sets the code to canceling call-forward-all on FXS ports.</p> <ul style="list-style-type: none"> • <i>keypad-character</i>—String that can be dialed on a phone keypad. Default is 2. • In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. • In Cisco IOS Release 12.4(20)YA and later releases, the length of <i>keypad-character</i> is a single character or 2 digits (00-99). <p>or</p> <ul style="list-style-type: none"> • To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <i>keypad-character</i> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). • In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <i>keypad-character</i> must be 3 or 4 digits (000-9999).
<p>Step 7</p> <p><code>cancel-call-waiting keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# cancel-call-waiting 9</p>	<p>(Optional) Sets the code to cancel call waiting on FXS ports.</p> <ul style="list-style-type: none"> • This command is supported in Cisco IOS Release 15.1(1)T and later releases. • <i>keypad-character</i>—String that can be dialed on a phone keypad. Allowed values are a single digit (0-9), two digits (00-99) and # or *. Default is 8. • To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <i>keypad-character</i> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#).

Command or Action	Purpose
<p>Step 8 <code>meetme-conference keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# meetme-conference #55</p>	<p>(Optional) Sets the code to use for enabling meet-me conferencing on FXS ports.</p> <ul style="list-style-type: none"> This command is supported in Cisco IOS Release 12.4(20)YA and later releases. <i>keypad-character</i>—String that can be dialed on a telephone keypad. Default is 5. Length of <i>keypad-character</i> is a single character (0-9, *, #) or two digits (00-99) <p>or</p> <ul style="list-style-type: none"> To configure the code so that the analog phone user is not required to dial the prefix to access this feature, the length is 2-4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <i>keypad-character</i> must be 3 or 4 digits (000-9999).
<p>Step 9 <code>pickup local keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# pickup local 6</p>	<p>(Optional) Sets the code to use for picking up calls from the local pickup group; that is, for picking up a call by dialing the prefix and code.</p> <ul style="list-style-type: none"> <i>keypad-character</i>—String that can be dialed on a phone keypad. Default is 3. In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. In Cisco IOS Release 12.4(20)YA and later releases, the length of <i>keypad-character</i> is a single character or 2 digits (00-99). <p>or</p> <ul style="list-style-type: none"> To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <i>keypad-character</i> must be 2 to 4 characters and the leading or ending character of the string must be an asterisk (*) or a number sign (#). In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <i>keypad-character</i> must be 3 or 4 digits (000-9999).

Command or Action	Purpose
<p>Step 10 <code>pickup group keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# pickup group 5</p>	<p>(Optional) Sets the code to use for picking up calls from a different pickup group; that is, for picking up a call by dialing the prefix, code, and pickup group number.</p> <ul style="list-style-type: none"> <code>keypad-character</code>—String that can be dialed on a phone keypad. Default is 4. In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. In Cisco IOS Release 12.4(20)YA and later releases, the length of <code>keypad-character</code> is a single character or 2 digits (00-99). <p>or</p> <ul style="list-style-type: none"> To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <code>keypad-character</code> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <code>keypad-character</code> must be 3 or 4 digits (000-9999).
<p>Step 11 <code>pickup direct keypad-character</code></p> <p>Example: Router(config-stcapp-fac)# pickup direct 4</p>	<p>(Optional) Sets the code to use for directly picking up calls; that is, for picking up a call by dialing the prefix, code, and extension number of a ringing phone or parked call.</p> <ul style="list-style-type: none"> <code>keypad-character</code>—String that can be dialed on a phone keypad. Default is 6. In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. In Cisco IOS Release 12.4(20)YA and later releases, the length of <code>keypad-character</code> is a single character or 2 digits (00-99). <p>or</p> <ul style="list-style-type: none"> To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <code>keypad-character</code> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). <p>Note This command is not supported for Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <code>keypad-character</code> must be 3 or 4 digits (000-9999).

	Command or Action	Purpose
Step 12	<pre>end</pre> <p>Example: Router(config-stcapp-fac)# end</p>	Exits STC application feature access-code configuration mode and returns to privileged EXEC mode.

Examples

The following example shows FACs enabled and the changes to some of the default settings:

```
Router# show running-config
.
.
.
stcapp feature access-code
  prefix *#
  call forward all 2
  call forward cancel 9
!
```

The following output from the **show stcapp feature codes** command displays the default and nondefault settings for FACs. The FAC prefix has been set to *# (asterisk, number sign).

```
Router# show stcapp feature codes

stcapp feature access-code
malicious call ID (MCID) ***
prefix *#
call forward all *#2
call forward cancel *#9
pickup local group *#3
pickup different group *#4
pickup direct *#6
cancel call waiting *#9
```

Cisco IOS Release 12.4(20)YA and Later Releases

In the following example configuration, phone users are not required to dial the FAC prefix to access the Call Forward All and Call Forward Cancel features because the feature code is at least two characters and begins or ends with an asterisk (*) or number sign (#), making it a flexible FAC. A phone user must dial only #74 and, following the confirmation tone, the target number to forward all incoming calls to the target phone number.

```
Router# show running-config
.
.
.
stcapp feature access-code
call forward all #74
call forward cancel 18#
```


The following output from the **show stcapp feature codes** command displays the default and nondefault settings for FACs. In this configuration, all of the FACs settings are for default values.

```
Router# show stcapp feature codes
```

```
stcapp feature access-code
malicious call ID (MCID) ***
prefix **
call forward all **1
call forward cancel **2
pickup local group **3
pickup different group **4
pickup direct **6
meetme-conference **5
cancel call waiting **8
```

Enabling and Changing Feature Speed-Dial Codes

To enable FSDs, define a prefix other than the default (*), and define speed-dial codes, perform the following steps on the Cisco voice gateway.



Note

This procedure enables analog phone users to access up to 99 speed-dial numbers configured on the call-control device. To use bulk speed-dial numbers up to 9,999, no specific configuration is required on the Cisco voice gateway. See the documentation provided for your call-control system for information on configuring up to 9,999 speed dials.

Prerequisites

- Speed dial codes from 0 to 9 require Cisco IOS Release 12.4(2)T or a later release; speed dial codes from 10 to 99 require Cisco IOS Release 12.4(6)T or a later release.
- To use speed-dial codes 34 to 99 on analog phones controlled by Cisco Unified CME, you must configure directory entries in telephony-service configuration mode. The following example sets a directory entry for speed-dial codes 34 and 35. When an analog phone user dials 34, extension 1602 is dialed.

```
Router(config)# telephony-service
Router(config-telephony)# directory entry 34 1602 name payroll
Router(config-telephony)# directory entry 35 1603 name security
```

For more information, see [“Configuring Speed Dial”](#) in the *Cisco Unified Communications Manager Express System Administration Guide*.

- To configure an FSD for Redial that does not require the phone user to dial a prefix, Cisco IOS Release 12.4(20)YA or a later release.
- To configure an all-numeric FSD for Redial, Cisco IOS 15.0(1)M or a later release.

Restrictions

- In Cisco IOS Release 12.4(20)YA and later releases, if you configure the same value for more than one feature code or speed-dial code, or for the Redial FSD, the system implements the first feature it matches in the order of precedence shown in the output of the **show stcapp feature codes** command.
- In Cisco IOS Release 12.4(20)YA and later releases, if you configure feature codes for FACs or speed-dial codes for FSDs, including the Redial FSD, to a value that precludes or is precluded by another code, the system implements the feature with the shortest feature code first. The precluded codes cannot be implemented.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp feature speed-dial**
4. **digit number**
5. **prefix prefix-string**
6. **speed dial from digit to digit**
7. **redial keypad-character**
8. **voicemail keypad-character**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp feature speed-dial Example: Router(config)# stcapp feature speed-dial	Enables FSD codes and enters STC application feature speed-dial configuration mode to set speed-dial prefixes and codes.

	Command or Action	Purpose
Step 4	<p>digit <i>number</i></p> <p>Example: Router(config-stcapp-fsd)# digit 2</p>	<p>(Optional) Sets the number of digits that are used for speed-dial codes.</p> <ul style="list-style-type: none"> This command is supported in Cisco IOS Release 12.4(6)T and later releases. <i>number</i>—Number of digits to enter for speed-dial codes. Value is 1 or 2. Default is 1. <p>Note Modifying the value of this command resets the speed dial and voicemail commands to their defaults.</p>
Step 5	<p>prefix <i>prefix-string</i></p> <p>Example: Router(config-stcapp-fsd)# prefix ##</p>	<p>(Optional) Sets a prefix string to indicate that the following keypad character is a speed-dial code.</p> <ul style="list-style-type: none"> <i>prefix-string</i>—One to five characters that can be dialed on a phone keypad. Lead character must be an asterisk (*) or a number sign (#). Default is *.
Step 6	<p>speed dial from <i>digit to digit</i></p> <p>Example: Router(config-stcapp-fsd)# speed dial from 2 to 7</p>	<p>(Optional) Sets the range of codes to use for dialing speed-dial numbers in ascending or descending order.</p> <ul style="list-style-type: none"> <i>digit</i>—Starting and ending number for the range of speed-dial codes. Range is: <ul style="list-style-type: none"> 0 to 9 for one-digit codes. Allows a maximum of nine speed-dial codes. This means that if you set the starting number to 0, the highest number you can set for the ending number is 8. Default is 1 to 9. 00 to 99 for two-digit codes. Allows a maximum of 99 speed-dial codes. Default is 01 to 99. <p>Note Number of allowed digits depends on the value set with the digit command.</p>

Command or Action	Purpose
<p>Step 7 <code>redial keypad-character</code></p> <p>Example: Router(config-stcapp-fsd)# redial 9</p>	<p>(Optional) Sets the code to use for redialing the last number dialed.</p> <ul style="list-style-type: none"> • <i>keypad-character</i>—String that can be dialed on a phone keypad. Default is #. • In Cisco IOS Release 12.4(20)YA and earlier releases, this is a single character. Value: 0-9, #, or *. • In Cisco IOS Release 12.4(20)YA and later releases, the length of <i>keypad-character</i> is a single character or 2 digits (00-99). <p>or</p> <ul style="list-style-type: none"> • To configure the code so that the phone user is not required to dial the prefix to access this feature, the length of <i>keypad-character</i> must be 2 to 4 characters and the leading or ending character must be an asterisk (*) or a number sign (#). • In Cisco IOS 15.0(1)M and later releases, to configure the code so that the phone user is not required to dial the prefix or any special character to access this feature, the length of <i>keypad-character</i> must be 3 or 4 digits (000-9999).
<p>Step 8 <code>voicemail keypad-character</code></p> <p>Example: Router(config-stcapp-fsd)# voicemail 8</p>	<p>(Optional) Sets the code to use for dialing the voice-mail number that is defined in Cisco Unified Communications Manager or the Cisco Unified CME router.</p> <ul style="list-style-type: none"> • <i>keypad-character</i>—One or two digits that can be dialed on a telephone keypad. Default is 0 (zero) for single digits; 00 (two zeros) for two digits. <p>Note Number of digits allowed depends on the value set with the digit command.</p>
<p>Step 9 <code>end</code></p> <p>Example: Router(config-stcapp-fsd)# end</p>	<p>Exits STC application feature speed-dial configuration mode and returns to privileged EXEC mode.</p>

Examples

Cisco IOS Release 12.4(2)T

The following example shows FSD codes enabled and the changes to some of the default settings in Cisco IOS Release 12.4(2)T:

```
Router# show running-config
.
.
.
stcapp feature speed-dial
  prefix ##
  redial 9
  voicemail 8
  speed dial from 2 to 7
!
```

The following output from the **show stcapp feature codes** command displays the default and nondefault settings for FSD codes and shows how the speed-dial range set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6. To dial the telephone number that is stored for speed-dial 1 on Cisco Unified Communications Manager or Cisco Unified CME, an analog phone user presses ##2.

```
Router# show stcapp feature codes
.
.
.
stcapp feature speed-dial
  prefix ##
  redial ##9
  voicemail ##8
  speeddial1 ##2
  speeddial2 ##3
  speeddial3 ##4
  speeddial4 ##5
  speeddial5 ##6
  speeddial6 ##7
```

Cisco IOS Release 12.4(6)T

The following example shows FSD codes enabled and the changes to some of the default settings in Cisco IOS Release 12.4(6)T:

```
Router# show running-config
.
.
.
stcapp feature speed-dial
 digit 2
 voicemail 55
 speed dial from 11 to 17
!
```

The following output from the **show stcapp feature codes** command displays the default and nondefault settings for FSD codes and shows how the speed-dial range set in the preceding example is mapped to the speed-dial positions on the call-control system. Note that the range from 11 to 17 is mapped to speed-dial 1 to 7. To dial the telephone number that is stored for speed-dial 1 on Cisco Unified Communications Manager or Cisco Unified CME, an analog phone user presses *11.

```
Router# show stcapp feature codes
.
.
.
stcapp feature speed-dial
 prefix *
 redial *#
 speeddial number of digit(s) 2
 voicemail *55
 speeddial1 *11
 speeddial2 *12
 speeddial3 *13
 speeddial4 *14
 speeddial5 *15
 speeddial6 *16
 speeddial7 *17
```

Configuration Examples for SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways

The following example shows a configuration for a Cisco VG224 Analog Phone Gateway:

```
Router# show running-config

Building configuration...

Current configuration : 3442 bytes
!
.
.
.
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource manager
!
ip subnet-zero
no ip dhcp use vrf connected
!
!
no ftp-server write-enable
!
stcapp ccm-group 1
stcapp
!
stcapp feature access-code
prefix *#
call forward all 2
call forward cancel 9
!
stcapp feature speed-dial
prefix ##
redial 9
voicemail 8
speed dial from 3 to 7
!
!
template address
!
voice-card 0
!
!
!
!
!
interface FastEthernet0/0
ip address 10.4.138.5 255.255.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
```

```
duplex auto
speed auto
!
ip default-gateway 10.4.0.1
ip classless
ip route 223.255.254.0 255.255.255.0 10.4.0.1
!
ip http server
!
!
!
control-plane
!
!
voice-port 2/0
  caller-id enable
!
voice-port 2/1
  caller-id enable
!
voice-port 2/2
  caller-id enable
!
voice-port 2/3
  caller-id enable
!
voice-port 2/4
!
.
.
.
!
voice-port 2/23
!
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.131.200 identifier 7815
sccp ccm 10.4.138.77 identifier 7825
sccp
!
sccp ccm group 1
  associate ccm 7815 priority 1
  associate ccm 7825 priority 2
!
!
dial-peer voice 500 pots
  service stcapp
  port 2/0
!
dial-peer voice 501 pots
  service stcapp
  port 2/1
!
dial-peer voice 502 pots
  service stcapp
  port 2/2
!
dial-peer voice 503 pots
  service stcapp
  port 2/3
!
dial-peer voice 504 pots
  service stcapp
```



```

port 2/4
!
.
.
!
dial-peer voice 523 pots
  service stcapp
  port 2/23
!
!
line con 0
  exec-timeout 0 0
  transport preferred all
  transport output all
line aux 0
  transport preferred all
  transport output all
line vty 0 4
  login
  transport preferred all
  transport input all
  transport output all
!
end

```

The following example shows the expanded command for call-control mode feature:

You can now configure a string of up to 4 characters (0 – 9, *, #) as the feature code for the 5 features (the defaults are #1 for “hangup last active call”, #2 for “transfer”, #3 for “conference”, #4 for “drop last conferee”, and #5 for “toggle between two calls”) under stcapp feature mode.

```

VG224 (config)#stcapp call-control mode feature
VG224 (config-stcapp-fmcode)#?
STCAPP feature fm-code configuration commands:
  conference           Select code for conference
  default              Set a command to its defaults
  drop-last-conferee  Select code for drop last conferee
  exit                 Exit from stcapp feature fmcode configuration mode
  hangup-last-active-call Select code for hangup last active call
  no                   Negate a command or set its defaults
  toggle-between-two-calls Select code for toggle between two calls
  transfer             Select code for transfer

VG224 (config-stcapp-fmcode)#hangup-last-active-call 456
VG224 (config-stcapp-fmcode)#toggle-between-two-calls 7890
VG224 (config-stcapp-fmcode)#conference 12#
VG224 (config-stcapp-fmcode)#end

VG224# show stcapp feature code

stcapp feature access-code
  malicious call ID (MCID) ***
  prefix **
  call forward all 111
  call forward cancel **2
  pickup local group **3
  pickup different group **4
  pickup direct **6
  meetme-conference **5
  forward-to-voicemail 1234

```

```
stccpp feature speed-dial
  prefix *
  redial *#
  speeddial number of digit(s) 1
  voicemail 777
  speeddial1 *1
  speeddial2 *2
  speeddial3 *3
  speeddial4 *4
  speeddial5 *5
  speeddial6 *6
  speeddial7 *7
  speeddial8 *8
  speeddial9 *9

stccpp call-control mode in feature mode
  456 -- hangup last active call
  #2 -- transfer
  12# -- conference
  #4 -- drop last conferee
  7890 -- toggle between two calls
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager documentation
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express documentation
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series documentation • Cisco 1800 Series Integrated Services Routers documentation • Cisco 2800 Integrated Services Routers documentation • Cisco 3800 Series Integrated services Routers documentation • Cisco Unified 500 Series documentation
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways

[Table 3](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(2)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 3](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for SCCP Controlled Analog (FXS) Ports

Feature Name	Releases	Feature Information
Cancel Call Waiting	15.1(1)T 15.0(1)XA	<p>Adds FAC for Cancel Call Waiting feature.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Cancel Call Waiting, page 69 • Configuring Feature Access Codes, page 71 <p>The following commands were introduced or modified by this feature: cancel-call-waiting, show stcapp device, show stcapp feature codes.</p>
Distinctive Ringing on SCCP IOS gateways	15.0(1)M	<p>Enables distinct ring tone to alert user whether incoming call is from an internal or external phone.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Summary of SCCP Supplementary Features for FXS ports, page 58 <p>The following command was modified by this feature: ring cadence</p>
Enhanced Speed Dial on SCCP Analog Phones	12.4(6)T	<p>Allows you to define two-digit speed-dial codes for accessing up to 99 local speed-dial numbers configured on the call-control device.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Enhanced Speed Dial on SCCP Analog Phones, page 68 • Enabling and Changing Feature Speed-Dial Codes, page 78 <p>The following commands were new or modified by this feature: digit, speed dial</p>

Table 3 Feature Information for SCCP Controlled Analog (FXS) Ports (continued)

Feature Name	Releases	Feature Information
Flexible Feature Access Codes	12.4(20)YA	<p>Allows you to configure feature codes for feature access codes (FACs), and the speed-dial code for Redial, so that phone users are not required to dial the prefix before dialing the feature code to access an SCCP feature on an analog phone.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Flexible Feature Access Codes, page 66 • Flexible Feature Access Code Support for Redial, page 68 • Configuring Feature Access Codes, page 71 <p>The following commands were modified by this feature: call forward all, call forward cancel, pickup direct, pickup group, pickup local, redial.</p>
Enhanced Flexible FACs	15.0(1)M	<p>Allows you to configure feature codes for Flexible feature access codes (FACs) so that phone users are not required to dial the prefix or special characters to access an SCCP feature on an analog phone.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Enhanced Flexible Feature Access Code, page 68 • Configuring Feature Access Codes, page 71 <p>The following commands were modified by this feature: call forward all, call forward cancel, pickup direct, pickup group, pickup local, redial.</p>
Forward to Voice Mail	15.0(1)M	<p>Adds FAC for Forward to Voice Mail feature.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • FACs for SCCP Supplementary Features for Analog FXS Ports, page 63 <p>The following command was modified by this feature:</p>

Table 3 Feature Information for SCCP Controlled Analog (FXS) Ports (continued)

Feature Name	Releases	Feature Information
SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways	12.4(2)T	<p>Enables SCCP supplementary features on analog FXS ports on a Cisco VG224 Analog Phone Gateway under the control of Cisco Unified Communications Manager or Cisco Unified CME.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Summary of SCCP Supplementary Features for FXS ports, page 58 • Configuring Feature Access Codes, page 71 <p>The following commands were introduced or modified by this feature: call forward all, call forward cancel, debug voip application stcapp buffer-history, pickup direct, pickup group, pickup local, prefix (stcapp-fac), prefix (stcapp-fsd), redial, show stcapp buffer-history, show stcapp device, show stcapp feature codes, speed dial, stcapp feature access-code, stcapp feature speed-dial, voicemail (stcapp-fsd).</p>
	12.4(9)T	<p>Adds support for SCCP supplementary features on analog FXS ports on Cisco ISRs.</p>
SCCP Meet-Me Conference	12.4(20)YA	<p>Adds FAC to enable user on an analog SCCP phone to start or join a meet-me conference call. To initiate a meet-me conference, a phone user presses the FAC prefix and feature code for SCCP Meet-Me Conference (default **5) and dials the meet-me conference number. Participants can join the conference by dialing in.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • SCCP Meet-Me Conference, page 69 • Configuring Feature Access Codes, page 71 <p>The following commands were introduced by this feature: meetme-conference.</p>



Configuring Feature Mode

First Published: June 22, 2006

Last Updated: March 19, 2010

This module describes how to enable the Skinny Client Control Protocol (SCCP) feature mode call-control mode for analog foreign exchange service (FXS) ports on Cisco voice gateways, including Cisco VG224 Analog Phone Gateways and Cisco Integrated Services Routers (ISRs), and under the control of Cisco Unified Communications Manager or Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Feature Mode for SCCP FXS Ports in Cisco IOS Feature](#)” section on page 104.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring Feature Mode for SCCP FXS Ports in Cisco IOS](#), page 94
- [Restrictions for Feature Mode for SCCP FXS Ports in Cisco IOS](#), page 94
- [Information About Feature Mode for SCCP FXS Ports in Cisco IOS](#), page 95
- [How to Configure Feature Mode for SCCP FXS Ports in Cisco IOS](#), page 98
- [Configuration Examples for Feature Mode for SCCP FXS Ports in Cisco IOS](#), page 102
- [Additional References](#), page 102
- [Feature Information for Feature Mode for SCCP FXS Ports in Cisco IOS Feature](#), page 104

Prerequisites for Configuring Feature Mode for SCCP FXS Ports in Cisco IOS

Cisco IOS Gateway

- Cisco IOS Release 12.4(6)XE or a later release.
- The Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the [Cisco IOS Voice Port Configuration Guide](#).
- SCCP and the SCCP telephony control (STC) application is enabled on the Cisco voice gateway. For configuration information, see the [“Configuring FXS Ports for Basic Calls” section on page 17](#).

Analog Endpoints in Cisco Unified Communications Manager

- Cisco Unified Communications Manager 4.2 or a later version.
- Phones are added and configured in Cisco Unified Communications Manager. See the “Directory Number Configuration” chapter under “Call Routing Configuration” and the “Gateway Configuration” chapter under “Device Configuration” in the appropriate [Cisco Unified Communications Manager Administration Guide](#).

Analog Endpoints in Cisco Unified CME

- Cisco Unified CME 4.0 or a later version.
- Ephone configurations and feature parameters for analog endpoints are configured in Cisco Unified CME. For information, see the [Cisco Unified CME Administration Guide](#).
- To use call transfer on analog endpoints in Cisco Unified CME, set the **transfer-system** command to full-consult on the Cisco router. For configuration information, see the [“Configuring Call Transfer and Forwarding”](#) module in the [Cisco Unified CME Administration Guide](#).

The following example shows how to configure full consultation as the call transfer method:

```
Router(config)# telephony-service
Router(config-telephony)# transfer-system full-consult
```

- For the Drop Last Party feature in Cisco Unified CME 4.0:
 - Cisco IOS Release 12.4(9)T or a later release.
 - The **keep-conference drop-last** command is enabled on Cisco router. For configuration information, see the [“Configuring Conferencing”](#) module in the [Cisco Unified CME Administration Guide](#).

Restrictions for Feature Mode for SCCP FXS Ports in Cisco IOS

Analog Endpoints in Cisco Unified CME

- Autoconfiguration using TFTP download of extensible markup language (XML) dial-peer configuration files from Cisco Unified Communications Manager is not supported
- This feature is not supported on a VIC2-2BRI-NT/TE.

Information About Feature Mode for SCCP FXS Ports in Cisco IOS

To configure the Feature Mode for SCCP FXS Ports in Cisco IOS feature, you should understand the following concepts:

- [Summary of Supported Features in Feature Mode, page 95](#)
- [Feature Mode for SCCP FXS Ports in Cisco IOS, page 96](#)

Summary of Supported Features in Feature Mode

Table 1 contains a list of SCCP supplementary features that are supported in feature mode on analog phones connected to FXS ports, along with descriptions and information about how to configure support for each feature in your Cisco call-control system.



Note

For information about individual commands in Cisco Unified CME, see the [Cisco Unified CME Command Reference](#).

Table 1 **Feature Mode: Supported Supplementary Features**

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
Call Transfer Connects call to a third party that the phone user dials.	User in basic call mode presses hookflash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, user presses hookflash to get feature tone and then dials #2 to transfer the call; the user hears silence after the call is transferred.	Cisco Unified Communications Manager For feature information, see the “Making and Receiving Multiple Calls Per Directory Number” section of the “Understanding Directory Numbers” chapter under “Dial Plan Architecture” in the Cisco Unified Communications Manager System Guide . Cisco Unified CME To configure, see “ Configuring Call Transfer and Forwarding ” in the Cisco Unified CME Administration Guide .
Conference Call Initiates a three-party conference.	User in basic call mode presses hookflash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, user presses hookflash to get feature tone and then dials #3 to initiate a three-party conference.	Cisco Unified Communications Manager For feature information, see the “Initiating an Ad Hoc Conference Bridge” section of the “Conference Bridges” chapter under “Media Resources” in the Cisco Unified Communications Manager System Guide . Cisco Unified CME To configure, see “ Configuring Conferencing ” in the Cisco Unified CME Administration Guide .

Table 1 Feature Mode: Supported Supplementary Features (continued)

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
Drop Last Conferee	<p>Cisco Unified Communications Manager</p> <p>The next hookflash after a three-party conference call is established drops the last conferee.</p> <p>Cisco Unified CME</p> <p>During a three-party conference, user presses hookflash to get feature tone and then dials #4 to drop the last active party. The conference becomes a basic call to the second call party.</p>	No additional configuration is required on the Cisco call-control system.
Hang Up Last Call	<p>During a three-party conference, user presses hookflash to get feature tone and then dials #1 to drop the last active call party. The conference becomes a basic call.</p>	<p>Cisco Unified Communications Manager</p> <p>No additional configuration is required on the Cisco call-control system.</p> <p>Cisco Unified CME</p> <p>The keep-conference drop-last command is enabled on Cisco router. For configuration information, see the “Configuring Conferencing” module in the <i>Cisco Unified CME Administration Guide</i>.</p>
Toggle Between Calls	<p>User in basic call mode presses hookflash to get the first dial tone, then dials an extension number to connect to a second call. During the second call, user presses a hookflash to get feature tone and then dials #5 to toggle back to the previous call party.</p>	No additional configuration is required on the Cisco call-control system.

Feature Mode for SCCP FXS Ports in Cisco IOS

In Cisco IOS Release 12.4(6)XE and later releases, Feature Mode for SCCP FXS Ports in Cisco IOS provides enhanced call-control mode capability on analog ports on Cisco voice gateways. Before Cisco IOS Release 12.4(6)XE, the SCCP analog gateway supported only standard mode feature activation, the default telephony mode which provides standard Bellcore features.

When feature mode is enabled on a Cisco voice gateway, calls through the analog FXS ports are controlled by Cisco Unified Communications Manager or by Cisco Unified CME, with basic call support in SRST mode. The SCCP telephony control (STC) application on the Cisco voice gateway functions as a proxy to translate call-control messages between the Cisco call-control system and the voice gateway.

In feature mode, the user enters a specific combination of digits called feature access codes (FACs) consisting of a prefix plus a feature code, for example #1. The prefix for FACs in feature mode is a number sign (#). In standard mode, the user uses a hookflash to activate supplementary features like call transfer and call conference.

Feature mode is limited to outgoing calls only. All feature mode functions are performed after the second call is established. A user in basic call mode performs a hookflash to get the first dial tone, then dials an extension number to connect to a second call. When the second call is established, the user performs a hookflash to get a feature tone, a special dial tone used to indicate feature mode, then dials the FAC.

[Table 2](#) lists FACs used to access telephony features in feature mode only.

Table 2 *FACs Used to Access Telephony Features in Feature Mode*

Feature	FAC
Drop last active call	#1
Call transfer	#2
Call conference	#3
Drop last conferee	#4
Toggle between two calls	#5



Note

For a list of FACs and feature speed dials (FSDs) that are available in both feature mode and standard mode, see the [“Summary of SCCP Supplementary Features for FXS ports”](#) section on page 58.

For configuration information for feature mode, see the [“How to Configure Feature Mode for SCCP FXS Ports in Cisco IOS”](#) section on page 98.

Flexible FACs in Feature Mode

Before Cisco IOS Release 15.0(1)M, FACs in feature mode were limited to two characters (# and 1 to 5) and could not be modified.

In Cisco IOS Release 15.0(1)M and later releases, you can configure FACs for accessing features that are supported in feature mode to create four-character (0-9, #, *) strings that can be dialed on the keypad after the user hears the feature tone. The default FACs for telephony features in feature mode continue to be supported. For default FACs in feature mode, see [Table 2](#).

If you attempt to set a FAC to a value that is already configured for another FAC in feature mode, you receive a warning message. If you configure a duplicate FAC, the system implements the first feature it matches in the order of precedence as determined by the value for each FAC.

If you attempt to set a FAC to a value that precludes or is precluded by another FAC in feature mode, you receive a warning message. For example, if you attempt to set a FAC of 123 and 12 is already configured for another feature, such as Call Transfer, the following message appears:

```
123 is precluded by call transfer(12)
```

Or if you attempt to configure 1 and 12 is already configured for another feature, such as Call Transfer, the following message appears:

```
1 precludes call transfer(12)
```

These messages will not prevent you from configuring the feature code.

For configuration information, see the [“Configuring Flexible FACs in Feature Mode”](#) section on page 99.

Feature Mode Error Handling

If the user does nothing after feature tone is heard, the interdigit timeout expires and a fast busy tone is played. The user must press hookflash again to toggle back to the previous state. User input other than a hookflash is not accepted during a fast busy tone.

If the user dials an incorrect combination of digits, the fast busy tone is played. The user must perform a hookflash to toggle back to the previous state.

If the user hangs up after feature tone is heard, then power-ring-back on the phone is played. If the user goes off hook, the user is connected to the first call.

If the user performs any of the following actions, the call is transferred:

- Hangs up after feature tone is heard and before the interdigit timeout expires.
- Hangs up after feature tone is heard and after the interdigit timeout expires and the fast busy tone is heard.
- Hangs up after the feature tone is heard and after an incomplete digit is pressed and no fast busy tone is heard.
- Hangs up after the feature tone is heard and after an incorrect digit combination is pressed and a fast busy tone is heard.

How to Configure Feature Mode for SCCP FXS Ports in Cisco IOS

This section contains the following tasks:

- [Configuring Feature Mode, page 98](#) (required)
- [Troubleshooting the Feature Mode for SCCP FXS Ports Configuration, page 99](#) (optional)
- [Configuring Flexible FACs in Feature Mode, page 99](#) (optional)

Configuring Feature Mode

To configure feature mode for SCCP analog phones on a Cisco voice gateway and enable SCCP analog phones to invoke features using standard FACs after hookflash, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp call-control mode feature**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp call-control mode feature Example: Router(config)# stcapp call-control mode feature	Enables feature call control mode.
Step 4	exit Example: Router(config-stcapp-fmcode)# exit	Exits global configuration mode.

Troubleshooting the Feature Mode for SCCP FXS Ports Configuration

Use the following commands to verify and troubleshoot call control modes and display debugging information for feature mode calls:

- **show stcapp feature codes**—Displays feature access codes.
- **debug voip application stcapp all**—Displays debugging messages for STC application-controlled phones configured in feature mode.
- **debug voip application stcapp port**—Displays debugging information for the components of the STCAPP for a specified port
- **debug vpm signal**—Displays information for signaling events for feature and standard mode calls, including PBX signaling.

For information about these commands, see the [Cisco IOS Voice Command Reference](#) or the [Cisco IOS Debug Command Reference, Release 12.4T](#), and [Cisco IOS Configuration Fundamentals Command Reference, Release 12.4](#).

Configuring Flexible FACs in Feature Mode

To define a feature access codes (FACs) to invoke features supported in feature mode, perform the following steps.

Prerequisites

- Cisco IOS Release 15.0(1)M or a later release.

Restrictions

- If you configure the same value for more than one feature code in feature mode, the system implements the first feature it matches in the order of precedence.
- If you configure a FAC to a value that precludes or is precluded by another FAC in feature mode, the system implements the feature with the shortest FAC first. The precluded FAC cannot be implemented.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp call-control mode feature**
4. **conference** *keypad-character*
5. **hangup-last-active-call** *keypad-character*
6. **drop-last-conferee** *keypad-character*
7. **toggle-between-two-calls** *keypad-character*
8. **transfer** *keypad-character*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp call-control mode feature Example: Router(config-stcapp-fmcode)# stcapp call-control mode feature	Enables feature call control mode and enters STC application feature-call-control configuration mode.
Step 4	conference <i>keypad-character</i> Example: Router(config-stcapp-fmcode)# conference *	(Optional) Sets the code to use for initiating a three-party conference. <ul style="list-style-type: none"> • <i>keypad-character</i>—String that can be dialed on a phone keypad. The length of <i>keypad-character</i> must be 1 to 4 characters (0-9, #, *). Default is #3.

	Command or Action	Purpose
Step 5	<p>drop-last-conferee <i>keypad-character</i></p> <p>Example: Router(config-stcapp-fmcode)# drop-last-conferee 44</p>	<p>(Optional) Sets the code to use for dropping last active call during a three-party conference.</p> <ul style="list-style-type: none"> <i>keypad-character</i>—String that can be dialed on a phone keypad. The length of <i>keypad-character</i> must be 1 to 4 characters (0-9, #, *). Default is #4. The keep-conference drop-last command must be enabled on Cisco router.
Step 6	<p>hangup-last-active-call <i>keypad-character</i></p> <p>Example: Router(config-stcapp-fmcode)# hangup-last-active-call 11</p>	<p>(Optional) Sets the code to use for dropping last active call during a three-party conference.</p> <ul style="list-style-type: none"> For phones controlled by Cisco Unified CME. This command does not affect user experience on phones controlled by Cisco Unified Communications Manager. <i>keypad-character</i>—String that can be dialed on a phone keypad. The length of <i>keypad-character</i> must be 1 to 4 characters (0-9, #, *). Default is #1.
Step 7	<p>toggle-between-two-calls <i>keypad-character</i></p> <p>Example: Router(config-stcapp-fmcode)# toggle-between-two-calls 55</p>	<p>(Optional) Sets the code to use for toggling between two active calls.</p> <ul style="list-style-type: none"> <i>keypad-character</i>—String that can be dialed on a phone keypad. The length of <i>keypad-character</i> must be 1 to 4 characters (0-9, #, *). Default is #5.
Step 8	<p>transfer <i>keypad-character</i></p> <p>Example: Router(config-stcapp-fmcode)# transfer ##</p>	<p>(Optional) Sets the code to use for connecting a call to a third party that the phone user dials.</p> <ul style="list-style-type: none"> <i>keypad-character</i>—String that can be dialed on a phone keypad. The length of <i>keypad-character</i> must be 1 to 4 characters (0-9, #, *). Default is #2.
Step 9	<p>end</p> <p>Example: Router(config-stcapp-fmcode)# end</p>	<p>Exits STC application feature access-code configuration mode and returns to privileged EXEC mode.</p>

Examples

The following example shows how to change the value of the feature code for supplementary features supported in feature mode from the defaults:

```
Router(config)# stcapp call-control mode feature
Router(config-stcapp-fmcode)# conference 33
Router(config-stcapp-fmcode)# drop-last-active-conferee 44
Router(config-stcapp-fmcode)# hangup-last-active-call 11
Router(config-stcapp-fmcode)# toggle-between-two-calls 55
Router(config-stcapp-fmcode)# transfer 22
Router(config-stcapp-fmcode)# exit
Router(config)#
```


Configuration Examples for Feature Mode for SCCP FXS Ports in Cisco IOS

The following example shows feature call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode feature
!
```

The following example shows standard call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode standard
!
```

Additional References

The following sections provide references related to the Feature Mode for SCCP FXS Ports in Cisco IOS feature.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager interoperability	Cisco Unified CallManager and Cisco IOS Interoperability Guide
Cisco Unified Communications Manager	Cisco Unified Communications Manager System Guide
Cisco Unified Communications Express	Cisco Unified CME Administrator Guide
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration guides	Cisco IOS Voice Configuration

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Feature Mode for SCCP FXS Ports in Cisco IOS Feature

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(6)XE or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Feature Mode for SCCP FXS Ports in Cisco IOS Feature

Feature Name	Releases	Feature Information
Feature Mode for SCCP FXS Ports in Cisco IOS	12.4(6)XE 12.4(11)T	<p>Enables feature mode call control on analog FXS ports on Cisco voice gateways and under the control of Cisco Unified Communications Manager or Cisco Unified CME.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Feature Mode for SCCP FXS Ports in Cisco IOS, page 95 • How to Configure Feature Mode for SCCP FXS Ports in Cisco IOS, page 98 <p>The following commands were introduced or modified by this feature: debug voip application stcapp all; debug voip application stcapp port; show stcapp feature codes; stcapp call-control mode</p>

Table 3 *Feature Information for Feature Mode for SCCP FXS Ports in Cisco IOS Feature (continued)*

Feature Name	Releases	Feature Information
Flexible FACs in Feature Mode	15.0(1)M	<p>Enables configurable feature access codes (FACs) for accessing supplementary features that are supported in feature mode.</p> <p>The following sections contain information about this feature:</p> <ul style="list-style-type: none"> • Flexible FACs in Feature Mode, page 97 • Configuring Flexible FACs in Feature Mode, page 99 <p>The following commands were introduced or modified by this feature: conference; drop-last-conferee; hangup-last-active-call; toggle-between-two-calls; transfer</p>



Configuring CallBack on Busy

First Published: August 1, 2008

Last Updated: March 19, 2010

This module describes the CallBack on Busy feature for analog phones that are connected to Foreign Exchange Station (FXS) ports on a Cisco VG224 Analog Phone Gateway or a Cisco Integrated Services Router (ISR), such as a Cisco 2800 or 3800 series ISR or a Cisco 1861. This feature is supported for analog endpoints that are controlled by Cisco Unified Communications Manager only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for CallBack on Busy for Analog Phones on Cisco Voice Gateways” section on page 114](#).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 108](#)
- [Restrictions for CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 108](#)
- [Information About CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 108](#)
- [How to Configure CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 110](#)
- [Additional References, page 113](#)
- [Feature Information for CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 114](#)

Prerequisites for CallBack on Busy for Analog Phones on Cisco Voice Gateways

Cisco IOS Gateway

- Cisco IOS Release 12.4(20)YA or a later version.
- The Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the *Cisco IOS Voice Port Configuration Guide*.
- SCCP and the SCCP telephony control (STC) application is enabled on the Cisco voice gateway. For configuration information, see the “Configuring FXS Ports for Basic Calls” section on page 17.
- SCCP supplementary features are enabled on the Cisco voice gateway. See the “Configuring Supplementary Features” section on page 55.

Analog Endpoints in Cisco Unified Communications Manager

- Cisco Unified Communications Manager 6.1.2 or a later version.
- Configure Cisco CallBack service parameters by accessing **System> Service Parameters** in Cisco Unified Communications Manager Administration; choose the server where the Cisco Unified Communications Manager service runs and then choose the Cisco Unified Communications Manager service. Unless instructed otherwise by the Cisco Technical Assistance Center, we recommend that you use the default service parameters settings. For information, see the “Call Back” section in the appropriate *Cisco Unified Communications Manager Features and Services Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Restrictions for CallBack on Busy for Analog Phones on Cisco Voice Gateways

- This feature is not supported for analog SCCP endpoints in Cisco Unified CME.
- This feature is not supported on the Cisco Unified 500 Series platform.

Information About CallBack on Busy for Analog Phones on Cisco Voice Gateways

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 109](#)
- [CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 109](#)

Feature Summary

Table 1 contains information about SCCP-based CallBack on Busy for Analog Phones on Cisco Voice Gateways, along with information about how to configure support for this feature in your Cisco call-control system.

Table 1 CallBack on Busy for Analog Phones

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>CallBack on Busy for Analog Phones</p> <p>Allows phone user to initiate an audio alert on the phone when a busy party becomes available.</p>	<p>After placing call to busy phone, user dials callback activation key to activate SCCP-based CallBack on Busy feature. Default activation key sequence is #1.</p> <p>After CallBack on Busy is activated, user hears a confirmation tone.</p> <p>The calling phone only supports one active CallBack request at a time. If a phone user tries to activate a second CallBack on Busy while a callback is already active, the first callback is canceled and replaced by an active callback for the second busy called number.</p> <p>Note The stcapp feature callback command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>Configure Cisco Callback service parameters by accessing System> Service Parameters in Cisco Unified Communications Manager Administration; choose the server where the Cisco Unified Communications Manager service runs and then choose the Cisco Unified Communications Manager service.</p> <p>Unless instructed otherwise by the Cisco Technical Assistance Center, we recommend that you use the default service parameters settings. For information on these parameters, click the question mark button in the upper corner of the Service Parameter window.</p> <p>Cisco Unified CME</p> <p>This feature is not supported for analog endpoints in Cisco Unified CME.</p>

CallBack on Busy for Analog Phones on Cisco Voice Gateways

Cisco IOS Release 12.4(20)YA introduces support for CallBack on Busy on analog phones that are connected to FXS ports on Cisco voice gateways and controlled by Cisco Unified Communications Manager 6.1.2 or a later version. In Cisco Unified Communications Manager 6.1.1 and earlier versions, CallBack on Busy is supported only on IP phones.

CallBack on Busy is supported for the following calling and called combinations:

- Calling and called phones are analog phones that are connected to the same voice gateway and are in the same Cisco Unified Communications Manager cluster.
- Calling and called phones are analog phones that are connected to different voice gateways and are in the same Cisco Unified Communications Manager cluster.
- The called phone is any Cisco Unified IP phone that is in the same Cisco Unified Communications Manager cluster as the calling phone.
- The called phone is any phone that is connected to Cisco Unified Communications Manager through a QSIG PRI trunk.

After a phone user initiates a call to a phone that is busy, the caller can activate CallBack on Busy by pressing the callback activation key sequence on the keypad. The callback activation key sequence is a one to five-character string that can be dialed on a telephone keypad (0-9, #, *). The default is #1.

The caller receives a confirmation tone indicating that CallBack on Busy is activated. The calling phone only supports one active callback request at a time. Pressing the callback activation key to activate a second callback request will cancel the first active callback and replace it with the second request. When CallBack on Busy is activated on the calling phone, the phone can be used to make other calls without affecting or canceling CallBack on Busy.

The system monitors the called and calling phones and when both phones are onhook, the calling phone receives a Callback Ringing. If the calling phone does not answer when ringing times out, CallBack on Busy is canceled.

If the caller lifts the handset when the calling phone receives a Callback Ringing, the caller hears a Ring Back Tone and the called phone begins ringing. If the called phone does not answer when ringing times out in Cisco Unified Communications Manager, CallBack on Busy is canceled.

The calling phone is not notified when a CallBack on Busy is canceled.

This feature is disabled by default. To enable this feature and to change default values for callback parameters, see the [“How to Configure CallBack on Busy for Analog Phones on Cisco Voice Gateways” section on page 110](#).

How to Configure CallBack on Busy for Analog Phones on Cisco Voice Gateways



Note

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To modify the default values of the callback activation key sequence or ringing timer for CallBack on Busy on analog SCCP phones connected to FXS ports, perform the following steps on the Cisco voice gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp feature callback**
4. **activation-key *string***
5. **ringing-timeout *seconds***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp feature callback Example: Router(config)# stcapp feature callback	Enables CallBack on Busy and enters STC application feature callback configuration mode.
Step 4	activation-key <i>string</i> Example: Router(config-stcapp-callback)# activation-key *22	(Optional) Defines the key sequence to use for activating CallBack on Busy. <ul style="list-style-type: none"><i>string</i>—String (0-9, # *) that can be dialed on a telephone keypad. Length: 1 to 5 characters. Default is #1.
Step 5	ringing-timeout <i>seconds</i> Example: Router(config-stcapp-callback)# ringing-timeout 45	(Optional) Defines the timeout period for ringing timer. <ul style="list-style-type: none"><i>seconds</i>— Range: 5 to 60. Default: 30.
Step 6	end Example: Router(config-stcapp-callback)# end	Exits STC application feature callback configuration mode and returns to privileged EXEC mode.

Configuration Examples for CallBack on Busy for Analog Phones on Cisco Voice Gateways

The following partial output from the **show stcapp feature codes** command shows the default values for the CallBack on Busy feature:

```
Router# show stcapp feature codes
```

```
.  
.
.
```

```
stcapp feature callback
  key #1
  timeout 30
```

The following example shows a configuration for CallBack on Busy on a Cisco voice gateway. In this configuration, the activation key and the timeout period for the ringing timer are modified from the defaults.

```
Router# show running-config

Building configuration...

Current configuration : 3442 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
.
.
.
!
stcapp ccm-group 1
stcapp
!
.
.
.
!
stcapp feature callback
  key *22
  timeout 45
!
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for CallBack on Busy for Analog Phones on Cisco Voice Gateways

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(20)YA or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 **Feature Information**

Feature Name	Releases	Feature Information
CallBack on Busy for Analog Phones	12.4(20)YA	<p>Provides callback notification when a busy called line becomes free. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 108. How to Configure CallBack on Busy for Analog Phones on Cisco Voice Gateways, page 110. <p>The following commands were introduced by this feature: stcapp feature callback, activation-key, ringing-timeout.</p>



Configuring CallBack on No Answer for Analog Phones

First Published: November 19, 2010

This module describes the CallBack on No Answer feature for analog phones that are connected to Foreign Exchange Station (FXS) ports on a Cisco VG2nn Analog Gateway or a Cisco Integrated Services Router (ISR). This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified Communications Manager (Cisco Unified CM) only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for CallBack on No Answer for Analog Phones](#)” section on [page 124](#).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for CallBack on No Answer for Analog Phones](#), page 116
- [Restrictions for CallBack on No Answer for Analog Phones](#), page 116
- [Benefits of Using CallBack on No Answer for Analog Phones](#), page 116
- [Information About CallBack on No Answer for Analog Phones](#), page 117
- [How to Configure CallBack on No Answer for Analog Phones](#), page 120
- [Configuration Examples for CallBack on No Answer for Analog Phones](#), page 122
- [Additional References](#), page 123
- [Feature Information for CallBack on No Answer for Analog Phones](#), page 124

Prerequisites for CallBack on No Answer for Analog Phones

Cisco IOS Gateway

- Cisco IOS Release 15.1(3)T or a later version.
- Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- Analog FXS voice ports are set up and configured for operation. For information, see the *Cisco IOS Voice Port Configuration Guide*.
- SCCP and the STCAPP are enabled on the Cisco voice gateway. For configuration information, see *Configuring FXS Ports for Basic Calls*.
- SCCP supplementary features are enabled on the Cisco voice gateway. See *Configuring Supplementary Features*.

Analog Endpoints in Cisco Unified CM

- Configure CallBack service parameters by accessing **System > Service Parameters** in Cisco Unified CM Administration; choose the server where the Cisco Unified CM service runs and then choose the Cisco Unified CM service. Unless instructed otherwise by the Cisco Technical Assistance Center, we recommend that you use the default service parameters settings. For information, see the “Call Back” section in the appropriate Cisco Unified CM Features and Services Guide at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

CallBack on No Answer for Analog Phones requires the following software components:

- Cisco Unified CM 8.5.
- Cisco Unified CM service running on at least one server in the cluster.
- Cisco Database Layer Monitor service running on the same server as the Cisco Unified CM service.
- Cisco real-time information server Data Collector service running on the same server as the Cisco Unified CM service.
- Cisco Unified CM Locale Installer, that is, if you want to use non-English phone locales or country-specific tones.
- Microsoft Internet Explorer or Netscape Navigator.

Restrictions for CallBack on No Answer for Analog Phones

- This feature is not supported in Cisco Unified CME.

Benefits of Using CallBack on No Answer for Analog Phones

The CallBack on No Answer feature provides parity with incumbent time-division multiplexing PBXs (remote endpoint can be behind a Public Switched Telephone Network gateway in specific cases).

Information About CallBack on No Answer for Analog Phones

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 117](#)
- [CallBack on No Answer for Analog Phones, page 118](#)

Feature Summary

Table 1 contains information about SCCP-based CallBack on No Answer for Analog Phones on Cisco Voice Gateways, along with information about how to configure support for this feature in your Cisco call-control system.

Table 1 *CallBack on No Answer for Analog Phones*

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>CallBack on No Answer for Analog Phones</p> <p>Allows phone user to initiate an audio alert on the phone when a party who does not answer becomes available.</p>	<p>After placing call to a phone that does not answer, user dials callback activation key to activate SCCP-based CallBack on No Answer feature. Default activation key sequence is #1.</p> <p>After CallBack on No Answer is activated, user hears a confirmation tone.</p> <p>The calling phone only supports one active CallBack request at a time. If a phone user tries to activate a second CallBack on No Answer while a callback is already active, the first callback is canceled and replaced by an active callback for the second no answer called number.</p> <p>Note The stcapp feature callback command must be enabled on the Cisco voice gateway.</p>	<p>Cisco Unified Communications Manager</p> <p>Configure Cisco Callback service parameters by accessing System> Service Parameters in Cisco Unified Communications Manager Administration; choose the server where the Cisco Unified Communications Manager service runs and then choose the Cisco Unified Communications Manager service.</p> <p>Unless instructed otherwise by the Cisco Technical Assistance Center, we recommend that you use the default service parameters settings. For information on these parameters, click the question mark button in the upper corner of the Service Parameter window.</p> <p>Cisco Unified CME</p> <p>This feature is not supported for analog endpoints in Cisco Unified CME.</p>

CallBack on No Answer for Analog Phones

When the analog FXS ports are enabled by the Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP), calls through the FXS endpoints are controlled by the Cisco Unified CM, with basic call support in Survivable Remote Site Telephony (SRST) mode. The STCAPP on the Cisco voice gateway functions as a proxy to translate call-control messages between the Cisco call-control system and the voice gateway.

The Cisco Unified CM monitors the called telephone when you activate the CallBack feature on an analog phone when the remote side is either not answering the phone or is busy. For more information, see the [“Configuring CallBack on Busy” section on page 107](#).

When the called telephone becomes available to receive a call, the Cisco Unified CM verifies that the calling phone is also available and if so, automatically activates the CallBack notification. The original calling phone generates a special CallBack ringtone. When the calling party lifts the handset, the called phone receives a call as a regular call from the calling party.



Note

Existing SCCP protocols for the CallBack feature are integrated with the IOS gateway and translated into analog phone tones and alert ringtones to support all phases of the CallBack scenario.

- In successful cases, the confirmation tone is used during CallBack activation. In cases where the Cisco Unified CM reports an error, a fast busy tone is played.
- If you activate the CallBack feature and go on-hook before the confirmation or error tones are played, you cannot determine whether the feature is activated successfully or not. If CallBack is activated, the scenario proceeds as usual and you hear the CallBack ringtone.

The following examples describe how CallBack on No Answer is supported on analog phones connected to IOS-based platforms, either on a call to another analog phone or to an IP phone:

- [Normal Operation, page 118](#)
- [CallBack not completed because Calling Party does not answer, page 119](#)
- [CallBack not completed because Called Party does not answer, page 119](#)
- [CallBack not completed because Calling Party receives another incoming call, page 119](#)



Note

In the succeeding scenarios, A and B are both analog telephones existing in the same Cisco Unified CM Cluster connected to the same or different Cisco VG2nn Analog Gateway or Cisco ISR router. Alternatively, B can be any Cisco IP Phone existing in the same Cisco Unified CM cluster or any off-net phone, connected to Cisco Unified CM using Q Signaling PRI trunk.

Normal Operation

User A calls user B, which does not answer (the phone rings).

User A hears ring back tone, then activates the CallBack feature by pressing #1 (configurable) and gets a confirmation tone from the system letting user A know that the feature has been activated. The system allows only one CallBack number to be activated at any time. If a CallBack to another destination is previously activated, it is automatically cancelled and replaced with the new destination.

User A is able to make calls to other users without affecting or cancelling the CallBack feature. The CallBack cannot be explicitly cancelled by the user.

When user B becomes available (by going on-hook), system checks if user A is also on-hook. If A is busy on another call, the system waits until both users A and B are available to establish CallBack call.

When both A and B are available (on-hook), user A receives the CallBack notification ringtone.

When user A lifts the handset he hears the CallBack ringtone and user B's phone rings normally.

CallBack not completed because Calling Party does not answer

User A calls user B, which does not answer (the phone rings).

User A hears ring back tone, then activates the CallBack feature by pressing #1 (configurable) and gets a confirmation tone from the system letting user A know that the feature has been activated. The system allows only one CallBack number to be activated at any time. If a CallBack to another destination is previously activated, it is automatically cancelled and replaced with the new destination.

User A is able to make calls to other users without affecting or cancelling the CallBack feature. The CallBack cannot be explicitly cancelled by the user.

When user B becomes available (by going on-hook), system checks if user A is also on-hook. If A is busy on another call, the system waits until both users A and B are available to establish CallBack call.

When both A and B are available (on-hook), user A receives a CallBack ringtone but does not answer.

The system keeps sending a CallBack ringtone to user A until the defined "ringing-timeout" set on the Cisco VG2nn Analog Gateway or Cisco ISR router is reached, if user A still does not answer, CallBack feature gets cancelled.

No further attempts to complete the call are made and there is NO notification to users about cancellation of the CallBack feature.

CallBack not completed because Called Party does not answer

User A calls user B, which does not answer (the phone rings).

User A hears ring back tone, then activates the CallBack feature by pressing #1 (configurable) and gets a confirmation tone from the system letting user A know that the feature has been activated. The system allows only one CallBack number to be activated at any time. If a CallBack to another destination is previously activated, it is automatically cancelled and replaced with the new destination.

User A is able to make calls to other users without affecting or cancelling the CallBack feature. The CallBack cannot be explicitly cancelled by the user.

When user B becomes available (by going on-hook), system checks if user A is also on-hook. If A is busy on another call, the system waits until both users A and B are available to establish CallBack call.

When both A and B are available (on-hook), user A receives the CallBack notification ringtone.

When user A lifts the handset he hears the CallBack ringtone and user B's phone rings normally.

User B does not answer, the system keeps ringing B until the "No Answer Ring Duration" time (set in CUCM) is reached. If user B still does not answer, the CallBack feature gets cancelled.

No further attempts to complete the call are made and there is NO notification to users about cancellation of the CallBack feature.

CallBack not completed because Calling Party receives another incoming call

User A calls user B, which does not answer (the phone rings).

User A hears ring back tone, then activates the CallBack feature by pressing #1 (configurable) and gets a confirmation tone from the system letting user A know that the feature has been activated. The system allows only one CallBack number to be activated at any time. If a CallBack to another destination is previously activated, it is automatically cancelled and replaced with the new destination.

User A is able to make calls to other users without affecting or cancelling the CallBack feature. The CallBack cannot be explicitly cancelled by the user.

When user B becomes available (by going on-hook), system checks if user A is also on-hook. If A is busy on another call, the system waits until both users A and B are available to establish CallBack call.

When both A and B are available (on-hook), user A receives the CallBack notification ringtone.

While user A hears CallBack ringtone, another incoming call comes in to A.

CallBack gets immediately cancelled and the ring pattern changes to normal.

When user A picks up the handset, the call is answered like a normal incoming call.

**Note**

CallBack on No Answer requires additional effort in the activation phase since the activation happens at different call states.

In the case where call progress tones (busy or ringback) are coming in-band, possibly with some third party PBXs interconnected through Q Signaling trunks, the call goes to the “active” state, the media flows to the gateway, and the tones are delivered as part of media. In this case, CallBack is activate and works like a normal incoming call.

How to Configure CallBack on No Answer for Analog Phones

CallBack on No Answer automatically installs when you install Cisco Unified CM.

The “[Configuring CallBack on No Answer for Analog Phones](#)” section on page 120 provides detailed configuration information

Configuring CallBack on No Answer for Analog Phones

**Note**

This document does not contain details about configuring Cisco Unified CM. See the documentation for this product for installation and configuration instructions.

To modify the default values of the CallBack activation key sequence or ringing timer for CallBack on No Answer on analog phones on IOS-based platforms, perform the following steps on the Cisco voice gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp feature callback**
4. **activation-key *string***
5. **ringing-timeout *seconds***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp feature callback Example: Router(config)# stcapp feature callback	Enables CallBack on No Answer and enters STCAPP feature CallBack configuration mode.
Step 4	activation-key <i>string</i> Example: Router(config-stcapp-callback)# activation-key *4	(Optional) Defines the key sequence to use for activating CallBack on No Answer. <ul style="list-style-type: none"><i>string</i>—String (0-9, # *) that can be dialed on a telephone keypad. Length: 1 to 5 characters. Default is #1.
Step 5	ringing-timeout <i>seconds</i> Example: Router(config-stcapp-callback)# ringing-timeout 45	(Optional) Defines the timeout period for ringing timer. <ul style="list-style-type: none"><i>seconds</i>—Range: 5 to 60. Default: 30,
Step 6	end Example: Router(config-stcapp-callback)# end	Exits STCAPP feature CallBack configuration mode and returns to privileged EXEC mode.

Configuration Examples for CallBack on No Answer for Analog Phones

This section provides the following configuration examples:

- [Example: Configuring Feature Callback in the STCAPP on a Cisco IOS Gateway, page 122](#)
- [Example: Configuring CallBack on No Answer on a Cisco IOS Gateway, page 122](#)

Example: Configuring Feature Callback in the STCAPP on a Cisco IOS Gateway

The following example shows a partial output of feature callback in the STCAPP on a Cisco IOS gateway with the key sequence for activating CallBack on No Answer defined as 1000 and the timeout period for the ringing timer defined as 10:

```
Router# show run all
.
.
.
stcapp feature callback
  activation-key #1000
  ringing-timeout 10
```

Example: Configuring CallBack on No Answer on a Cisco IOS Gateway

The following example shows how to configure CallBack on No Answer on a Cisco IOS gateway. In this configuration, the activation key and the timeout period for the ringing timer are modified from the defaults.

```
Building configuration...
Current configuration : 3442 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
.
.
.
!
stcapp ccm-group 1
stcapp
!
.
.
.
!
stcapp feature callback
  activation-key *22
  ringing-timeout 45
!
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for CallBack on No Answer for Analog Phones

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for CallBack on No Answer for Analog Phones

Feature Name	Releases	Feature Information
CallBack on No Answer for Analog Phones	15.1(3)T	<p>Provides CallBack notification when a called phone becomes available. This feature is supported on analog SCCP endpoints in Cisco Unified CM only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About CallBack on No Answer for Analog Phones, page 117 Configuring CallBack on No Answer for Analog Phones, page 120. <p>No new commands were introduced by this feature.</p>



Configuring Call Waiting Tone Cadence

First Published: November 19, 2010

This module describes the Configurable Call Waiting Tone Cadence feature, a Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) supplementary-service feature supported on an analog Foreign Exchange Station (FXS) voice port. This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified Communications Manager (Cisco Unified CM) only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Configurable Call Waiting Tone Cadence](#)” section on page 131.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Configurable Call Waiting Tone Cadence, page 126](#)
- [Benefits of Configurable Call Waiting Tone Cadence, page 126](#)
- [Information About Configurable Call Waiting Tone Cadence, page 126](#)
- [How to Configure Call Waiting Tone Cadence, page 126](#)
- [Configuration Examples for Configurable Call Waiting Tone Cadence, page 128](#)

- [Additional References, page 130](#)
- [Feature Information for Configurable Call Waiting Tone Cadence, page 131](#)

Restrictions for Configurable Call Waiting Tone Cadence

- This feature is not supported in Cisco Unified CME.

Benefits of Configurable Call Waiting Tone Cadence

The Configurable Call Waiting Tone Cadence feature provides parity with incumbent time-division multiplexing switches.

It also provides backward compatibility, with the single-beep tone as default behavior, as long the existing configuration is not modified.

Information About Configurable Call Waiting Tone Cadence

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Configurable Call Waiting Tone Cadence, page 126](#)

Configurable Call Waiting Tone Cadence

For analog endpoints in Cisco Unified CM, the Configurable Call Waiting Tone Cadence enables the call waiting tone to be configured as a distinct ringtone played continuously on Cisco IOS SCCP voice gateways until the called party switches from the active call to an incoming call and the new caller has not hung up.

A configurable CLI allows you to choose the ring cadence to use for the call waiting tone.

If it is configured, the ringtone will periodically repeat with configured interval until either the user switches to the new call or the calling party hangs up.

The IOS managed timer is utilized to provide this functionality. A separate timer is used for each port but it is activated only when the call waiting tone is being played.

The value of 0 (the default for compatibility reasons) means that no repetition should occur.

The offhook caller ID is displayed only once if the repetitive call waiting tone is configured.

How to Configure Call Waiting Tone Cadence

The “[Configuring Call Waiting Tone Cadence](#)” section on [page 127](#) provides detailed configuration information.

Configuring Call Waiting Tone Cadence



Note

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To modify the default values of the repetition interval for Call Waiting Tone Cadence for analog endpoints in the Cisco Unified CM, perform the following steps on the Cisco voice gateway:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp supplementary-services**
4. **port** *port-number*
5. **cptone call-waiting repetition interval** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp supplementary-services Example: Router(config)# stcapp supplementary-services	Enters supplementary-service configuration mode.
Step 4	port <i>port-number</i> Example: Router(config-stcapp-supp)# port 2/0	Specifies analog FXS voice port on which STC application supplementary-service features are to be supported. <ul style="list-style-type: none"> • <i>port-number</i>—Voice port number. Range is 2/0 to 2/23.

	Command or Action	Purpose
Step 5	cptone call-waiting repetition interval <i>seconds</i> Example: Router(config-stcapp-supp-port)# cptone call-waiting repetition interval 20	Defines the interval for tone repetition. <ul style="list-style-type: none"> <i>seconds</i>—Range: 0 to 30. Default: 0. Note The default ringtone is a single-beep tone.
Step 6	end Example: Router(config-stcapp-supp-port)# end	Exits STC application supplementary-service configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configurable Call Waiting Tone Cadence

This section provides the following configuration example:

- [Example: Configurable Call Waiting Tone Cadence on a Cisco IOS Gateway, page 128](#)
- [Example: Configurable Call Waiting Tone Cadence on a Cisco VG204, page 128](#)

Example: Configurable Call Waiting Tone Cadence on a Cisco IOS Gateway

The following is a sample output from the **show run** command showing how to enable the Configurable Call Waiting Tone Cadence STCAPP supplementary-service feature for analog phones connected to port 2/4 on a Cisco VG224. A similar sample output can also be displayed using the **show stcapp device voice-port x/x** (or **x/x/x**) command.

```
Router(config)# show run
.
.
.
stcapp supplementary-services
port 2/0
cptone call-waiting repetition interval 20
end
```

Example: Configurable Call Waiting Tone Cadence on a Cisco VG204

The following is a sample output from the **show stcapp device** command showing you how to verify the configured call waiting tone cadence (repetition interval) on port 0/0 of a Cisco VG204:

```
Router(config)# show stcapp device voice-port 0/0

Port Identifier: 0/0
Device Type:    ALG
Device Id:      1
Device Name:    AN1FCAC3B790000
Device Security Mode : None
Modem Capability: None
Device State:   IS
Diagnostic:     None
Directory Number: 9886087490
```

```
Dial Peer(s):      87486
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:            OFF
mwi config:       Both
Privacy:          Not configured
PLAR:            DISABLE
Callback State:   IDLE
CWT Repetition Interval: 3 second(s)
Number of CCBs:   0
Global call info:
  Total CCB count      = 1
  Total call leg count = 1
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	<i>Cisco Unified Communications Manager</i>
Cisco Unified Communications Manager Express	<i>Cisco Unified Communications Manager Express</i>
Cisco IOS debugging	<i>Cisco IOS Debug Command Reference</i>
Cisco IOS voice commands	<i>Cisco IOS Voice Command Reference</i>
Cisco IOS voice configuration	<i>Cisco IOS Voice Configuration Library</i>
Cisco voice gateway	<ul style="list-style-type: none"> • <i>Cisco VG200 Series Gateway</i> • <i>Cisco 1800 Series Integrated Services Routers</i> • <i>Cisco 2800 Series Integrated Services Routers</i> • <i>Cisco 3800 Series Integrated services Routers</i> • <i>Cisco Unified 500 Series</i>
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the <i>Cisco Unified CallManager and Cisco IOS Interoperability Guide</i>. • <i>Cisco CallManager and IOS Gateway DSP Farm Configuration Example</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Configurable Call Waiting Tone Cadence

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Configurable Call Waiting Tone Cadence

Feature Name	Releases	Feature Information
Configurable Call Waiting Tone Cadence	15.1(3)T	<p>Allows the call waiting tone to continuously play when the called party has not switched to the new call and the new caller has not hung up. This feature is supported in Cisco Unified CM only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About Configurable Call Waiting Tone Cadence, page 126 Configuring Call Waiting Tone Cadence, page 127 <p>The following commands were introduced or modified: cptone call-waiting repetition interval, show stcapp device.</p>



Configuring AMWI and VMWI

First Published: November 19, 2010

This module describes the configurable audible message waiting indication/visible message waiting indication (AMWI/VMWI) feature for Skinny Client Control Protocol (SCCP)-controlled Analog Ports. This feature provides users with the option to enable one message waiting indication (MWI): audible, visible, or both.

This feature is supported for analog endpoints that are connected to Foreign Exchange Station (FXS) ports or a Cisco VG224 Analog Phone Gateway and controlled by a Cisco call-control system, such as a Cisco Unified Communications Manager (Cisco Unified CM) or a Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configurable AMWI and VMWI”](#) section on page 142.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configurable AMWI and VMWI, page 134](#)
- [Information About Configurable AMWI and VMWI, page 134](#)
- [How to Configure AMWI and VMWI, page 135](#)
- [Configuration Examples for Configurable AMWI and VMWI, page 136](#)
- [Additional References, page 141](#)
- [Feature Information for Configurable AMWI and VMWI, page 142](#)

Prerequisites for Configurable AMWI and VMWI

Cisco IOS Gateway

- Cisco IOS Release 15.1(3)T or a later version.
- The Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- SCCP and the SCCP telephony control (STC) application are enabled on the Cisco voice gateway. For configuration information, see [“Configuring FXS Ports for Basic Calls”](#).
- SCCP supplementary features are enabled on the Cisco voice gateway. See [“Configuring Supplementary Features”](#).

Information About Configurable AMWI and VMWI

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 134](#)
- [Configurable AMWI and VMWI, page 134](#)

Feature Summary

[Table 1](#) contains information about SCCP-based Configurable AMWI and VMWI on Cisco Voice Gateways.

Table 1 *Configurable AMWI and VMWI*

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
Configurable AMWI and VMWI Allows users to configure AMWI only, VMWI only, or both.	When a voicemail is available, the user goes offhook to hear a special AMWI tone or goes onhook to see an MWI light (when the phone is equipped with one).	No configuration tasks required on your Cisco call-control system.

Configurable AMWI and VMWI

MWI is used to remind you that there is a voicemail message waiting. When a voicemail is available, the phone receives AMWI, which plays a special AMWI tone when you go offhook. A VMWI, which turns on an MWI light, is also activated when the phone is equipped with one. No configuration tasks are required to enable MWI feature for analog phones because it plays both AMWI and VMWI by default. However, you can configure your phone to have VMWI or AMWI only.

When configuring MWI, you need to make sure that there are no existing voicemail messages. Configuring MWI while the phone still has voicemail messages is not supported by this feature. You need to clear all voicemail messages and make sure VMWI/AMWI is not active before configuring the MWI setting.

The two types of VMWI, the frequency-shift keying message and DC voltage, are both supported by this feature.

How to Configure AMWI and VMWI

**Note**

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To enable any of the MWI options, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp supplementary-services**
4. **port** *port-number*
5. **mwi** { **audible** | **visible** | **both** }
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>stcapp supplementary-services</code> Example: Router(config)# stcapp supplementary-services	Enters supplementary-service configuration mode.
Step 4	<code>port port-number</code> Example: Router(config-stcapp-suppl-serv)#port 2/2	Specifies analog FXS voice port on which STCAPP supplementary-service features are to be supported. <ul style="list-style-type: none">• <i>port-number</i>—Voice port number. Range is 2/0 to 2/23.
Step 5	<code>mwi {audible visible both}</code> Example: Router(config-stcapp-suppl-serv-port)#mwi audible	Enables mwi as audible only (AMWI), visible only (VMWI), or both (default configuration). <ul style="list-style-type: none">• audible—AMWI is enabled.• visible—VMWI is enabled.• both—Default configuration. Both AMWI and VMWI are enabled. Note The current configuration is that MWI (AMWI/VMWI) is automatically turned on when the port is configured in SCCP, MWI cannot be turned off in SCCP.
Step 6	<code>end</code> Example: Router(config-stcapp-suppl-serv-port)#end	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configurable AMWI and VMWI

This section provides the following configuration examples:

- [Example: Configuring AMWI and VMWI, page 137](#)
- [Example: How to Check the Current MWI Configuration, page 139](#)

Example: Configuring AMWI and VMWI

The following example shows how to configure AMWI and VMWI on specific analog FXS voice ports on which STCAPP supplementary-service features are supported:

```
Router# show running-config
Building configuration...

Current configuration : 5518 bytes
!
! Last configuration change at 17:02:32 PST Sun Feb 28 1993
!
version 15.1
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
logging buffered 20000000
!
no aaa new-model
clock timezone PST -7 0
ip source-route
ip cef
no ipv6 cef
!
stcapp ccm-group 20
stcapp
!
!
stcapp supplementary-services
  port 2/1
    fallback-dn 3001
  port 2/2
    fallback-dn 3102
    mwi visible
  port 2/3
    fallback-dn 3203
    mwi audible
!
!
voice-card 0
!
archive
  log config
  hidekeys
!
!
!
!
!
interface FastEthernet0/0
  ip address 1.5.42.80 255.255.255.0
  duplex auto
  speed auto
!
```

```
interface FastEthernet0/1
 ip address 1.4.197.150 255.255.255.0
 ip access-group 3 in
 duplex auto
 speed auto
 !
 ip default-gateway 1.5.0.1
 !
 ip forward-protocol nd
 ip http server
 ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
 !
 !
 !
 control-plane
 !
 !
 voice-port 2/0
 !
 voice-port 2/1
  timeouts ringing infinity
  station-id number 3001
  caller-id enable
 !
 voice-port 2/2
  vmwi dc-voltage
  timeouts ringing infinity
  station-id number 3102
  caller-id enable
 !
 voice-port 2/3
  timeouts ringing infinity
  station-id number 3203
  caller-id enable
 !
 voice-port 2/4
 !
 voice-port 2/5
 !
 voice-port 2/6
 !
 voice-port 2/7
 !
 voice-port 2/8
 !
 voice-port 2/9
 !
 voice-port 2/10
 !
 voice-port 2/11
 !
 voice-port 2/12
 !
 voice-port 2/13
 !
 voice-port 2/14
 !
 voice-port 2/15
 !
 voice-port 2/16
 !
 voice-port 2/17
 !
 voice-port 2/18
```

```

!
voice-port 2/19
!
voice-port 2/20
!
voice-port 2/21
!
voice-port 2/22
!
voice-port 2/23
!
!
mgcp fax t38 ecm
!
sccp local FastEthernet0/0
sccp ccm 1.5.42.40 identifier 40 version 6.0
sccp
!
!
sccp ccm group 20
  associate ccm 40 priority 1
!
dial-peer voice 21 pots
  service stcapp
  port 2/1
!
dial-peer voice 22 pots
  service stcapp
  port 2/2
!
dial-peer voice 23 pots
  service stcapp
  port 2/3
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  login
  transport input all
!
exception data-corruption buffer truncate
end

Router#

```

Example: How to Check the Current MWI Configuration

Users can use the **show** command to check the current MWI configuration.

```

Router# show stcapp device voice-port 2/2
Port Identifier: 2/2
Device Type:    ALG
Device Id:      1
Device Name:    AN0C863949F6402
Device Security Mode : None
Modem Capability: None
Device State:   IS
Diagnostic:     None
Directory Number: 3102
Dial Peer(s):  12

```

```
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:          STCAPP_DC_EV_DEVICE_SET_LAMP_PROCESS_DC_VMWI
Line State:          IDLE
Line Mode:           CALL_BASIC
Hook State:          ONHOOK
mwi:                 DISABLE
vmwi:                OFF
mwi config:          Visible
Privacy:             Not configured
PLAR:                DISABLE
Callback State:      DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:      0
Global call info:
  Total CCB count      = 0
  Total call leg count = 0
Router#
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated Services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Configurable AMWI and VMWI

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Configurable AMWI and VMWI

Feature Name	Releases	Feature Information
Configurable AMWI and VMWI	15.1(3)T	<p>Allows users to configure AMWI only, VMWI only, or both.</p> <p>MWI is used to remind the user that there is a voicemail message waiting. When a voicemail is available, the phone receives an AMWI that plays a special AMWI tone when the user goes offhook or a VMWI that turns on an MWI light (when the phone is equipped with one) when the user goes onhook.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About Configurable AMWI and VMWI, page 134 How to Configure AMWI and VMWI, page 135 <p>The following commands were introduced or modified: mwi (supplementary-service).</p>



Configuring DC Voltage Based VMWI for SCCP Controlled Analog Ports

First Published: August 1, 2008
Last Updated: March 19, 2010

This module describes the DC Voltage Based VMWI for SCCP Controlled Analog Ports feature. This feature is supported for analog endpoints that are connected to Foreign Exchange Station (FXS) ports on a Cisco VG224 Analog Phone Gateway with analog device version V1.2 or V3.1 and controlled by a Cisco call-control system such as Cisco Unified Communications Manager or Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for DC Voltage Based VMWI for SCCP Controlled Analog Ports](#)” section on page 149.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About DC Voltage Based VMWI for SCCP Controlled Analog Ports](#), page 144
- [How to Configure DC Voltage Based VMWI for SCCP Controlled Analog Ports](#), page 146
- [Additional References](#), page 148
- [Feature Information for DC Voltage Based VMWI for SCCP Controlled Analog Ports](#), page 149

Information About DC Voltage Based VMWI for SCCP Controlled Analog Ports

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 144](#)
- [VMWI for SCCP FXS Ports in Cisco IOS Software, page 145](#)
- [DC Voltage VMWI, page 145](#)

Feature Summary

[Table 1](#) contains information about the DC Voltage Based VMWI for SCCP Controlled Analog Ports feature, along with information about how to configure support for this feature in your Cisco call-control system.

Table 1 DC Voltage Based VMWI for SCCP Controlled Analog Ports

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>VMWI for SCCP Controlled VG224 Analog Ports</p> <p>Allows the phone user to see if there are new voice messages by looking at the message waiting lamp.</p>	<p>If the phone is on hook, the MWI lamp turns on when a new message is received. The lamp turns off after the user has reviewed all messages. If the phone is off hook, the MWI lamp is turned on or off the next time the phone goes on hook.</p>	<p>No configuration tasks required on your Cisco call-control system.</p>
<p>DC Voltage Based VMWI for SCCP Controlled Analog Ports</p> <p>Allows the phone user to see if there are new voice messages by looking at the message waiting lamp on certain analog phones that support a DC-voltage-controlled message waiting lamp.</p>	<p>When the voice port is in an idle and onhook state, the MWI lamp flashes with a 600 ms on and 1200 ms off cadence to indicate that there are waiting voice messages.</p> <p>When the voice port is not in an idle state or if the port is off hook or ringing, the MWI lamp is turned off.</p> <p>After the operation state of this voice port returns to idle and onhook, the MWI lamp resumes flashing.</p> <p>Note This feature is only supported for SCCP endpoints connected to onboard analog FXS ports on a Cisco VG224 with analog device version V1.3 or V2.1. It is not supported on analog FXS ports on a Cisco ISR.</p>	<p>No configuration tasks required on your Cisco call-control system.</p>

VMWI for SCCP FXS Ports in Cisco IOS Software

This feature provides visual message waiting indication (VMWI) capability on analog FXS ports connected to Cisco voice gateways.

The VMWI on SCCP controlled analog phones feature works with the voice-mail system to send message waiting notification to the user. The SCCP gateway provides VMWI light activation using frequency shift keying (FSK) messaging that is supported on the analog phone with a 24- to 48-volt lamp. If the phone is on hook, the VMWI lamp light turns on when a new message is received. The light turns off after the user has reviewed all messages. If the phone is off hook, the VMWI light is turned on or off the next time the phone goes on hook.

The VMWI feature for analog phones also supports shared-line VMWI in Cisco Unified Communications Manager 4.2 and later versions and Cisco Unified CME 4.0 and later versions. The VMWI LED is turned on or off only when all phones are on hook. Overlay VMWI is supported in Cisco Unified CME, with the VMWI signaled on the first ephone-dn (directory number).

No configuration is required on the SCCP analog gateway to enable this feature.

DC Voltage VMWI

The DC Voltage VMWI feature is used to flash the message-waiting lamp on an analog phone which requires DC voltage instead of an FSK message. DC voltage VMWI is supported for the SCCP telephony control (STC) application only. For all other applications, such as MGCP, FSK VMWI will be used even if the voice gateway is configured for DC voltage VMWI. The configuration for DC voltage VMWI is supported only for FXS ports on the Cisco VG224 analog voice gateway with analog device version V1.3 and V2.1.

The Cisco VG224 can only support 12 REN for ringing 24 onboard analog FXS voice ports. In order to support ringing and DC Voltage VMWI for 24 analog voice ports, stagger-ringing logic is used to maximize the limited REN resource. When a system runs out of REN because too many voice ports are being rung, the MWI lamp temporarily turns off to free up REN to ring the voice ports.

DC voltage VMWI is also temporarily turned off any time the port's operational state is no longer idle and onhook, such as when one of the following events occur:

- Incoming call on voice port
- Phone goes off hook
- Voice port is shut down or busied out

Once the operational state of the port changes to idle and onhook again, the MWI lamp resumes flashing until the application receives a requests to clear it; for example, if there are no more waiting messages.

For configuration information, see the [“How to Configure DC Voltage Based VMWI for SCCP Controlled Analog Ports”](#) section on page 146.

How to Configure DC Voltage Based VMWI for SCCP Controlled Analog Ports

**Note**

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To enable DC voltage VMWI on a Cisco VG224 onboard analog FXS voice port, perform the following steps.

Prerequisites for DC Voltage Based VMWI for SCCP Controlled Analog Ports

Cisco IOS Gateway

- Cisco IOS Release 12.4(20)YA or a later version.
- Cisco VG224 Analog Phone Gateway with analog device version V1.3 or V2.1.
- The Cisco voice gateway must be set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- SCCP and the SCCP telephony control (STC) application are enabled on the Cisco voice gateway. For configuration information, see the [“Configuring FXS Ports for Basic Calls”](#) section on page 17.
- SCCP supplementary features are enabled on the Cisco voice gateway. See the [“Configuring Supplementary Features”](#) section on page 55.

Restrictions for DC Voltage Based VMWI for SCCP Controlled Analog Ports

- DC voltage VMWI configuration is supported for the SCCP telephony control (STC) application only. For all other applications, such as MGCP, FSK VMWI is used regardless of the DC voltage VMWI configuration.
- DC voltage VMWI is supported only on Cisco VG224 onboard analog FXS ports with loop start signaling type. This feature is not supported on analog FXS ports with ground start.
- DC voltage VMWI is not supported on analog FXS ports on a Cisco integrated service router (ISR) or on a Cisco Unified 500 series platform.
- DC voltage VMWI is not supported on analog phones with neon bulbs.
- DC voltage VMWI is not supported on analog phones that support FSK VMWI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port*
4. **vmwi dc-voltage**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-port port Example: Router(config)# voice-port 2/0	Enters voice-port configuration mode. <ul style="list-style-type: none"><i>port</i>—Syntax is platform-dependent. Type ? to determine.
Step 4	vmwi dc-voltage Example: Router(config-voiceport)# vmwi dc-voltage	Enables DC voltage VMWI on the port being configured.
Step 5	end Example: Router(config-voiceport)# end	Exits voice-port configuration mode and returns to privileged EXEC mode.

Configuration Examples for DC Voltage Based VMWI for SCCP Controlled Analog Ports

This section contains the following example:

- [Example: VMWI for SCCP FXS Ports in Cisco IOS Features, page 147](#)

Example: VMWI for SCCP FXS Ports in Cisco IOS Features

The following example shows VMWI activated on Cisco VG224 port 2/4:

```
Router# show stcapp device voice-port 2/4

Port Identifier: 2/4
Device Type:    ALG
Device Id:     4
Device Name:   AN0C863967C9404
Modem Capability: None
Device State:  IS
Diagnostic:    None
Directory Number: 7204
Dial Peer(s): 4
Dialtone after remote onhook feature: activated
Last Event:    STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:    IDLE
```

Additional References

```

Hook State:      ONHOOK
mwi:            ENABLE
vmwi:          ON
PLAR:          DISABLE
Number of CCBs: 0
!
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for DC Voltage Based VMWI for SCCP Controlled Analog Ports

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(20)YA or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a command, see the command reference documentation. For information about these commands, see the *Cisco IOS Voice Command Reference* at

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases* at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information

Feature Name	Releases	Feature Information
DC Voltage Based VMWI for SCCP Controlled Analog Ports	12.4(20)YA	<p>Allows the phone user to see if there are new voice messages by looking at the message waiting lamp on certain analog phones that support a DC voltage-controlled MWI lamp.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About DC Voltage Based VMWI for SCCP Controlled Analog Ports, page 144 • How to Configure DC Voltage Based VMWI for SCCP Controlled Analog Ports, page 146. <p>The following command was introduced: vmwi dc-voltage.</p>



Configuring Call Hold/Resume for Shared Lines

First Published: August 1, 2008

Last Updated: March 19, 2010

This chapter describes the Call Hold/Resume for Shared Lines for SCCP Analog Ports feature for analog phones that are connected to Foreign Exchange Station (FXS) ports on a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway. This feature is supported for analog endpoints that are controlled by Cisco Unified Communications Manager only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Call Hold/Resume for Shared Lines for SCCP Analog Ports](#)” section on page 157.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 152
- [Restrictions for Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 152
- [Information About Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 152
- [How to Configure Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 154
- [Configuration Examples for Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 155
- [Additional References](#), page 156
- [Feature Information for Call Hold/Resume for Shared Lines for SCCP Analog Ports](#), page 157

Prerequisites for Call Hold/Resume for Shared Lines for SCCP Analog Ports

Cisco IOS Gateway

- Cisco IOS Release 12.4(20)YA or a later release.
- The Cisco voice gateway must be set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the [Cisco IOS Voice Port Configuration Guide](#).
- SCCP and the SCCP telephony control (STC) application is enabled on the Cisco voice gateway. For configuration information, see the [“Configuring FXS Ports for Basic Calls” section on page 17](#).
- SCCP supplementary features are enabled on the Cisco voice gateway. See the [“Configuring Supplementary Features” section on page 55](#).

Restrictions for Call Hold/Resume for Shared Lines for SCCP Analog Ports

- This feature is not supported for analog SCCP endpoints in Cisco Unified Communications Manager Express (Cisco Unified CME).
- This feature is not supported for FXS ports on a Cisco Unified 500 Series platform.
- If Call Hold/Resume for Shared Lines is configured and a call is connected, the analog phone user must press a second hookflash to get a feature tone and then dial a Feature Access Code (FAC) to invoke call transfer, call waiting, or call conference features.

Information About Call Hold/Resume for Shared Lines for SCCP Analog Ports

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 153](#)
- [Call Hold/Resume for Shared Lines for SCCP Analog Ports, page 153](#)

Feature Summary

[Table 1](#) contains information about the Call Hold/Resume for Shared Lines for SCCP Analog Ports feature, along with information about how to configure support this feature in your Cisco call-control system.

Table 1 *Call Hold/Resume for Shared Lines for SCCP Analog Ports*

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>Call Hold/Resume for Shared Lines for SCCP Analog Ports</p> <p>Enables user on an analog SCCP phone that shares a line with an IP phone to hold and resume an active call by pressing hookflash.</p>	<p>During an active call, an analog phone user on a shared line presses hookflash to place an active call on hold. The analog phone user hears a dial tone and can place a call, go on-hook, or press hookflash again to resume the call.</p> <p>The held call can be resumed by any phone on the shared line as follows:</p> <ul style="list-style-type: none"> Any analog phone on the shared line goes off-hook. Any IP phone on the shared line goes off-hook and the user presses Resume. <p>Note This feature is configured at a port-level.</p>	<p>Cisco Unified Communications Manager</p> <p>For feature information, see the “Making and Receiving Multiple Calls Per Directory Number” section of the “Understanding Directory Numbers” chapter under “Dial Plan Architecture” in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>This feature is enabled in Cisco Unified Communications Manager by default. No feature-specific configuration is required to support Hold/Resume on Shared Lines.</p> <p>Cisco Unified CME</p> <p>This feature is not supported for analog endpoints in Cisco Unified CME.</p>

Call Hold/Resume for Shared Lines for SCCP Analog Ports

Call Hold/Resume for SCCP analog ports that share a directory number with one or more other phones in Cisco Unified Communications Manager is supported in Cisco IOS Release 12.4(20)YA and later releases. This feature is supported only on analog SCCP phones connected to FXS ports on which Hold/Resume is configured.

During an active call, an analog phone user on a shared line presses hookflash to place the call on hold to answer an incoming call or to access a dialtone if a line is available. To resume the held call, the analog phone user presses hookflash a second time. To resume the held call on another phone on the shared line, any analog phone on the shared line goes off-hook or any IP phone on the shared line goes off-hook and the user presses Resume.

This feature also allows the analog phone user to place a new call while the shared line is in use. The new call is restricted to basic calling; supplementary services is not supported for the new call from an analog SCCP phone on an in-use shared line.

The default maximum number of calls supported on analog phones on a shared line is two. When an analog phone on a shared line is off-hook, it is in an active-call state. If two analog phones on a shared line are off-hook, other analog phones on the shared line cannot access a dialtone nor receive incoming calls. If an analog phone user presses hookflash while the shared line is in-use by two analog phones, the user hears a fast busy tone. Number of calls on analog phones and on IP phones on the same shared line are counted separately and the maximum-number configuration on one does not affect the other.

To configure Hold/Resume for Shared Lines, see the [“How to Configure Call Hold/Resume for Shared Lines for SCCP Analog Ports”](#) section on page 154.

How to Configure Call Hold/Resume for Shared Lines for SCCP Analog Ports



Note

This module does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To enable Call Hold/Resume for Shared Lines for analog SCCP endpoints connected to an analog FXS port on a Cisco voice gateway, perform the following steps for each port to be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp supplementary-services**
4. **port** *port*
5. **hold-resume**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp supplementary-services Example: Router(config)# stcapp supplementary-services	Creates a supplementary-service configuration mode for configuring STC application supplementary-service features on analog FXS ports. Note Removing the supplementary-service configuration permanently removes all port-specific subordinate STC application supplementary-service feature configurations.
Step 4	port <i>port</i> Example: Router(config-stcapp-suppl-serv)# port 2/0	Enters supplementary-service voice-port configuration mode for associating a STC application supplementary-service feature to a specific analog FXS port. <ul style="list-style-type: none"> • <i>port</i>—Syntax is platform-dependent. Type ? to determine.

	Command or Action	Purpose
Step 5	hold-resume Example: Router(config-stcapp-suppl-serv-port)# hold-resume	Enables Call Hold/Resume feature on port being configured.
Step 6	end Example: Router(config-stcapp-suppl-serv-port)# end	Exits supplementary-service voice-port configuration mode and returns to privileged EXEC mode.

Configuration Examples for Call Hold/Resume for Shared Lines for SCCP Analog Ports

The following partial output from the **show running-config** command shows a configuration for Call Hold/Resume for Shared Lines for SCCP Analog Ports:

```
Router# show running-config

Building configuration...

Current configuration : 3442 bytes
!
.
.
.
!
stcapp ccm-group 1
stcapp
!
!
stcapp feature access-code
prefix ##
call forward all *74
call forward cancel 9
!
stcapp feature speed-dial
prefix ##
redial 78*
voicemail 8
speed dial from 3 to 7
!
stcapp feature callback
code *22
timeout 45
!
!
stcapp supplementary-services
port 2/0
hold-resume
port 2/1
hold-resume
port 2/2
hold-resume
port 2/3
hold-resume
```

```

port 2/4
  hold-resume
port 2/5
  hold-resume
port 2/6
  hold-resume
!
stcapp call-control mode feature
!
.
.
.
end

```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager documentation
Cisco Unified Communications Manager Express	Cisco Unified CME documentation
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers documentation • Cisco 2800 Integrated Services Routers documentation • Cisco 3800 Series Integrated services Routers documentation • Cisco Unified 500 Series documentation
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Call Hold/Resume for Shared Lines for SCCP Analog Ports

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(20)YA or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information

Feature Name	Releases	Feature Information
Call Hold/Resume for Shared Lines for SCCP Analog Ports	12.4(20)YA	<p>Enables an analog phone on a shared line to use hookflash to hold and resume an active call. This feature is supported on analog SCCP endpoints in Cisco Unified Communications Manager only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Call Hold/Resume for Shared Lines for SCCP Analog Ports, page 153 • How to Configure Call Hold/Resume for Shared Lines for SCCP Analog Ports, page 154 <p>The following commands were introduced by this feature: hold-resume, port (supplementary-service), stcapp supplementary-services.</p>



Configuring cBarge and Privacy for Shared Lines

First Published: November 19, 2010

This module describes the cBarge and Privacy Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) supplementary-service features for IP and analog phones connected to the same Foreign Exchange Station (FXS) ports on a Cisco VG2nn Analog Gateway. While the cBarge feature allows an idle phone to automatically join an already active call on the same shared line just by going offhook, the Privacy feature disallows other users to cBarge into an active call on a shared line. These features are not supported in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for cBarge and Privacy for Shared Lines](#)” section on page 168.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for cBarge and Privacy for Shared Lines, page 160](#)
- [Restrictions for cBarge and Privacy for Shared Lines, page 160](#)
- [Benefits of cBarge and Privacy for Shared Lines, page 160](#)
- [Information About cBarge and Privacy for Shared Lines, page 160](#)
- [How to Configure cBarge and Privacy for Shared Lines, page 162](#)
- [Configuration Examples for cBarge and Privacy for Shared Lines, page 164](#)

- [Additional References, page 167](#)
- [Feature Information for cBarge and Privacy for Shared Lines, page 168](#)

Prerequisites for cBarge and Privacy for Shared Lines

cBarge and Privacy for Shared Lines require the following software component:

- Cisco Unified Communications Manager (Cisco Unified CM) 7.0 or later

cBarge for Shared Lines requires the following hardware component:

- Hardware conference (DSPfarm) resource is registered so that the Cisco Unified CM can perform media mixing with the hardware conference digital signal processors

Restrictions for cBarge and Privacy for Shared Lines

- These features are not supported in Cisco Unified CME.

Benefits of cBarge and Privacy for Shared Lines

The cBarge feature provides parity with incumbent time-division multiplexing PBXs.

Information About cBarge and Privacy for Shared Lines

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Feature Summary, page 161](#)
- [cBarge and Privacy for Shared Lines, page 161](#)

Feature Summary

Table 1 contains information about SCCP-based cBarge and Privacy for Shared Lines on Cisco Voice Gateways.

Table 1 cBarge and Privacy for Shared Lines

Feature	How Phone User Accesses Feature	Configuration on Call-Control System
<p>cBarge for Shared Lines</p> <p>Allows idle IP or analog phones that are connected to the same FXS ports on a Cisco VG2nn Analog Gateway to automatically join already active calls on the same shared lines by simply going offhook.</p>	<p>When there is an existing conversation on a shared line, user goes offhook to cBarge into the conversation.</p> <p>Note Only one analog phone is allowed to cBarge into an active call. When one phone has already been allowed to cBarge into an existing conversation, no other shared line analog phone can cBarge into it.</p>	<p>No configuration tasks required on your Cisco call-control system.</p>
<p>Privacy for Shared Lines</p> <p>Disallows other users to cBarge into active calls on the same FXS ports on a Cisco VG2nn Analog Gateway.</p>	<p>Configuring the port on a shared line on the Cisco Unified CM to Privacy prevents other phones on the shared line to barge into active calls.</p>	<p>No configuration tasks required on your Cisco call-control system.</p>

cBarge and Privacy for Shared Lines

The cBarge feature allows any idle IP or analog phone on a shared line or connected to the same port to automatically join an already active call on the same shared line by simply going offhook. Through the Cisco Unified CM, the three parties are allowed to hold a conference call.



Note

Only one analog phone is allowed to cBarge into an active call. When one phone has already been allowed to cBarge into an existing conversation, no other shared line analog phone can cBarge into it.

In analog switching systems, a single analog port can be connected to multiple analog phones such that when a phone is in an active conversation, any other phone that is connected to the same port can go offhook to join in the conversation.

In digital IP switching (or PBX) systems, a similar capability is supported and it is called a shared line. All the phones using the same directory number are called shared line phones. When there is an existing conversation on a shared line, going offhook enables another shared line phone to cBarge into the conversation.



Note

When cBarge is configured, privacy might be an issue because any idle phone on the shared line that goes offhook can join an existing conversation regardless of the idle phone user's desire to join the call or not.

Privacy is a feature that blocks other phones on a shared line to cBarge into a conversation.

Configuring the port on a shared line on the Cisco Unified CM to Privacy prevents other phones on the shared line to barge into active calls.

How to Configure cBarge and Privacy for Shared Lines

**Note**

This document does not contain details about configuring Cisco Unified CM. See the documentation for this product for installation and configuration instructions.

This section contains the following tasks for configuring cBarge and Privacy for shared lines:

- [Configuring cBarge for Shared Lines, page 162](#)
- [Configuring Privacy for Shared Lines, page 163](#)

Configuring cBarge for Shared Lines

To enable cBarge for analog endpoints in the Cisco Unified CM, perform the following steps on the Cisco VG2nn Analog Gateways.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp supplementary-services**
4. **port *port-number***
5. **hold-resume**
6. **cbarge**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp supplementary-services Example: Router(config)# stcapp supplementary-services	Enters supplementary-service configuration mode.
Step 4	port <i>port-number</i> Example: Router(config-stcapp-supp)# port 2/0	Specifies analog FXS voice port on which STCAPP supplementary-service features are to be supported. <ul style="list-style-type: none"><i>port-number</i>—Voice port number. Range is 2/0 to 2/23.
Step 5	hold-resume Example: Router(config-stcapp-supp-port)# hold-resume	Supports the two-call feature cBarge.
Step 6	cbarge Example: Router(config-stcapp-supp-port)# cbarge	Enables idle phones to join an active call on a shared line. Note Hold/Resume has to be configured if cBarge is to be supported.
Step 7	end Example: Router(config-stcapp-supp-port)# end	Exits STC application supplementary-service configuration mode and returns to privileged EXEC mode.

Configuring Privacy for Shared Lines

To enable Privacy for analog endpoints in the Cisco Unified CM, perform the following steps on the Cisco VG2nn Analog Gateways.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp supplementary-services**
4. **port *port-number***
5. **privacy{ on | off }**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp supplementary-services Example: Router(config)# stcapp supplementary-services	Enters supplementary-service configuration mode.
Step 4	port <i>port-number</i> Example: Router(config-stcapp-supp)# port 2/0	Specifies analog FXS voice port on which STC application supplementary-service features are to be supported. <ul style="list-style-type: none"> <i>port-number</i>—Voice port number. Range is 2/0 to 2/23.
Step 5	privacy { on off } Example: Router(config-stcapp-supp-port)# privacy on	Prevents other ports on the shared line to cBarge into its active call. <ul style="list-style-type: none"> on—Privacy is turned on on this port. off—Privacy is turned off on this port.
Step 6	end Example: Router(config-stcapp-supp-port)# end	Exits STC application supplementary-service configuration mode and returns to privileged EXEC mode.

Configuration Examples for cBarge and Privacy for Shared Lines

This section provides the following configuration examples:

- [Example: Configuring cBarge for Shared Lines, page 165](#)
- [Example: Configuring Privacy for Shared Lines, page 165](#)
- [Example: Privacy for Shared Lines on Cisco VG204, page 165](#)

Example: Configuring cBarge for Shared Lines

The following is a sample output from the **show run** command showing how to enable the cBarge STCAPP supplementary-service feature for analog phones connected to port 2/4 on a Cisco VG224. A similar sample output can also be displayed using the **show stcapp device voice-port x/x (or x/x/x)** command.

```
Router(config)# show run
.
.
.
stcapp supplementary-services
port 2/4
  hold-resume
  cbarge
fallback-dn 5005
end
```

Example: Configuring Privacy for Shared Lines

The following is a sample output from the **show run** command showing how to enable the Privacy STCAPP supplementary-service feature for analog phones connected to port 2/4 on a Cisco VG224. A similar sample output can also be displayed using the **show stcapp device voice-port x/x (or x/x/x)** command.

```
Router(config)# show run
.
.
.
stcapp supplementary-services
port 2/4
  privacy on
end
```

Example: Privacy for Shared Lines on Cisco VG204

The following is a sample output from the **show stcapp device** command showing the Privacy STCAPP supplementary-service feature disabled on port 0/2 of a Cisco VG204:

```
Router(config)# show stcapp device voice-port 0/2

Port Identifier: 0/2
Device Type:    ALG
Device Id:     3
Device Name:   AN1FCAC3B790002
Device Security Mode : None
Modem Capability: None
Device State:  IS
Diagnostic:   None
Directory Number: 9886087491
Dial Peer(s): 87488
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:    STCAPP_DC_EV_DEVICE_FEATURE_STATUS
Line State:    IDLE
Line Mode:     CALL_BASIC
Hook State:    ONHOOK
mwi:          DISABLE
```



```
vmwi:                OFF
mwi config:          Both
Privacy:              OFF
PLAR:                 DISABLE
Callback State:      IDLE
CWT Repetition Interval: 3 second(s)
Number of CCBs:      0
Global call info:
  Total CCB count     = 1
  Total call leg count = 1
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for cBarge and Privacy for Shared Lines

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for cBarge and Privacy for Shared Lines

Feature Name	Releases	Feature Information
cBarge for Shared Lines	15.1(3)T	<p>Allows idle IP or analog phones that are connected to the same FXS ports on a Cisco VG2nn Analog Gateway to automatically join already active calls on the same shared lines by simply going offhook. This feature is supported in Cisco Unified CM only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About cBarge and Privacy for Shared Lines, page 160 • How to Configure cBarge and Privacy for Shared Lines, page 162. <p>The following commands were introduced or modified: cbarge.</p>
Privacy for Shared Line Phones	15.1(3)T	<p>Disallows other users to cBarge into active calls on the same FXS ports on a Cisco VG2nn Analog Gateway. This feature is supported in Cisco Unified CM only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About cBarge and Privacy for Shared Lines, page 160 • How to Configure cBarge and Privacy for Shared Lines, page 162. <p>The following commands were introduced or modified: privacy (supplementary-service).</p>



Configuring Single Number Reach for Analog Phones

First Published: November 19, 2010

This module describes the Single Number Reach (SNR) feature for analog phones connected to Cisco gateway Foreign Exchange Station (FXS) ports. This feature is supported in both the Cisco Unified Communications Manager (Cisco Unified CM) and the Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Single Number Reach for Analog Phones](#)” section on page 175.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Single Number Reach for Analog Phones, page 171](#)
- [Benefits of Using Single Number Reach for Analog Phones, page 172](#)
- [Information About Single Number Reach for Analog Phone, page 172](#)
- [How to Configure Single Number Reach for Analog Phones, page 173](#)
- [Additional References, page 174](#)
- [Feature Information for Single Number Reach for Analog Phones, page 175](#)

Restrictions for Single Number Reach for Analog Phones

This feature does not support mobility.

Benefits of Using Single Number Reach for Analog Phones

The SNR feature provides parity with incumbent time-division multiplexing PBXs.

Information About Single Number Reach for Analog Phone

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concept:

- [Single Number Reach for Analog Phones, page 172](#)

Single Number Reach for Analog Phones

The SNR feature allows you to answer incoming calls to your analog phones on preconfigured alternate phones (external phones), such as desktop or mobile phones.

When an incoming call is directed to your analog phone, all the alternate phones configured in the SNR ring simultaneously (configurable). When you answer the call on one of the assigned numbers, all the other assigned numbers stop ringing (configurable).

You can pick up active calls on any of the assigned external phones, enabling callers to dial a single number (extension number) to reach you.

For SNR, the incoming call is regarded as a normal call. The only difference lies in what controls the analog endpoints: the Cisco Unified CME or the Cisco Unified CM.

In Cisco Unified CME, only one external phone can be configured but that external phone can also be a Cisco Unified CME extension (also called an internal phone).

When the assigned external phone answers the call, the internal phone is put on hold. Once you pick up the internal phone, the external phone is disconnected and the call continues on the internal phone. However, once the call is answered on the internal phone, the call cannot be switched to the external phone.

In Cisco Unified CM, only external phones can be configured as an SNR phone for your analog phones.

When you answer a call using an external phone, the internal phone goes into the remote multiline state. When the external phone disconnects from the call, the Cisco Unified CM puts the call on hold for a configured period of time. During this period, the call can be picked up on the internal phone by going offhook. In case the internal phone does not go offhook before the end of the configured time is reached, the internal phone is also disconnected.

When you answer a call using the Cisco Unified CM extension (internal phone), all the external phones are disconnected and are put in the idle state. However, once the call is answered on the internal phone, the call cannot be switched to the external phone.

If you have several phone numbers, you can setup all the numbers into your analog phones.

**Note**

The SNR feature is required for users who have analog phones on their desks but would like to get calls simultaneously on their predefined mobile or alternate telephone number.

How to Configure Single Number Reach for Analog Phones

**Note**

This document does not contain details about configuring Cisco Unified Communications Manager or Cisco Unified CME. See the documentation for these products for installation and configuration instructions.

To configure SNR in Cisco Unified CM, see [Configuring Cisco Unified Mobility](#).

To configure SNR in Cisco Unified CME, see [Configuring Single Number Reach](#).

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	<i>Cisco Unified Communications Manager</i>
Cisco Unified Communications Manager Express	<i>Cisco Unified Communications Manager Express</i>
Cisco IOS debugging	<i>Cisco IOS Debug Command Reference</i>
Cisco IOS voice commands	<i>Cisco IOS Voice Command Reference</i>
Cisco IOS voice configuration	<i>Cisco IOS Voice Configuration Library</i>
Cisco voice gateway	<ul style="list-style-type: none"> • <i>Cisco VG200 Series Gateway</i> • <i>Cisco 1800 Series Integrated Services Routers</i> • <i>Cisco 2800 Series Integrated Services Routers</i> • <i>Cisco 3800 Series Integrated services Routers</i> • <i>Cisco Unified 500 Series</i>
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the <i>Cisco Unified CallManager and Cisco IOS Interoperability Guide</i>. • <i>Cisco CallManager and IOS Gateway DSP Farm Configuration Example</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Single Number Reach for Analog Phones

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

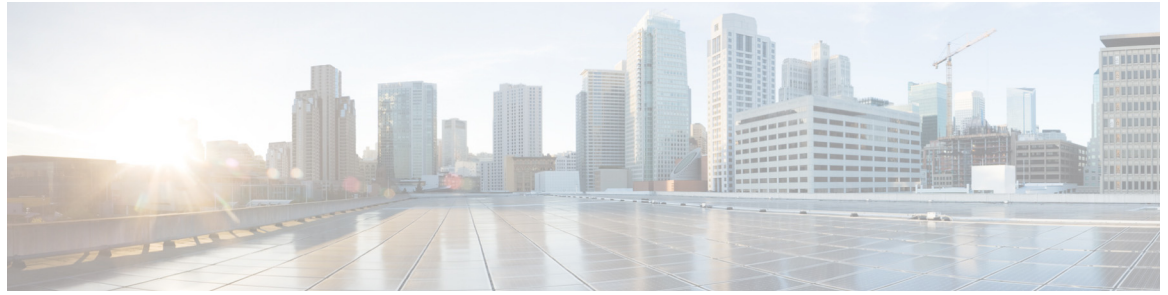
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Single Number Reach for Analog Phones

Feature Name	Releases	Feature Information
Single Number Reach for Analog Phones	15.1(3)T	<p>Enables incoming calls to analog phones connected to Cisco gateway FXS ports to be received on predefined alternate telephone numbers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Single Number Reach for Analog Phone, page 172 • How to Configure Single Number Reach for Analog Phones, page 173 <p>No new commands were introduced by this feature.</p>



Media Renegotiation

First Published: November 19, 2010

This module describes the Media Renegotiation feature for the enhancement of the media setup process in the Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) state machine. This feature enables media setup call flows to have improved interworking with third-party call control/Computer Telephony Integration (3PCC/CTI) that control analog endpoints behind IOS gateways.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Media Renegotiation](#)” section on page 180.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Benefits of Media Renegotiation](#), page 178
- [Information About Media Renegotiation](#), page 178
- [Additional References](#), page 179
- [Feature Information for Media Renegotiation](#), page 180

Benefits of Media Renegotiation

Media Renegotiation enables media setup call flows to have improved interworking with 3PCC/CTI that control analog endpoints behind IOS gateways.

This feature does not change the user behavior such that you do not notice any difference when you are having a call that experiences media renegotiation.

Information About Media Renegotiation

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concepts:

- [Media Renegotiation, page 178](#)

Media Renegotiation

In some customer environments, the media setup messages may arrive in a different sequence and involve a different protocol translation. If the remote side uses a different protocol from that of the calling phone, the media setup message sequence might be different.

Through Media Renegotiation, the media setup process in the STCAPP state machine can be enhanced to support any of the most possible sequences of the media setup messages.

Through this feature, media renegotiation can be introduced in the middle of a call and after early media (before and after the call is connected) is flowing.

The basic concept of the Media Renegotiation design is that no matter which media event is received, the event handler handles only the media direction that belongs to the event. For example, when an event involving the closure of the receiving channel is received, the event handler disconnects the receiving part of the media only, leaving the sending part unaffected in case the media path works both ways.

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Media Renegotiation

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 *Feature Information for Media Renegotiation*

Feature Name	Releases	Feature Information
Media Renegotiation	15.1(3)T	Enhances the STCAPP state machine to support any of the most possible sequences of the media setup messages. The following section provides information about this feature: <ul style="list-style-type: none"> Information About Media Renegotiation, page 178 No new commands were introduced by this feature.



Configuring DTMF Relay, Fax Relay, and Modem Relay

First Published: June 22, 2006
Last Updated: March 19, 2010

This document describes how to enable DTMF Relay, Fax Relay and Modem Relay for analog Foreign Exchange Service (FXS) ports on Cisco voice gateways under the control of Cisco Unified Communications Manager or Cisco Unified Communications Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#)” section on page 191.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 182
- [Restrictions for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 182
- [Information About DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 182
- [How to Configure DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 184
- [Configuration Examples for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 189
- [Additional References](#), page 190
- [Feature Information for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#), page 191

Prerequisites for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

Cisco IOS Gateway

- Cisco IOS Release 12.4(6)XE or a later release.
- The Cisco IOS gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see the [Cisco IOS Voice Port Configuration Guide](#).
- SCCP version 4.0 or a later version and the SCCP telephony control (STC) application is enabled on the Cisco IOS gateway. For configuration information, see the “[Configuring FXS Ports for Basic Calls](#)” section on page 17.

Analog Endpoints in Cisco Unified Communications Manager

- Cisco Unified Communications Manager 4.2 or a later version.
- For RFC 2833 DTMF Digit Relay: Cisco Unified Communications Manager 5.0.1 or a later version.

Analog Endpoints in Cisco Unified CME

- Cisco Unified CME 4.0 or a later version.

Restrictions for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

- Autoconfiguration using TFTP download of extensible markup language (XML) dial-peer configuration files from Cisco Unified Communications is not supported.
- RFC 2833 DTMF Digit Relay is not supported for Cisco Unified CME or Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST).
- RFC 2833 DTMF Digit Relay does not support FXS ports configured for SCCP private line, automatic ring-down (PLAR).
- RFC 2833 DTMF Digit Relay is not supported between two SCCP analog phones; one of the endpoints must be a Session Initiation Protocol (SIP) trunk, a Cisco IOS gateway, or a port.

Information About DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

To configure DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS, you should understand the following concepts:

- [RFC 2833 DTMF Digit Relay Support on SCCP Controlled Endpoints, page 183](#)
- [SCCP Gateway Controlled Fax Relay, page 183](#)
- [SCCP Gateway Controlled Modem Relay, page 183](#)

RFC 2833 DTMF Digit Relay Support on SCCP Controlled Endpoints

The RFC 2833 DTMF Digit Relay feature on the SCCP analog gateway sends RFC 2833 digits through Real-time Transport Protocol (RTP) packets and out-of-band (OOB) digits to Cisco Unified Communications Manager. This feature is not supported in Cisco Unified CME or Cisco Unified SRST.

The RFC 2833 DTMF Digit Relay feature is enabled by default on the Cisco IOS gateway and on the Cisco Unified Communications Manager, where it can be disabled. No configuration is required on the SCCP analog gateway or on Cisco Unified Communications Manager to enable this feature.

SCCP Gateway Controlled Fax Relay

Before Cisco IOS Release 12.4(6)XE, SCCP gateways supported fax passthrough only. In Cisco IOS Release 12.4(6)XE and later releases, SCCP Gateway Controlled Fax Relay adds support for the following fax relay features for SCCP analog endpoints:

- T.38 named signaling events (NSE) forced fax relay—Provides an ITU-T standards-based method for fax relay. Data is packetized and encapsulated according to the T.38 standard fax protocol. The SCCP gateway uses NSEs to indicate T.38 fax relay switchover. Configuring the gateway to unconditionally use T.38 NSE forced fax relay enables interoperability with a Cisco voice gateway that does not support interworking and negotiation of T.38 fax relay and NSE attributes at the time of call setup.
- Cisco fax relay—Proprietary fax relay implementation that uses RTP to transport fax data. Fax relay is the default mode for passing faxes through a VoIP network, and Cisco fax relay is the default fax relay type on Cisco voice gateways.
- Super Group 3 (SG3) to G3 fax relay—Allows the fax stream between two SG3 fax machines to negotiate down to G3 speeds (less than 14.4 kbps) allowing SG3 fax machine interoperability over T.38 fax relay with G3 fax machines.

For configuration information, see the [“Configuring SCCP Gateway Fax Relay Features”](#) section on page 184.

SCCP Gateway Controlled Modem Relay

There are two ways to transport modem traffic over VoIP networks: modem pass-through and modem relay.

Modem pass-through transports modem signals through a packet network using PCM encoded packets; traffic is susceptible to packet loss, jitter, and latency in the IP network.

With modem relay, the modem signals are demodulated at one gateway, converted into digital form, and carried in Simple Packet Relay Transport (SPRT) packets to the other gateway. There the modem signal is re-created and remodulated, then passed to the receiving modem. Modem relay lessens bandwidth requirements and significantly reduces the effect that dropped packets, jitter, and latency have on the modem session.

Before Cisco IOS Release 12.4(6)XE, only modem pass-through only and Cisco Unified Communications Manager-controlled modem relay were supported for SCCP gateways. In Cisco IOS Release 12.4(6)XE and later releases, the SCCP Gateway Controlled Modem Relay feature adds support for SCCP gateway-controlled modem relay.

Cisco uses a proprietary protocol, NSE, to signal events that are exchanged between gateways, using Real-time Transport Protocol (RTP) packets. SCCP gateway-controlled modem-relay bypasses NSE parameter negotiation between gateways and uses the NSE mechanism to indicate the gateway control mode to the other gateway. NSE signaling capability must be configured on both the originating and terminating gateways to enable modem-relay calls for SCCP analog endpoints.

For configuration information, see the [“Configuring SCCP Gateway Controlled Modem Relay” section on page 186](#).

**Note**

In addition to a proprietary, NSE-based modem-relay implementation, Cisco offers V.150.1 modem-relay implementation. The VMWI for SCCP FXS Ports in Cisco IOS feature supports only NSE modem relay. For information about feature mode, see the [“Configuring Feature Mode” section on page 93](#).

How to Configure DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

This section contains the following tasks:

- [Configuring SCCP Gateway Fax Relay Features, page 184](#)
- [Configuring SCCP Gateway Controlled Modem Relay, page 186](#)
- [Verifying and Troubleshooting DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS Feature Configuration, page 187](#)

Configuring SCCP Gateway Fax Relay Features

To configure SCCP gateway fax relay features, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **fax protocol t38 nse force**
5. **fax protocol cisco**

- 6. `fax-relay sg3-to-g3`
- 7. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code> Example: Router(config)# voice service voip	Enters voice service configuration mode and specifies VoIP encapsulation.
Step 4	<code>fax protocol t38 nse force</code> Example: Router(config-voi-serv)# fax protocol t38 nse force	(Optional) Specifies ITU-T T.38 standard fax protocol. <ul style="list-style-type: none">nse force—Configures the SCCP gateway to use NSEs to indicate T.38 fax relay switchover, whether T.38 functionality is negotiated with the far-end gateway or not.
Step 5	<code>fax protocol cisco</code> Example: Router(config-voi-serv)# fax protocol cisco	(Optional) Specifies the Cisco-proprietary fax protocol as the default fax protocol for SCCP analog endpoints.
Step 6	<code>fax-relay sg3-to-g3</code> Example: Router(config-voi-serv)# fax relay sg3-to-g3	(Optional) Enables the fax stream between two SG3 fax machines to negotiate down to G3 speeds.
Step 7	<code>end</code> Example: Router(config-voi-serv)# end	Exits the current configuration mode and returns to global configuration mode.

Examples

The following output from the `show voice dsp` command displays fax codec settings:

```
Router# show voice dsp
TYPE  NUM    CH CODEC    VERSION    STATE.....
=====
C5510 001    01 fax        9.0.108    busy
C5510 001    02 fax        9.0.108    busy
```

The following output from the `show voice call summary` command display fax codec settings:

```

Router# show voice call summary

PORT          CODEC          VAD VTSP.....
=====
1/0/0         t38 (or cisco) n S_CONNECT
1/0/1         t38 (or cisco) n S_CONNECT

```

Troubleshooting Tips

The following commands can help troubleshoot SCCP fax relay features:

- **debug voip application stcapp all**
- **debug voip vtsp all**

Configuring SCCP Gateway Controlled Modem Relay

This task configures SCCP gateway controlled modem relay.

Prerequisites

SCCP gateway controlled modem relay must be configured on both the originating and terminating gateways.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **modem relay nse codec [g711u | g711a] gw-controlled**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters voice service configuration mode and specifies VoIP encapsulation.
Step 4	modem relay nse codec [g711u g711a] gw-controlled Example: Router(conf-voi-serv)# modem relay nse codec g711u gw-controlled	Configures modem relay over VoIP. <ul style="list-style-type: none"> g711u—Specifies codec G.711m u-law 64,000 bits per second (bps) for T1. g711a—Specifies codec G.711 a-law 64,000 bps for E1. gw-controlled—Specifies the gateway-configured method for establishing modem relay parameters.
Step 5	end Example: Router(conf-voi-serv)# end	Exits the current configuration mode and returns to global configuration mode.

Verifying and Troubleshooting DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS Feature Configuration

To verify the configuration of VMWI for SCCP FXS Ports in Cisco IOS features, use the **show-running config** command. A sample output is located in the “[Configuration Examples for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS](#)” section on page 189.

Use the following commands to verify and troubleshoot the configuration of the dial tone generation after remote onhook feature:

- show dial-peer voice *number***—Displays whether the dial tone after remote onhook feature is enabled.
- show stcpp device voice-port *port***—Displays whether the dial tone after remote onhook feature is enabled.
- debug voip application stcpp all**—Displays detailed debugging for SCCP and STC application ports.
- debug voip application stcpp port *port-number***—Displays detailed debugging for the specified SCCP and STC application port.

Use the following commands to verify and troubleshoot the configuration of the ground start FXS ports feature:

- **show stcpp device summary**—Displays a summary of endpoints associated with the STC application, their states, types and call control device.
- **show voice port slot/subunit/port**—Displays whether ground-start signaling is enabled and displays port states.
- **debug vpm signal**—Displays supervisory disconnect event messages.

Use the following commands to verify and troubleshoot the RFC 2833 DTMF digit relay feature.

- **debug voip application stcpp port port-number**—Displays RFC 2833 send and receive payload messages.
- **debug voip hpi**—Displays digital signal processor (DSP) programming.
- **debug voip rtp session named-event**—Verifies the gateway sending inband DTMF signaling.

Use the following commands to verify and troubleshoot SCCP gateway controlled modem relay:

- **show voice call summary**—Displays modem relay voice port settings.
- **show voice dsp**—Displays modem relay DSP channel status.
- **debug voip application stcpp all**—Displays STC application modem relay information.
- **debug voip dsm all**—Displays modem relay DSP stream manager (DSM) messages.
- **debug voip dsmp all**—Displays modem relay distributed stream media processor (DSMP) messages.
- **debug voip hpi all**—Displays gateway DSP modem relay termination codes and messages indicating probable causes for disconnection.

Use the following commands to verify and troubleshoot SCCP gateway controlled fax relay:

- **show voice call summary**—Displays fax relay voice port settings.
- **show voice dsp**—Displays fax relay DSP channel status.
- **debug voip application stcpp all**— Displays STC application fax relay information.
- **debug voip dsm all**—Displays fax relay DSM messages.
- **debug voip dsmp all**—Displays fax relay DSMP messages.
- **debug voip hpi all**—Displays gateway DSP fax relay information on RTP packet events.
- **debug voip vtsp all**—Displays gateway voice telephony service provider (VTSP) debugging information for fax calls.



Note

For more information on these commands, see the [Cisco IOS Voice Command Reference](#), [Cisco IOS Debug Command Reference, Release 12.4T](#), and [Cisco IOS Configuration Fundamentals Command Reference, Release 12.4](#).

Configuration Examples for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

The following example shows modem relay enabled and dial tone after remote onhook is disabled. The **fax protocol cisco** command does not appear in the output because it is set to its default value.

```
Router# show running-config
.
.
modem relay nse codec g711ulaw
.
.
no tone dialtone remote-onhook
dial-peer voice 3002 pots
  service stcapp
  port 1/1/0
!
!
!
```


Additional References

The following sections provide references related to the VMWI for SCCP FXS Ports in Cisco IOS feature.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager interoperability	<i>Cisco Unified CallManager and Cisco IOS Interoperability Guide</i>
Cisco Unified Communications Manager	<i>Cisco Unified Communications Manager System Guide</i>
Cisco Unified Communications Express	<i>Cisco Unified CME Administrator Guide</i>
Cisco IOS debugging	<i>Cisco IOS Debug Command Reference</i>
Cisco IOS voice commands	<i>Cisco IOS Voice Command Reference</i>
Cisco IOS voice configuration guides	<i>Cisco IOS Voice Configuration</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(6)XE or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for VMWI for SCCP FXS Ports in Cisco IOS Feature

Feature Name	Releases	Feature Information
DTMF Relay, Fax Relay and Modem Relay for SCCP FXS Ports in Cisco IOS	12.4(6)XE 12.4(11)T	<p>Enhances the transmission of DTMF digits, faxes and modems between SCCP FXS ports on Cisco IOS gateways. DTMF digit transmission is supported by using RFC 2833. Cisco Fax Relay, Cisco T.38 Fax Relay, and Cisco Modem Relay are supported using Names Signaling Events (NSE).</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS, page 182. How to Configure DTMF Relay, Fax Relay, and Modem Relay for SCCP FXS Ports in Cisco IOS, page 184. <p>The following commands were introduced or modified by this feature: debug voip application stcapp all; debug voip application stcapp port; show stcapp device; tone dialtone remote-onhook</p>



Configuring Secure Signaling and Media Encryption for the Cisco VG224

Last Updated: March 19, 2010

This chapter describes the Secure Signaling and Media Encryption for analog phones that are connected to Foreign Exchange Station (FXS) ports on a Cisco VG224 Analog Phone Gateway and controlled by Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this chapter. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Secure Signaling and Media Encryption for the Cisco VG224](#)” section on page 212.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Secure Signaling and Media Encryption for the Cisco VG224](#), page 194
- [Information About Secure Signaling and Media Encryption for the Cisco VG224](#), page 194
- [How to Configure Secure Signaling and Media Encryption for the Cisco VG224](#), page 195
- [Configuration Examples for Secure Signaling and Media Encryption for the Cisco VG224](#), page 206
- [Additional References](#), page 211
- [Feature Information for Secure Signaling and Media Encryption for the Cisco VG224](#), page 212

Prerequisites for Secure Signaling and Media Encryption for the Cisco VG224

Cisco IOS Gateway

- Cisco IOS Release 12.4(11)XW or a later release.
- Set the system clock by using one of the following methods. For configuration information, see the “[Performing Basic System Management](#)” chapter of the *Cisco IOS Network Management Configuration Guide* for your Cisco IOS release.
 - Configure Network Time Protocol (NTP).
 - Manually set the software clock by using the **clock set** command. On Cisco integrated services routers, use the **clock set** and **clock update-calendar** commands.

Analog Endpoints in Cisco Unified CME

- Cisco Unified CME 4.2 or a later version.

Restrictions for Secure Signaling and Media Encryption for the Cisco VG224

- This feature is not supported for analog SCCP endpoints in Cisco Unified Communications Manager.

Information About Secure Signaling and Media Encryption for the Cisco VG224

To enable Secure Signaling and Media Encryption for the Cisco VG224, you should understand the following concept:

- [Media Encryption \(SRTP\), page 194](#)

Media Encryption (SRTP)

Media Encryption (SRTP) and companion voice security Cisco IOS features in Cisco Unified CME 4.2 and later versions provide secure voice call capabilities including secure analog endpoints connected to Cisco VG224 Analog Phone Gateway endpoints.

The Media Encryption (SRTP) on Cisco Unified CME feature supports the following features:

- Secure voice calls using SRTP for SCCP endpoints
- Secure voice calls in a mixed shared line environment that allows both RTP and SRTP capable endpoints; shared line media security depends on the endpoint configuration.
- Secure supplementary services using H.450 including:
 - Call forward
 - Call transfer

- Call hold and resume
- Call park and call pickup
- Nonsecure software conferenc

**Note**

SRTP conference calls over H.323 may experience a 0 to 2 second noise interval when the call is joined to the conference.

- Secure calls in a nonH.450 environment
- Secure Cisco Unified CME interaction with secure Cisco Unity
- Secure Cisco Unified CME interaction with Cisco Unity Express (interaction is supported and calls are downgraded to nonsecure mode)
- Secure transcoding for remote phones with DSP farm transcoding configured.

For information about these features in Cisco Unified CME, see the “[Configuring Security](#)” module of the *Cisco Unified CME System Administration Guide*.

To configure SRTP for a Cisco VG224 Analog Phone Gateway, see the “[How to Configure Secure Signaling and Media Encryption for the Cisco VG224](#)” section on page 195.

How to Configure Secure Signaling and Media Encryption for the Cisco VG224

Media Encryption (SRTP) on Cisco Unified CME provides secure voice call capabilities including secure Cisco VG224 Analog Phone Gateway endpoints.

**Note**

For information about this feature in Cisco Unified CME, see the “[Configuring Security](#)” module in the *Cisco Unified CME System Administration Guide*.

To add a Cisco VG224 Analog Phone Gateway to a secure Cisco Unified CME system, perform the following tasks:

- [Configuring an External CA Server, page 195](#) (required)
- [Creating a Trustpoint on the VG224, page 198](#) (required)
- [Configuring STCAPP, Trustpoint, and Security, page 201](#) (required)
- [Verifying and Troubleshooting Secure Signaling and Media Encryption on the Cisco VG224, page 203](#) (optional)

Configuring an External CA Server

To configure an external certificate authority (CA) server, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto pki server** *cs-label*
4. **database level** {**minimal** | **names** | **complete**}
5. **grant auto**
6. **database url** *root-url*
7. **no shutdown**
8. **exit**
9. **crypto pki trustpoint** *label*
10. **revocation-check** *method1* [*method2* [*method3*]]
11. **rsa keypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **ip http server**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki server <i>cs-label</i> Example: Router(config)# crypto pki server cserver1	Defines a label for the certificate server and enters certificate server configuration mode. <ul style="list-style-type: none"> <i>cs-label</i>—Name for CA certificate server.
Step 4	database level { minimal names complete }	(Optional) Controls the type of data stored in the certificate enrollment database. <ul style="list-style-type: none"> minimal—Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality. names—The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke a particular certificate, if necessary. complete—In addition to the information given in the minimal and names levels, each issued certificate is written to the database. <p>Note The complete keyword produces a large amount of information; so specify an external TFTP server in which to store the data using of the database url command.</p>

	Command or Action	Purpose
Step 5	<p>grant auto</p> <p>Example: Router(cs-server)# grant auto</p>	<p>(Optional) Allows an automatic certificate to be issued to any requester. The recommended method and default if this command is not used is manual enrollment.</p> <p>Tip Use this command only during enrollment when testing and building simple networks. A security best practice is to disable this functionality using the no grant auto command after configuration so that certificates cannot be continually granted.</p>
Step 6	<p>database url root-url</p> <p>Example: Router(cs-server)# database url nvram:</p>	<p>(Optional) Specifies the location where all database entries for the certificate server are to be written out. If this command is not specified, all database entries are written to NVRAM.</p> <ul style="list-style-type: none"> <i>root-url</i>—Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system. If the CA is going to issue a large number of certificates, select an appropriate storage location like flash or other storage device to store the certificates. <p>Note When the storage location chosen is flash and the file system type on this device is Class B (LEFS), make sure to check free space on the device periodically and use the squeeze command to free the space used up by deleted files. This process may take several minutes and should be done during scheduled maintenance periods or off-peak hours.</p>
Step 7	<p>no shutdown</p> <p>Example: Router(cs-server)# no shutdown</p>	<p>(Optional) Enables the CA.</p> <ul style="list-style-type: none"> You should use this command only after you have completely configured the CA. Enter your password when prompted.
Step 8	<p>exit</p> <p>Example: Router(cs-server)# exit</p>	Exits certificate server configuration mode.
Step 9	<p>crypto pki trustpoint label</p> <p>Example: Router(config)# crypto pki trustpoint cserver1</p>	<p>(Optional) Declares a trustpoint and enters CA-trustpoint configuration mode.</p> <ul style="list-style-type: none"> Use this command and the enrollment url command if this CA is local to the Cisco Unified CME router. These commands are not needed for a CA running on an external router. <i>label</i>—Name for the trustpoint. The <i>label</i> in this step should be the same as the <i>cs-label</i> in Step 3.

Command or Action	Purpose
<p>Step 10 <code>revocation-check method1 [method2[method3]]</code></p> <p>Example: Router(ca-trustpoint)# revocation-check crl</p>	<p>(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.</p> <p>Valid values for the <i>method</i> argument are as follows:</p> <ul style="list-style-type: none"> • crl—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • none—Certificate checking is not required. • ocsp—Certificate checking is performed by an Online Certificate Status Protocol (OCSP) server.
<p>Step 11 <code>rsa-keypair key-label [key-size [encryption-key-size]]</code></p> <p>Example: Router(ca-trustpoint)# rsa-keypair exampleCAkeys 1024 1024</p>	<p>(Optional) Specifies an RSA key pair to use with a certificate.</p> <ul style="list-style-type: none"> • <i>key-label</i>—Name of the key pair, which is generated during enrollment if it does not already exist or if the auto-enroll regenerate command is used. • <i>key-size</i>—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • <i>encryption-key-size</i>—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. <p>Note Multiple trustpoints can share the same key.</p>
<p>Step 12 <code>exit</code></p> <p>Example: Router(ca-trustpoint)# exit</p>	<p>Exits CA-trustpoint configuration mode.</p>
<p>Step 13 <code>ip http server</code></p> <p>Example: Router(config)# ip http server</p>	<p>Enables the Cisco web-browser user interface on the local Cisco Unified CME router.</p>
<p>Step 14 <code>exit</code></p> <p>Example: Router (config)# exit</p>	<p>Exits global configuration mode.</p>

Creating a Trustpoint on the VG224

To create a trustpoint on the Cisco VG224, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto key generate rsa general-keys label** *key-label*
4. **crypto pki trustpoint** *label*
5. **enrollment url** *ca-url*
6. **serial-number** *none*
7. **fqdn** *none*
8. **ip-address** *none*
9. **subject-name** [*x.500-name*]
10. **revocation-check** *none*
11. **rsa keypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **crypto pki authenticate** *trustpoint-label*
14. **crypto pki enroll** *trustpoint-label*
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa general-keys label <i>key-label</i> Example: Router(config)# crypto key generate rsa general-keys label VG224	(Optional) Generates Rivest, Shamir, and Adelman (RSA) key pairs. <ul style="list-style-type: none">• general-keys—Specifies that the general-purpose key pair should be generated.• label <i>key-label</i>—(Optional) Name that is used for an RSA key pair when they are being exported.
Step 4	crypto pki trustpoint <i>label</i> Example: Router(config)# crypto pki trustpoint VG224	Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode. <ul style="list-style-type: none">• <i>label</i>—Name for the trustpoint and RA.
Step 5	enrollment url <i>ca-url</i> Example: Router(ca-trustpoint)# enrollment url http://10.3.105.40:80	Specifies the enrollment URL of the issuing CA certificate server (root certificate server). <ul style="list-style-type: none">• <i>ca-url</i>—URL of the router on which the root CA has been installed.

	Command or Action	Purpose
Step 6	<p>serial-number none</p> <p>Example: Router(ca-trustpoint)# serial-number none</p>	<p>Specifies whether the router serial number should be included in the certificate request.</p> <ul style="list-style-type: none"> none—Specifies that a serial number will not be included in the certificate request.
Step 7	<p>fqdn none</p> <p>Example: Router(ca-trustpoint)# fqdn none</p>	<p>Specifies a fully qualified domain name (FQDN) that will be included as “unstructuredName” in the certificate request.</p> <ul style="list-style-type: none"> none—Router FQDN will not be included in the certificate request.
Step 8	<p>ip-address none</p> <p>Example: Router(ca-trustpoint)# ip-address none</p>	<p>Specifies a dotted IP address or an interface that will be included as “unstructuredAddress” in the certificate request.</p> <ul style="list-style-type: none"> none—Specifies that an IP address is not to be included in the certificate request.
Step 9	<p>subject-name [x.500-name]</p> <p>Example: Router(ca-trustpoint)# subject-name cn=VG224, ou=ABU, o=Cisco Systems Inc.</p>	<p>Specifies the subject name in the certificate request.</p> <p>Note The example shows how to format the certificate subject name to be similar to that of an IP phone’s.</p>
Step 10	<p>revocation-check none</p> <p>Example: Router(ca-trustpoint)# revocation-check none</p>	<p>(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.</p> <ul style="list-style-type: none"> none—Certificate checking is not required.
Step 11	<p>rsakeypair key-label [key-size [encryption-key-size]]</p> <p>Example: Router(ca-trustpoint)# rsakeypair VG224</p>	<p>(Optional) Specifies an RSA key pair to use with a certificate.</p> <ul style="list-style-type: none"> key-label—Name of the key pair, which is generated during enrollment if it does not already exist or if the auto-enroll regenerate command is used. key-size—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. encryption-key-size—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. <p>Note Multiple trustpoints can share the same key.</p>
Step 12	<p>exit</p> <p>Example: Router(ca-trustpoint)# exit</p>	<p>Exits CA-trustpoint configuration mode.</p>

	Command or Action	Purpose
Step 13	<pre>crypto pki authenticate trustpoint-label</pre> <p>Example: Router(config)# crypto pki authenticate VG224</p>	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted. <ul style="list-style-type: none"> <i>trustpoint-label</i>—Trustpoint label. <p>Note This command is optional if the CA certificate is already loaded into the configuration.</p>
Step 14	<pre>crypto pki enroll trustpoint-label</pre> <p>Example: Router(config)# crypto pki enroll VG224</p>	Enrolls with the CA and obtains the certificate for this trustpoint. <ul style="list-style-type: none"> <i>trustpoint-label</i>—Trustpoint label.
Step 15	<pre>exit</pre> <p>Example: Router(config)# exit</p>	Exits global configuration mode.

Configuring STCAPP, Trustpoint, and Security

To configure STCAPP, trustpoint, and security mode, perform the following steps on the Cisco VG224.

Prerequisites

- SCCP is enabled on the Cisco voice gateway. STC application group to be configured is created. For configuration information, see the [“Enabling SCCP on the Voice Gateway”](#) section on page 21.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `stcapp ccm-group group-id`
4. `stcapp security trustpoint line`
5. `stcapp security mode [authenticated | encrypted | none]`
6. `stcapp`
7. `dial-peer voice tag pots`
8. `security mode [authenticated | encrypted | none]`
9. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp ccm-group group-id Example: Router(config)# stcapp ccm-group 1	Configures an STC application group. <ul style="list-style-type: none"> Group to be configured is already created by using the scp ccm group command. See the “Enabling SCCP on the Voice Gateway” section on page 21.
Step 4	stcapp security trustpoint line Example: Router(config)# stcapp security trustpoint VG224	Specifies the trustpoint to be used for setting up the TLS connection for STCAPP endpoints. <ul style="list-style-type: none"> This command must be configured for the STCAPP service to start.
Step 5	stcapp security mode [authenticated encrypted none] Example: Router(config)# stcapp security mode encrypted	Enables security for STCAPP endpoints. <ul style="list-style-type: none"> This command and the stcapp security trustpoint command in the previous step must be configured for security to be enabled for the STCAPP endpoint.
Step 6	stcapp Example: Router(config)# stcapp	Enables the STCAPP at the global level.
Step 7	dial-peer voice tag pots Example: Router(config)# dial-peer voice 1 pots	(Optional) Enters dial peer voice configuration mode.
Step 8	security mode [authenticated encrypted none] Example: Router(config-dialpeer)# security mode encrypted	(Optional) Enables dialpeer level STCAPP endpoint security and overrides global configuration. <ul style="list-style-type: none"> authenticated—Enables STCAPP endpoints using signaling authentication. encrypted—Enables STCAPP endpoints using data encryption. none—Disables dialpeer level STCAPP endpoint security configuration and defaults to global level configuration.
Step 9	end Example: Router(config-dialpeer)# end	Exits dial-peer configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting Secure Signaling and Media Encryption on the Cisco VG224

To verify and troubleshoot secure signaling and media encryption on the VG224, perform the following steps:

SUMMARY STEPS

1. `show sccp`
2. `show dial-peer voice`
3. `debug sccp tls`
4. `debug sccp message`
5. `debug voip application stcapp all`
6. `show stcapp device voice-port port`
7. `show call active voice brief`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show sccp</code> Example: Router> show sccp	Displays SCCP information such as administrative and operational status.
Step 2	<code>show dial-peer voice</code> Example: Router> show dial-peer voice	Displays dial peer information including security mode
Step 3	<code>debug sccp tls</code> Example: Router# configure terminal	Displays debugging information for SCCP and its related applications (transcoding and conferencing).
Step 4	<code>debug sccp message</code> Example: Router# debug sccp message	Displays debugging information for SCCP and its related applications (transcoding and conferencing).
Step 5	<code>debug voip application stcapp all</code> Example: Router# debug voip application stcapp all	Displays debugging information for the components of the STCAPP.

	Command or Action	Purpose
Step 6	<code>show stcapp device voice-port port</code> Example: Router# show stcapp device voice-port 1/0/0	Displays configuration information about a specified STCAPP analog voice port.
Step 7	<code>show call active voice brief</code> Example: Router# show call active voice brief	Displays a truncated version of call information for voice calls in progress.

Examples

The following examples show sample output for commands used to verify and troubleshoot STCAPP and security mode configuration:

show dial-peer voice: Example

```
Show dial-peer voice 5001

VoiceEncapPeer5001
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 5001, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
.....
.....
digit_strip = enabled,
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system, payload size = 20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
    maximum = 64 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
    inbound = `', outbound = ` '
dial tone generation after remote onhook = enabled
The following lines show encryption enabled:

Signaling and Media Security = Encrypted

Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

show sccp: Example

```
show sccp
SCCP Admin State: UP
Gateway IP Address: 10.4.177.53, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
```

```
Call Manager: 10.4.177.51, Port Number: 2000
Priority: N/A, Version: 4.0, Identifier: 1
```

```
Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2443
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D400
```

The following lines show secure media and signaling status:

```
Security
  Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220
```

```
Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D401
```

The following lines show secure media and signaling status:

```
Security
  Signaling Security: AUTHENTICATED TLS
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220
```

```
Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D402
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220
```

show stcapp device voice-port: Example

```
Show stcapp device voice-port 2/0
Port Identifier: 2/0
Device Type:     ALG
Device Id:       2
Device Name:     AN0C8639A24D400
```

The following line shows device security status:

```
Device Security Mode : Encrypted
Modem Capability: None
Device State:        IS
```



```

Diagnostic:          None
Directory Number:   5001
Dial Peer(s):       5001
Dialtone after remote onhook feature: activated
Last Event:         STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:         IDLE
Hook State:         ONHOOK
mwi:                DISABLE
vmwi:               OFF
PLAR:               DISABLE
Number of CCBs:     0
Global call info:
  Total CCB count    = 0
  Total call leg count = 0

```

Configuration Examples for Secure Signaling and Media Encryption for the Cisco VG224

The following examples show STCAPP security enabled at the system level and the security mode configured on the dial peer:

```

Router# show running-config
Building configuration...
Current configuration : 8906 bytes
!
! Last configuration change at 15:41:09 PDT Mon Oct 23 2006
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname akash
!
boot-start-marker
boot-end-marker
!
logging buffered 400000 debugging
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no ip domain lookup
!
!
!

```

The following lines show STCAPP security enabled at the system level:

```

stcapp ccm-group 1
stcapp security trustpoint analog
stcapp security mode encrypted
stcapp
!
voice-card 0
dsp services dspfarm
!
crypto pki trustpoint analog
enrollment url http://10.4.177.51:80
serial-number
revocation-check none
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BF AFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
crypto pki certificate chain analog
certificate 0A
308201BF 30820128 A0030201 0202010A 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35333032
31313630 345A170D 30373035 33303231 31363034 5A302A31 28301206 03550405
130B4648 4B303930 37463050 47301206 092A8648 86F70D01 09021605 616B6173
68305C30 0D06092A 864886F7 0D010101 0500034B 00304802 4100A6AD 0A376A6C
9EB668CC D0DF2A17 180E6CA2 FA5F243B 861EAA29 BE5FC488 A22AD4E8 5DFC22AC
13B43337 2F9FBA64 14E838EA 888E79DE 93AB63E4 4B4E2ECD 256D0203 010001A3
4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 14B54182
87D061FE 277C9A18 62B3673B F7F70E47 DD301D06 03551D0E 04160414 34D2D41C
274AB6E3 71A3A32C EC19D533 D3C0A020 300D0609 2A864886 F70D0101 04050003
818100A2 3947B1D0 FC5E9B79 0C1A28E7 BCB34C6C BB68C5F6 356F3F61 7525053E
0AED7325 9F286888 887810A6 B62FBAF3 BDC81542 C9828BBF 6A9FE936 AD3ED33B
D4F5AD22 E703C8E0 C3DDEAC8 2097A209 542551F7 6340A2A4 55A25A99 6A87367F
A0CBD9B6 E38D5E40 6479EB71 EFA644B3 93222D6F 235039AE BB9AA7B7 B1D07B3C FC6339
quit
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BF AFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC

```

```

7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
!
!
voice service voip
!
!
interface FastEthernet0/0
ip address 10.4.177.53 255.255.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 1.4.0.1
!
ip http server
no ip http secure-server
!
no cdp advertise-v2
!
!
control-plane
!
!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
!
voice-port 2/4
!
.
.
.
!
voice-port 2/23
!
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.177.51 identifier 1 version 4.0
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
!
dial-peer voice 5001 pots
service stcapp
port 2/0
!
dial-peer voice 5002 pots
service stcapp

```

The following line shows the security mode configured on the dial peer:

```
security mode authenticated
port 2/1
!
dial-peer voice 5003 pots
service stcapp
security mode none
port 2/2
!
dial-peer voice 2000 voip
destination-pattern 7...
session target ipv4:10.4.177.100
incoming called-number 7000
codec g711ulaw
!
dial-peer voice 1 pots
!
dial-peer voice 5004 pots
service stcapp
shutdown
port 2/3
!
dial-peer voice 5005 pots
shutdown
destination-pattern 3001
port 2/4
!
.
.
.
!
dial-peer voice 5018 pots
service stcapp
shutdown
port 2/17
!
dial-peer voice 2001 pots
destination-pattern 2001
port 2/18
!
dial-peer voice 1000 voip
destination-pattern 1...
session target ipv4:10.3.105.5
!
dial-peer voice 5900 voip
destination-pattern 59..
session target ipv4:10.3.105.5
!
dial-peer voice 500 voip
destination-pattern 5...
session target ipv4:10.4.177.51
!
dial-peer voice 5019 pots
service stcapp
shutdown
port 2/18
!
dial-peer voice 5020 pots
service stcapp
shutdown
port 2/19
!
.
```

```
.  
. !  
dial-peer voice 5024 pots  
service stcapp  
shutdown  
port 2/23  
!  
!  
!  
line con 0  
transport output all  
line aux 0  
transport output all  
line vty 0 4  
password lab  
login  
transport input all  
transport output all  
!  
ntp clock-period 17179541  
ntp server 10.4.177.51  
end
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager documentation
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express documentation
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series documentation • Cisco 1800 Series Integrated Services Routers documentation • Cisco 2800 Integrated Services Routers documentation • Cisco 3800 Series Integrated services Routers documentation • Cisco Unified 500 Series documentation
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Secure Signaling and Media Encryption for the Cisco VG224

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(20)YA or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information**

Feature Name	Releases	Feature Information
Secure Signaling and Media Encryption for the Cisco VG224	12.4(11)XW	<p>Provides secure voice call capabilities for analog phones that are connected to FXS ports on a Cisco VG224 Analog Phone Gateway and controlled by Cisco Unified CME.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Media Encryption (SRTP), page 194 How to Configure Secure Signaling and Media Encryption for the Cisco VG224, page 195



Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager

First Published: November 19, 2010

Last Updated: June 29, 2015

This module describes how the Secure Skinny Client Control Protocol (SCCP) enhances SCCP telephony control (STC) application (STCAPP) Foreign Exchange Station (FXS) security analog endpoints through secure signaling and media encryption using Transport Layer Security (TLS). This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified Communications Manager (Cisco Unified CM) only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM”](#) section on page 224.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 214](#)
- [Restrictions for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 214](#)
- [Benefits of Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 214](#)
- [Information About Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 215](#)
- [How to Configure Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 217](#)
- [Configuration Examples for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 221](#)
- [Additional References, page 222](#)

- [Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 224](#)

Prerequisites for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Secure SCCP Analog Endpoints over TLS with Cisco Unified CM require the following software component:

- Cisco Unified CM 8.5 or later

Cisco IOS Voice Gateway

- Cisco IOS Release 15.1(3)T or a later version
- Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- Analog FXS voice ports are set up and configured for operation. For information, see [Cisco IOS Voice Port Configuration Guide](#).
- SCCP and the STCAPP are enabled on the Cisco voice gateway. For configuration information, see [Configuring FXS Ports for Basic Calls](#).

Restrictions for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

- This feature supports only the following Cisco IOS platforms:
 - Cisco ISR 1861/2801/2811/2821/2851/3825/3845
 - Cisco ISR G2 2901/2911/2921/2951/3925/3945/3925E/3945E
 - Cisco VG202/VG204/VG224
- If you have an existing Non-secure SCCP Gateway, you will not be able to reconfigure it as Secure in CUCM.

Benefits of Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

The Secure SCCP enhances STCAPP FXS analog endpoints through signaling integrity and media encryption using TLS and Secured Real-time Transport Protocol (SRTP) with Cisco Unified CM.

This feature provides parity with incumbent time-division multiplexing systems.

Information About Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concept:

- [Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 215](#)

Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

In a nonsecure Cisco Unified CM-gateway environment, the SCCP connection between the Cisco Unified CM and the Cisco IOS Voice Gateway is established through a TCP connection on port 2000 and media between the gateway and the Cisco Unified CM is RTP. Since these connections are not encrypted, hackers create damage by disrupting signaling or by listening to the media connection.

The Secure SCCP over TLS feature enhances STCAPP security endpoints by using an existing Cisco IOS Public Key Infrastructure (PKI) to manage security certificates on Cisco IOS Voice Gateways and connect to the Cisco Unified CM.

This feature aims to provide call signaling integrity and media encryption in the IP telephony environment through the following:

- [SCCP signaling authentication, integrity and encryption using TLS, page 215](#)
- [Media protection by SRTP, page 216](#)

SCCP signaling authentication, integrity and encryption using TLS

Dynamic, secure SCCP signaling per media channel instead of secure signaling through the IPSEC tunnel, which is complex to configure in large-scale deployments, complements the secure media through SRTP and avoids the complexity necessary to setup static IPSEC tunnels.

Signaling can be secured by implementing a secure TLS connection between multiple IOS SCCP Analog Voice Gateways and the Cisco Unified CM through the following steps:

- Establish an identity for the STCAPP by getting a digital security certificate (that contains public keys used for encryption and digital signatures) from a root Certificate Authority (CA) server used by both the Cisco Unified CM and the STCAPP.

**Note**

Since the gateway is running the Cisco IOS with a PKI subsystem there is no need for a proxy function called the Certificate Authority Proxy Function (CAPF) to issue certificates. For Cisco Unified CM, any third-party CA supporting standards based on the Simple Certificate Exchange Protocol (SCEP) or a dedicated Cisco IOS router acts as a CA server. The Cisco Unified CM can also get a certificate from the Cisco IOS CA server using built-in support to manually request and import certificates from external CAs. Each Cisco IOS Voice Gateway receives its own security certificate from the Cisco IOS CA server through PKI autoprovisioning to allow large-scale deployments.

- Establish an identity for the gateway and Cisco Unified CM by getting a certificate from the same root CA. The TLS uses a standard handshake with mutual authentication. The gateway and the Cisco Unified CM authenticate each other by exchanging and validating the certificates during the TLS handshake. In addition to the standard TLS handshake, the Cisco Unified CM also examines the device name or MAC address from the gateway's certificate Subject field.

**Note**

Registration is rejected and an error message indicating a mismatch in the configuration is received when a secure gateway attempts to register with a nonsecure Cisco Unified CM or a nonsecure gateway attempts to register with a secure Cisco Unified CM.

Theoretically, up to 24 certificates can be issued to each of the 24 analog phones on the Cisco VG224 Voice Gateway. However, only one certificate is issued to a single VG224 box with all the analog phones sharing this certificate while establishing TLS connection to the Cisco Unified CM. The reasons for this are:

- Each analog port with its own certificate consumes a large amount of NVRAM memory, which is limited on Cisco IOS platforms.
- There is no significant enhancement in security with individual certificates for each analog port because of the single data path between Cisco Unified CM and the gateway.

Media protection by SRTP

SRTP is used to encrypt the call control signaling and the media streams from one end to the other for IP endpoints. For media encryption, the two analog endpoints controlled by the Cisco Unified CM exchange keys used to encrypt and decrypt the call control signaling packets. The transmission end has a key (tx key) used to encrypt the packets while the receiving end has a similar key (rx key) required to decrypt the packets. To decrypt the packets properly, the receiving end's "rx key" must be similar to the transmitter's "tx key".

Media protection involves the following:

- [Security keys generation and the distribution, page 216](#)
- [Media security through digital signal processor \(DSP\) programming using security keys, page 216](#)

Security keys generation and the distribution

The security keys are generated at the Cisco Unified CM and distributed to the SCCP analog endpoints as part of the SCCP signaling messages over the TLS protocol.

Media security through digital signal processor (DSP) programming using security keys

The SCCP FXS analog endpoints using the PVDM2 and PVDM3 packet voice DSP modules are supported.

To achieve media security through SRTP with secure capable end points, the SRTP keys are exchanged before the media really starts or the commands are sent to the endpoints.

The DSP is programmed by the Cisco IOS to use SRTP after the DSP is put in voice mode. A DSP channel (associated with a call leg) toggles from secure to nonsecure modes and vice versa when supplementary services are used. The DSP is reprogrammed based on the instructions from the application. The reprogramming of the DSP occurs after the DSP is reset and put in voice mode.

How to Configure Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

**Note**

This document does not contain details about configuring Cisco Unified CM or an IOS CA server. See the documentation for these products for installation and configuration instructions.

To enable dynamic, secure SCCP signaling to complement secure media through SRTP on a Cisco voice gateway connected to a Cisco Unified CM, perform the following tasks:

- [Creating a Trustpoint on a Cisco IOS Voice Gateway, page 217](#)
- [Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 220](#)

Creating a Trustpoint on a Cisco IOS Voice Gateway

To create a security trustpoint on a Cisco IOS gateway, perform the following steps:

**Note**

While using Cisco Voice Gateway 3xx Series (VG 310, VG 320, VG 350), activate securityK9 licenses for enabling secure SRTP Calls.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **serial-number** [none]
6. **fqdn** [*name* | none]
7. **ip-address** none
8. **subject-name** cn=*AA:BB:CC:DD:EE*
9. **revocation-check** [none]
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint label Example: Router(config)# crypto pki trustpoint VG224	Specifies a trustpoint that your registration authority mode certificate server should use and enters CA-trustpoint configuration mode. <ul style="list-style-type: none"> <i>label</i>—Name for the trustpoint and registration authority.
Step 4	enrollment url ca-url Example: Router(ca-trustpoint)# enrollment url http://1.4.32.7:80	Specifies the enrollment URL of the issuing CA certificate server (root certificate server). <ul style="list-style-type: none"> <i>ca-url</i>—URL of the router on which the root CA has been installed.
Step 5	serial-number [none] Example: Router(ca-trustpoint)# serial-number none	Specifies whether the router serial number should be included in the certificate request. <ul style="list-style-type: none"> none—(Optional) Specifies that a serial number will not be included in the certificate request.
Step 6	fqdn [name none] Example: Router(ca-trustpoint)# fqdn none	Specifies a fully qualified domain name to be included in the certificate request. <ul style="list-style-type: none"> <i>name</i>—FQDN that will be included as “unstructured Name” in the certificate request. none—Router FQDN will not be included in the certificate request.
Step 7	ip-address none Example: Router(ca-trustpoint)# ip-address none	Specifies a dotted IP address or an interface to be included as “unstructuredAddress” in the certificate request. <ul style="list-style-type: none"> none—Specifies that an IP address is not to be included in the certificate request.
Step 8	subject-name cn=AA:BB:CC:DD:EE Example: Router(ca-trustpoint)# subject-name cn=11:22:22:11:11	Specifies the subject name in the certificate request. <ul style="list-style-type: none"> cn=AA:BB:CC:DD:EE—last 10 digit of SCCP Interface MAC address

	Command or Action	Purpose
Step 9	revocation-check [none] Example: Router(ca-trustpoint)# revocation-check none	Checks the revocation status of a certificate and specifies a method to check the status. <ul style="list-style-type: none"> • none—(Optional) Certificate checking is not required.
Step 10	exit Example: Router(config)# exit	Exits CA-trustpoint configuration mode.

Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified CM



Note

This document does not contain details about configuring STCAPP. For more information, see the [“Enabling SCCP on the Voice Gateway” section on page 21](#).

To configure secure SCCP analog endpoints, perform the following steps on the Cisco IOS voice gateway:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp security trustpoint *line***
4. **stcapp security mode {authenticated | encrypted | none}**
5. **stcapp**
6. **dial-peer voice *tag pots***
7. **security mode [authenticated | encrypted | none]**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	stcapp security trustpoint <i>line</i> Example: Router(config)# stcapp security trustpoint VG204	Enables security for STCAPP endpoints and specifies the trustpoint to be used for setting up the TLS connection. <ul style="list-style-type: none"> • <i>line</i>—Security trustpoint for the STCAPP endpoint.

	Command or Action	Purpose
Step 4	<pre>stccapp security mode {authenticated encrypted none}</pre> <p>Example: Router(config)# stccapp security mode encrypted</p>	<p>Enables STCAPP endpoints and specifies the global security mode to be used for setting up the TLS connection.</p> <ul style="list-style-type: none"> authenticated—Security mode is authenticated and enables SCCP signaling between the voice gateway and the Cisco Unified CM through the secure TLS connection. encrypted—Security mode is encrypted. STCAPP endpoints are encrypted using data encryption through SRTP. none—Security mode is disabled. Defaults to global configuration mode.
Step 5	<pre>stccapp</pre> <p>Example: Router(config)# stccapp</p>	<p>Enables the STCAPP feature.</p> <p>Note Both the stccapp security trustpoint and the stccapp security mode must be entered to enable security for the STCAPP endpoints.</p>
Step 6	<pre>dial-peer voice tag pots</pre> <p>Example: Router(config)# dial-peer voice 1 pots</p>	<p>(Optional) Enters dial peer voice configuration mode.</p> <ul style="list-style-type: none"> tag—Digits that define a particular dial peer. Range: 1 to 2147483647. pots—Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
Step 7	<pre>security mode [authenticated encrypted none]</pre> <p>Example: Router(config-dialpeer)# security mode encrypted</p>	<p>(Optional) Enables dial-peer level STCAPP endpoint security and overrides global configuration.</p> <ul style="list-style-type: none"> authenticated—Enables STCAPP endpoints using signaling authentication. encrypted—Enables STCAPP endpoints using data encryption. none—Disables dial-peer-level STCAPP endpoint security configuration and defaults to global level configuration.
Step 8	<pre>end</pre> <p>Example: Router(config-dialpeer)# end</p>	<p>Exits dial-peer configuration mode and returns to privileged EXEC mode.</p>

Configuration Examples for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

This section provides the following configuration examples:

- [Example: Configuring a Cisco IOS CA Server, page 222](#)
- [Example: Configuring a Cisco IOS VG224 Voice Gateway, page 222](#)

Example: Configuring a Cisco IOS CA Server

The following example shows how to configure a Cisco IOS CA server, where the IP address of the CA server is entered as the enrollment url:

```
Router# show run
.
.
.
crypto pki server cserver1
 grant auto
!
crypto pki trustpoint cserver1
 enrollment url http://1.4.32.7:80
 revocation-check crl
 rsakeypair cserver1
```

Example: Configuring a Cisco IOS VG224 Voice Gateway

The following example shows how to configure a Cisco IOS VG224 Voice Gateway, where the IP address of the CA server is entered as the enrollment url:

```
Router# show run
.
.
.
crypto pki trustpoint VG224
 enrollment url http://1.4.32.7:80
 serial-number none
 fqdn none
 ip-address none
 mac-address FastEthernet0/0
 revocation-check none
!
stcapp security trustpoint VG224
stcapp security mode encrypted
stcapp
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> • Cisco VG200 Series Gateway • Cisco 1800 Series Integrated Services Routers • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated services Routers • Cisco Unified 500 Series
Conferencing and transcoding resources	<ul style="list-style-type: none"> • “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter in the Cisco Unified CallManager and Cisco IOS Interoperability Guide. • Cisco CallManager and IOS Gateway DSP Farm Configuration Example

RFCs

RFC	Title
RFC 2246	The TLS Protocol Version 1.0

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Feature Name	Releases	Feature Information
Secure SCCP Analog Endpoints over TLS with Cisco Unified CM	15.1(3)T	<p>Enhances STCAPP FXS security analog endpoints through secure signaling and media encryption using TLS. This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified CM only.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 215 How to Configure Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 217. <p>No new commands were introduced by this feature.</p>



Implementing Enhanced Serviceability

First Published: November 19, 2010

This module describes how to perform line tests and connectivity checks on analog Foreign Exchange Station (FXS) voice ports using the Enhanced Serviceability features.

The Enhanced Serviceability feature provides analog FXS line measurement support for analog voice ports that use Infineon Vinetic PEB3304HL or Silicon Lab Pro SLIC si3241 chipset. The analog FXS line measurements supported by this feature include:

- AC/DC line voltage
- AC/DC foreign voltage
- AC/DC transversal and longitudinal current
- AC/DC current
- AC ring voltage
- AC ring current
- Loop resistance
- REN detection
- Receiver offhook detection
- Analog phone detection

The Enhanced Serviceability feature also provides digital signal processor (DSP)-level signaling and media connectivity checks of analog FXS voice ports. The feature enables troubleshooting of large deployments by cyclically establishing test calls to each port in the gateway.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Enhanced Serviceability”](#) section on page 244.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Enhanced Serviceability, page 226](#)
- [Information About Enhanced Serviceability, page 226](#)
- [How to Configure Enhanced Serviceability Features on Analog Voice Gateways, page 229](#)
- [Configuration Examples for Enhanced Serviceability, page 242](#)
- [Additional References, page 243](#)
- [Feature Information for Enhanced Serviceability, page 244](#)

Prerequisites for Enhanced Serviceability

- Cisco IOS Release 15.1(3)T or a later version.
- The Cisco voice gateway (VG) is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- The analog FXS voice ports are set up and configured for operation. For information, see [Cisco IOS Voice Port Configuration Guide](#).
- The analog FXS voice ports must use the Vinetic chipset version 2.1 from Infineon Technologies or the Pro SLIC Si3241 chipset from Silicon Laboratories.
- Cisco Unified Communications Manager 6.1.2 or a later version.

Information About Enhanced Serviceability

To configure the Cisco voice gateway to implement the enhanced serviceability features, you should understand the following concepts:

- [Benefits of Analog FXS Line Measurements, page 227](#)
- [Benefits of Analog FXS Connectivity Checks, page 227](#)
- [Supported Gateways, Modules, and Voice Interface Cards, page 228](#)

Benefits of Analog FXS Line Measurements

Analog FXS Line Measurements are a set of tests used to monitor and diagnose a variety of failures in voice gateways. These tests involve measurements of resistance, capacitance, leakage, and interfering currents and voltages that reduce network quality.

Among the different types of line measurements that can be performed on analog FXS lines include the following:

- AC/DC line voltage – measures the voltage generated by the chip on tip-ring, tip-to-ground, and ring-to-ground
- AC/DC foreign voltage – it measures the unknown/dangerous voltage on tip-ring, tip-to-ground, and ring-to-ground
- AC/DC transversal and longitudinal current – measures the current on tip-ring (transversal) and tip/ring-to-ground (longitudinal)
- AC/DC current – measures the current on tip-ring, tip-to-ground and ring-to-ground
- Loop resistance – measures the resistance on tip-ring, tip-to-ground and ring-to-ground
- Ringer Equivalent Number (REN) detection – measures the REN required by the analog phone
- Receiver offhook detection – detects whether the port is in onhook or offhook state
- Analog phone detection – detects whether the analog phone is plugged in or not

Benefits of Analog FXS Connectivity Checks

Analog FXS connectivity checks are tests done on analog voice ports to verify signaling and media path quality. These tests can be implemented one port at a time or by cyclically establishing test calls to each port in a gateway which is critical in troubleshooting errors in large deployments.

Among the different types of connectivity tests that can be performed using analog FXS connectivity checks include the following:

- Sequential verification of end-to-end connectivity for signalling and media for each VG end-point through test calls from each end-point to a test verification phone
- Sequential verification of end-to-end connectivity after an image upgrade or image change
- Sequential verification of end-to-end connectivity after of a specific port during troubleshooting of voice quality issues
- Verification of full-duplex connectivity by putting the end-point in loopback so that any digit depressed by the test verification phone is relayed back to the VG

Supported Gateways, Modules, and Voice Interface Cards

Table 1 lists Cisco voice gateways, modules, and voice interface cards (VICs) on which line measurements for FXS ports are supported

Table 1 Gateways, Modules, VICs and their Supported Line Measurements

Voice Port chipset	Gateways	Modules and VICs	Supported Line Measurements
<ul style="list-style-type: none"> Infineon Vinitic PEB3304HL 	<ul style="list-style-type: none"> Cisco VG224 Analog Voice Gateway Cisco IAD2430 Integrated Access Device 	—	<ul style="list-style-type: none"> AC/DC voltage AC ring voltage AC/DC foreign voltage AC/DC current AC ring current Loop resistance REN detection Phone detection
<ul style="list-style-type: none"> Silicon Lab Pro SLIC si3241 	<ul style="list-style-type: none"> Cisco VG202 Analog Voice Gateway Cisco VG204 Analog Voice Gateway Cisco Unified Communications 500 Series Cisco 880 Integrated Services Router (ISR) Other ISR platforms that support Tenor VIC and EM V3-8FXS-DID modules (e.g. C28xx, C29xx, C38xx, C39xx) 	<ul style="list-style-type: none"> Venom EM V3-8FXS-DID 3 Tenor FXS VICs Onboard analog FXS on VG202 and VG204 platforms Onboard analog FXS on C880 platform Onboard analog FXS on UC500 platform 	<ul style="list-style-type: none"> AC/DC foreign voltage AC/DC current Loop resistance REN detection Receiver Off-hook detection Phone detection

Table 2 lists Cisco voice gateways, modules, and VICs on which connectivity checks for FXS ports are supported.

Table 2 *Gateways, Modules, VICs and their Supported Connectivity Checks*

Gateways	Modules and VICs	Supported Connectivity Checks
All ISR platforms that support analog FXS voice ports	—	<ul style="list-style-type: none"> • Tone Originate • Tone Terminate • COT

How to Configure Enhanced Serviceability Features on Analog Voice Gateways



Note This document does not contain details about configuring Cisco Unified CM. See the documentation for this products for installation and configuration instructions.

This section contains the following procedures:

- [Performing Analog FXS Line Measurements on Voice Ports Using Vinetic PEB3304HL Chipsets, page 229](#)
- [Performing Analog FXS Line Measurements on Voice Ports Using Pro SLIC si3241 Chipsets, page 232](#)
- [Performing Connectivity Checks on a Single Analog FXS Port, page 234](#)
- [Performing Connectivity Checks on All Analog FXS Ports in a Router, page 239](#)

Performing Analog FXS Line Measurements on Voice Ports Using Vinetic PEB3304HL Chipsets

The onboard voice ports on the Cisco VG224 Analog Voice Gateway and the Cisco IAD2430 Integrated Access Device use the Vinetic PEB3304HL chipset from Infineon Technologies AG. The chipset has a set of integrated test and diagnostic functions that can perform various line measurements.

Prerequisites

The line measurements described in this task are only supported in the Vinetic PEB3304HL chipset version 2.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port 2/port**
4. **shutdown**
5. **end**
6. **test voice port 2/port line-test type-of-line-test**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-port 2/port Example: Router(config)# voice-port 2/2	Enters voice-port configuration mode. <ul style="list-style-type: none"> • 2/port—The address of the port to be tested.
Step 4	shutdown Example: Router(config-voiceport)# shutdown	Takes the specified voice port offline and triggers deregistration of the device with Cisco Unified Communications Manager.
Step 5	end Example: Router(config-voiceport)# end	Exits the voice port configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
<p>Step 6</p> <pre>test voice port 2/port line-test dc-voltage or test voice port 2/port line-test ac-voltage or test voice port 2/port line-test ac-ring-voltage or test voice port 2/port line-test dc-foreign-voltage or test voice port 2/port line-test ac-foreign-voltage or test voice port 2/port line-test dc-current or test voice port 2/port line-test ac-current or test voice port 2/port line-test ac-ring-current or test voice port 2/port line-test loop-resistance or test voice port 2/port line-test REN-detection or test voice port 2/port line-test phone-detection</pre>	<p>Example: Router# test voice port 2/1 line-test phone-detection</p>	<p>Measures the DC voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the AC voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the AC ring voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>Note The analog phone is rung.</p> <p>or</p> <p>Measures the DC foreign voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the AC foreign voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the DC Transversal and Longitudinal current generated by the specified port.</p> <p>or</p> <p>Measures the AC Transversal and Longitudinal current generated by the specified port.</p> <p>or</p> <p>Measures the AC ring current generated by the specified port between tip-ring.</p> <p>Note The analog phone is rung.</p> <p>or</p> <p>Measures the loop resistance generated by the specified port between tip-ring.</p> <p>or</p> <p>Measures the REN value on the specified port.</p> <p>Note The analog phone is rung.</p> <p>or</p> <p>Checks if there is a phone connected to the specified port.</p> <p>Note The analog phone is rung silently.</p>
		<ul style="list-style-type: none"> • <i>2/port</i>—The address of the port to be tested.

What to Do Next

To perform analog FXS line measurements on analog voice ports that uses Silicon Lab Pro SLIC si3241 chipset, proceed to the [“Performing Analog FXS Line Measurements on Voice Ports Using Pro SLIC si3241 Chipsets”](#) section on page 232.

Performing Analog FXS Line Measurements on Voice Ports Using Pro SLIC si3241 Chipsets

The onboard voice ports on the Cisco VG202/204 Analog Voice Gateway, Cisco Unified Communications 500 Series, C880 module, Venom EM V3-8FXS-DID, and Tenor FXS VICs use the Pro SLIC si3241 chipset from Silicon Laboratories. The chipset includes functionalities for performing various line fault testing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *slot-number/subunit-number/port*
4. **shutdown**
5. **end**
6. **test voice port** *slot-number/subunit-number/port line-test type-of-line-test*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-port <i>slot-number/subunit-number/port</i> Example: Router(config)# voice-port 1/1/1	Enters voice-port configuration mode. <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested.
Step 4	shutdown Example: Router(config-voiceport)# shutdown	Takes the specified voice port offline and triggers deregistration of the device with Cisco Unified Communications Manager.

	Command or Action	Purpose
Step 5	<code>end</code>	Exits the voice port configuration mode and returns to privileged EXEC mode.
	Example: Router(config-voiceport)# end	
Step 6	<pre>test voice port slot-number/subunit-number/port line-test dc-foreign-voltage or test voice port slot-number/subunit-number/port line-test ac-foreign-voltage or test voice port slot-number/subunit-number/port line-test dc-current or test voice port slot-number/subunit-number/port line-test ac-current or test voice port slot-number/subunit-number/port line-test loop-resistance or test voice port slot-number/subunit-number/port line-test REN-detection or test voice port slot-number/subunit-number/port line-test receiver-offhook-detection</pre>	<p>Measures the DC foreign voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the AC foreign voltage generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the DC current generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the AC current generated by the specified port on tip-ring, tip-to-ground, ring-to-ground.</p> <p>or</p> <p>Measures the loop resistance generated by the specified port between tip-ring.</p> <p>or</p> <p>Measures the REN value on the specified port.</p> <p>Note The analog phone is rung.</p> <p>or</p> <p>Checks if the phone connected to the specified port is onhook, offhook, or has a resistive fault on tip-ring.</p> <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested.
	Example: Router# test voice port 1/1/1 line-test receiver-offhook-detection	

What to Do Next

To perform analog FXS line measurements on analog voice ports that uses Vinetic PEB3304HL chipsets, proceed to the [“Performing Analog FXS Line Measurements on Voice Ports Using Vinetic PEB3304HL Chipsets”](#) section on page 229.

Performing Connectivity Checks on a Single Analog FXS Port

To test the signaling and media path quality of a single analog FXS port, the user needs to perform the following tasks:

- [Performing Tone Originate Checks on a Single Analog FXS Port, page 235](#)
- [Performing Tone Terminate Checks on a Single Analog FXS Port, page 236](#)
- [Performing Continuity Tests, page 237](#)

Performing Tone Originate Checks on a Single Analog FXS Port

To perform tone originate checks on a single port, the user needs 2 routers or 1 router and 1 phone on a Public Switched Telephone Network (PSTN). The user first issues a test CLI on the router where the port to be tested is located. The tested port then sends a call to a voice port/phone either on the other router or on a phone on a PSTN. The user answers the test call to check for the sound of 7 test tones. The user confirms hearing the test tones by pressing any key on the phone's digit pad. The user can also verify the signaling and media path quality by using a test equipment. The test is completed when the user places the phone onhook.

SUMMARY STEPS

1. **enable**
2. **test voice port** *slot-number/subunit-number/port connectivity tone originate phone-number*
3. Answer the test call.
4. Verify the test tones.
5. Confirm the sound of the test tones.
6. End connectivity check.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	test voice port slot-number/subunit-number/port connectivity tone originate phone-number Example: Router# test voice port 1/1/1 connectivity tone originate 4085251234	Tests the signaling and media path quality of a call originating from the tested port to the test phone number. <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested. <i>phone-number</i>—The number of port/phone on the other router or on a phone on a PSTN that receives the test call. <p>Note The user issues the command on the router where the port to be tested is located.</p> <p>The tested port then sends a call to a voice port/phone on the other router or on a phone on a PSTN.</p>
Step 3	Answer the test call.	The user answers the test call.
Step 4	Verify the test tone.	The user checks for the sound of 7 test tones, each lasting 1 second, on the test call.
Step 5	Confirm the sound of the test tones.	The user confirms hearing the test tones by pressing any key on the phone's digit pad. The user can also verify the signaling and media path quality by using a test equipment.
Step 6	End Connectivity check.	The user places the test call onhook to end the test.

Performing Tone Terminate Checks on a Single Analog FXS Port

To perform tone terminate checks on a single port, the user needs 2 routers or 1 router and 1 phone on a PSTN. The user first issues a test CLI on the router where the port to be tested is located. Using a phone on the other router or a phone on a PSTN, the user calls the voice port/phone to be tested. The tested port will then send 7 test tones to the calling party. The user confirms hearing the test tones by pressing any key on the phone's digit pad. The test is completed when the user places the phone onhook.

SUMMARY STEPS

- enable**
- test voice port slot-number/subunit-number/port connectivity tone terminate**
- Call the tested port.
- Verify the test tones.
- Confirm the sound of the test tones.
- End connectivity check.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	test voice port slot-number/subunit-number/port connectivity tone terminate Example: Router# test voice port 1/1/1 connectivity tone terminate	Configures the port to receive a test call from a test port/phone on another router or a phone on a PSTN. <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested.
Step 3	Call the tested port.	The user calls the voice port/phone to be tested using a phone on the other router or a phone on a PSTN. No ring is generated on the tested port. The tested port will then send 7 test tones to the calling party.
Step 4	Verify the test tone.	The user checks for the sound of 7 test tones, each lasting 1 second, on the test call.
Step 5	Confirm the sound of the test tones.	The user confirms hearing the test tones by pressing any key on the phone's digit pad.
Step 6	End Connectivity check.	The user places the test call onhook to end the test.

Performing Continuity Tests

To perform a Continuity Test (COT) on a single port, the user needs 2 routers. The user first issues a COT terminate command on the router where the first port to be tested for COT terminate is located. The user then issues a COT originate command on the other router where the port to be tested for COT originate is located. After the COT originate command is issued, the port tested for COT originate makes a test call to the port tested for COT terminate. The test proceeds automatically and the test call is disconnected after the test is done. The results of the test is displayed on the screen.

SUMMARY STEPS

- enable**
- test voice port slot-number/subunit-number/port connectivity cot terminate**
- test voice port slot-number/subunit-number/port connectivity cot originate phone-number**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>test voice port slot-number/subunit-number/port connectivity cot terminate</pre> <p>Example: Router# test voice port 1/1/1 connectivity cot terminate</p>	<p>Configures the port to receive a test call from a test port on another router.</p> <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested. <p>Note The command is issued on the router where the port to be tested for COT terminate is located.</p>
Step 3	<pre>test voice port slot-number/subunit-number/port connectivity cot originate phone-number</pre> <p>Example: Router# test voice port 2/2/2 connectivity cot originate 4085251234</p>	<p>Configures a port in another router to send a test call to the port that was configured for COT terminate.</p> <ul style="list-style-type: none"> <i>slot-number/subunit-number/port</i>—The address of the port to be tested. <i>phone-number</i>—The number of the phone that is connected to the port configured for COT terminate. <p>Note The command is issued on the router where the port to be tested for COT originate is located.</p>

What to Do Next

To perform connectivity checks on all analog FXS ports in a router, proceed to the [“Performing Connectivity Checks on All Analog FXS Ports in a Router”](#) section on page 239.

Performing Connectivity Checks on All Analog FXS Ports in a Router

To test the signaling and media path quality of all analog FXS ports in a router, the user needs to perform the following tasks:

- [Performing Tone Originate Connectivity Checks, page 239](#)
- [Performing Continuity Tests, page 240](#)
- [Displaying Results of Connectivity Checks, page 241](#)

Performing Tone Originate Connectivity Checks

To perform tone originate checks on all analog FXS ports in a router, the user needs 2 routers or 1 router and 1 phone on a PSTN. The user first issues a test CLI on the router where the ports to be tested are located. The CLI configures all analog FXS ports on the router to make a call one at a time to a specified phone on another router or to a phone on a PSTN. The user answers the test call to check for the sound of 7 test tones. The user confirms hearing the test tones by pressing any key on the phone's digit pad. The test is completed for one voice port when the user places the phone onhook. The next voice port on the router automatically makes a call to the specified number and the test process is repeated. The test is completed after all the ports in the router are tested.

SUMMARY STEPS

1. **enable**
2. **test voice port all connectivity tone originate** *phone-number*
3. Answer the test call.
4. Verify the test tones.
5. Confirm the sound of the test tones.
6. End connectivity check for the port.
7. Repeat steps 3 to 6 until the last port has been tested.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>test voice port all connectivity tone originate phone-number</code> Example: Router# test voice port all connectivity tone originate 4085251234	Configures all analog FXS ports on the router to make a call one at a time to a specified phone on another router or to a phone on a PSTN. <ul style="list-style-type: none"> <i>phone-number</i>—The number of the phone on another router or a phone on a PSTN that will receive the test calls from the tested ports. <p>Note The command is issued on the router where the ports to be tested for COT originate is located.</p>
Step 3	Answer the test call.	The user answers the test call.
Step 4	Verify the test tones.	The user checks for the sound of 7 test tones, each lasting 1 second, on the test call.
Step 5	Confirm the sound of the test tones.	The user confirms hearing the test tones by pressing any key on the phone's digit pad.
Step 6	End connectivity check for the port.	The test ends for each voice port when the user places the phone onhook.
Step 7	Repeat steps 3 to 6 until the last port has been tested.	The next voice port on the router automatically makes a call to the specified number and the test process is repeated. The test is completed after all the ports in the router are tested.

Performing Continuity Tests

To perform COT on all analog FXS ports in a router, the user needs 2 routers. The user first issues a test CLI on any voice port on the first router. The CLI configures the port to receive test calls and remain in COT receive mode after the test is complete. The user then issues a CLI on the other router. The CLI configures all ports on the router to make test calls one at a time to the port on the first router that is configured to accept test calls. The test proceeds automatically and the test result for each port is displayed after every call is completed. After all the ports have been tested, the user issues a CLI on the port receiving the test call to place the port back in to normal mode.

SUMMARY STEPS

- `enable`
- `test voice port slot-number/subunit-number/port connectivity cot terminate remain-in-test-mode`
- `test voice port all connectivity cot originate phone-number`
- `test voice port slot-number/subunit-number/port connectivity terminate-cancel`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>test voice port slot-number/subunit-number/port connectivity cot terminate remain-in-test-mode</code> Example: Router# test voice port 1/1/1 connectivity cot terminate remain-in-test-mode	Configures the port to receive test calls from all ports on another router and remain in COT receive mode after the test. • <i>slot-number/subunit-number/port</i> —The address of the port to be tested. Note The CLI is issued on the router where the port receiving the test calls is located.
Step 3	<code>test voice port all connectivity cot originate phone-number</code> Example: Router# test voice port all connectivity cot originate 4085251234	Configures all ports on another router to send a test call to the port that was configured for COT terminate. • <i>phone-number</i> —The number of the phone that is connected to the port configured to receive test calls. Note The CLI is issued on the router where the ports sending test calls is located.
Step 4	<code>test voice port slot-number/subunit-number/port connectivity terminate-cancel</code> Example: Router# test voice port 1/1/1 connectivity terminate-cancel	Places the port receiving the test calls back on normal mode. • <i>slot-number/subunit-number/port</i> —The address of the port to be tested. Note This CLI should only be used when all analog FXS ports have been tested.

Displaying Results of Connectivity Checks

Use this command to display the results of the last connectivity checks performed on all analog FXS ports on a router.

SUMMARY STEPS

1. `enable`
2. `show voice connectivity summary`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>show voice connectivity summary</code> Example: Router# show voice connectivity summary	Displays the results of the last connectivity checks performed on all analog FXS ports on a router.

What to Do Next

To perform connectivity checks on a single analog FXS port, proceed to the [“Performing Connectivity Checks on a Single Analog FXS Port”](#) section on page 234.

Configuration Examples for Enhanced Serviceability

This section provides the following configuration examples:

- [Example: Performing a DC Voltage Line Test on an Analog FXS Port, page 242](#)
- [Example: Performing a Connectivity Checks on an Analog FXS Port, page 242](#)

Example: Performing a DC Voltage Line Test on an Analog FXS Port

The following example shows a partial output of a DC Voltage line test performed on an analog FXS port using a Vinetic PEB3304HL chipset:

```
Router> enable
Router# configure terminal
Router(config)# voice-port 2/1
Router (config-voiceport)# shutdown
Router (config-voiceport)# end
!
! Performs a DC voltage line test on the specified voice port
Router# test voice port 2/1 line-test dc-voltage
Router#
    DC voltage measurement between tip-ring: xx.xx V
    DC voltage measurement on tip-to-ground: xx.xx V
    DC voltage measurement on ring-to-ground: xx.xx V
```

Example: Performing a Connectivity Checks on an Analog FXS Port

The following example shows a partial output of a COT performed on all analog FXS ports in a router:

```
Router> enable
!
! Configure the port to receive test calls from all analog voice ports on another router
Router# test voice port 1/1/1 connectivity cot terminate remain-in-test-mode
!
```

```

! Configure all analog voice ports to send test calls to the port/phone configured to
! receive test calls
Router# test voice port all connectivity cot originate 4085251234
.
.
.
! End the COT terminate CLI and place the terminated port back to normal mode.
Router# test voice port 1/1/1 connectivity terminate-cancel

```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	Cisco Unified Communications Manager
Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express
Cisco IOS debugging	Cisco IOS Debug Command Reference
Cisco IOS voice commands	Cisco IOS Voice Command Reference
Cisco IOS voice configuration	Cisco IOS Voice Configuration Library
Cisco voice gateway	<ul style="list-style-type: none"> Cisco VG200 Series Gateways Cisco Unified 500 Series for Small Business

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Enhanced Serviceability

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Supplementary Services Features Roadmap](#)” section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Enhanced Serviceability

Feature Name	Releases	Feature Information
Enhanced Serviceability	15.1(3)T	<p>Provides line measurement and connectivity check support for analog voice ports.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Enhanced Serviceability, page 226 • How to Configure Enhanced Serviceability Features on Analog Voice Gateways, page 229. <p>The following commands were introduced or modified: show voice connectivity summary.</p>