



Cisco UBE Standards Compliance Configuration Guide, Cisco IOS Release 12.4

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Cisco Unified Border Element Standards Compliance	1
Finding Feature Information	1
Cisco Unified Border Element Cisco UBE Standards Compliance Features	1
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	3
Finding Feature Information	3
Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers	4
Modem Passthrough over VoIP	4
Prerequisites for the Modem Passthrough over VoIP Feature	5
Restrictions for the Modem Passthrough over VoIP Feature	6
How to Configure Modem Passthrough over VoIP	6
Configuring Modem Passthrough over VoIP Globally	7
Configuring Modem Passthrough over VoIP for a Specific Dial Peer	8
Verifying Modem Passthrough over VoIP	10
Troubleshooting Tips	11
Monitoring and Maintaining Modem Passthrough over VoIP	11
Configuration Examples	11
Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers	13
SIP RFC 2782 Compliance with DNS SRV Queries	15
Finding Feature Information	15
Prerequisites SIP RFC 2782 Compliance with DNS SRV Queries	15
Information SIP RFC 2782 Compliance with DNS SRV Queries	16
How to Configure SIP-RFC 2782 Compliance with DNS SRV Queries	16
Configuring DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries	16
Verifying	17
Feature Information for SIP RFC 2782 Compliance with DNS SRV Queries	18
Additional References	21
Related Documents	21
Standards	22
MIBs	22

[RFCs](#) 23

[Technical Assistance](#) 24

[Glossary](#) 25



Cisco Unified Border Element Standards Compliance

This Cisco Unified Border Element is a special Cisco IOS software image that provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.



Note

Cisco Product Authorization Key (PAK)--A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL <http://www.cisco.com/go/license> .

- [Finding Feature Information, page 1](#)
- [Cisco Unified Border Element Cisco UBE Standards Compliance Features, page 1](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Cisco Unified Border Element Cisco UBE Standards Compliance Features

This chapter contains the following configuration topics:

Cisco UBE Prerequisites and Restrictions

- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

Cisco UBE Standards Compliance

- ENUM Support (RFC2916)
- SIP--RFC 2782 Compliance with DNS SRV Queries
- SIP - DNS SRV RFC2782 Compliance

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft
- Lawful Intercept
- Media Inactivity
- [Modem Passthrough over VoIP, page 4](#)
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

- [Finding Feature Information, page 3](#)
- [Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers, page 4](#)
- [Modem Passthrough over VoIP, page 4](#)
- [Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers, page 13](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets.

The Modem Passthrough over VoIP feature performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under *normal* network conditions.

For further details, the functions of the Modem Passthrough over VoIP feature are described in the following sections.

Modem Tone Detection

The gateway is able to detect modems at speeds up to V.90.

Passthrough Switchover

When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before switchover. You can configure the codec by selecting the **g711alaw** or **g711ulaw** option of the **codec** command.

See also the [How to Configure Modem Passthrough over VoIP, page 6](#) section in this document.

Controlled Redundancy

You can enable payload redundancy so that the Modem Passthrough over VoIP switchover causes the gateway to emit redundant packets.

Packet Size

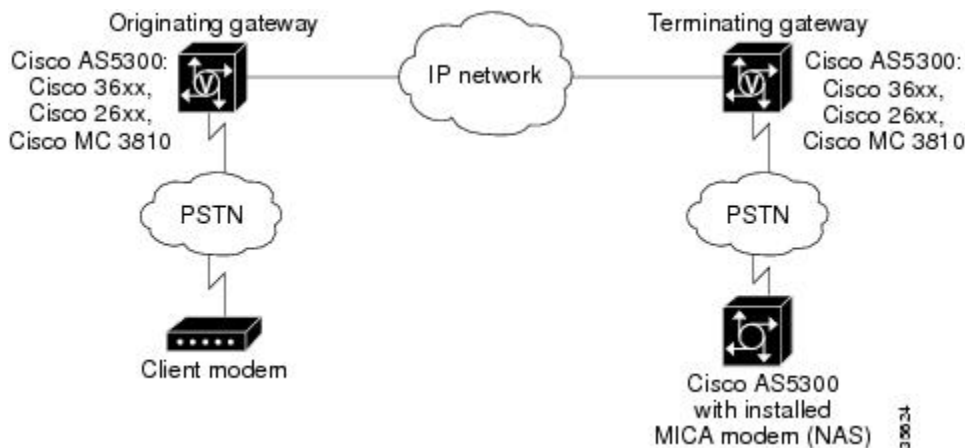
When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Clock Slip Buffer Management

When the gateway detects a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating gateway and the terminating gateway. At the conclusion of the modem call, the voice ports revert to dynamic jitter buffers.

The figure below illustrates the connection from the client modem to a MICA technologies modem network access server (NAS).

Figure 1 *Modem Passthrough Connection*



- [Prerequisites for the Modem Passthrough over VoIP Feature, page 5](#)
- [Restrictions for the Modem Passthrough over VoIP Feature, page 6](#)
- [How to Configure Modem Passthrough over VoIP, page 6](#)
- [Configuring Modem Passthrough over VoIP Globally, page 7](#)
- [Configuring Modem Passthrough over VoIP for a Specific Dial Peer, page 8](#)
- [Verifying Modem Passthrough over VoIP, page 10](#)
- [Troubleshooting Tips, page 11](#)
- [Monitoring and Maintaining Modem Passthrough over VoIP, page 11](#)
- [Configuration Examples, page 11](#)

Prerequisites for the Modem Passthrough over VoIP Feature

- VoIP enabled network.

- Cisco IOS Release 12.1(3)T must run on the gateways for the Modem Passthrough over VoIP feature to work.
- Network suitability to pass modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS feature Service Assurance Agent.

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for the Modem Passthrough over VoIP Feature

Cisco Unified Border Element (Enterprise)

- If call started as g729, upon modem tone (2100Hz) detection both the outgoing gateway (OGW) and the trunking gateway (TGW) will generate NSE packets towards peer side and up speed to g711 as Cisco UBE(Enterprise) passes these packets to the peer side.



Note

That OGW and TGW display the new codec, but the Cisco UBE (Enterprise) continues to show the original codec g729 in the show commands.

How to Configure Modem Passthrough over VoIP

By default, modem passthrough over VoIP capability and redundancy are disabled.



Tip

You need to configure modem passthrough in both the originating gateway and the terminating gateway for the Modem Passthrough over VoIP feature to operate. If you configure only one of the gateways in a pair, the modem call will not connect successfully.

Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets.

See the following sections for the Modem Passthrough over VoIP feature. The two configuration tasks can configure separately or together. If both are configured, the dial-peer configuration takes precedence over the global configuration. Consequently, a call matching a particular dial-peer will first try to apply the modem passthrough configuration on the dial-peer. Then, if a specific dial-peer is not configured, the router will use the global configuration:

Configuring Modem Passthrough over VoIP Globally

For the Modem Passthrough over VoIP feature to operate, you need to configure modem passthrough in both the originating gateway and the terminating gateway so that the modem call matches a voip dial-peer on the gateway.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem passthrough with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match.

To configure the Modem Passthrough over VoIP feature for all the connections of a gateway, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **voice service voip**
3. **modem passthrough nse** [payload-type *number*] codec {g711ulaw | g711alaw} [redundancy] [maximum-sessions *value*]
4. **exit**
5. **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 voice service voip Example: Router(config)# voice service voip	Enters voice-service configuration mode. Configures voice service for all the connections for the gateways.

Command or Action	Purpose
<p>Step 3 <code>modem passthrough nse [payload-type number] codec {g711ulaw g711alaw} [redundancy] [maximum-sessions value]</code></p> <p>Example:</p> <pre>Router(config)# Router(conf-voi-serv)# modem passthrough nse payload-type 97 codec g711alaw redundancy maximum-sessions 3</pre>	<p>Configures the Modem Passthrough over VoIP feature. The default behavior is no modem passthrough.</p> <p>The payload type is an optional parameter for the nse keyword. Use the same payload-type number for both the originating gateway and the terminating gateway. The payload-type number can be set from 96 to 119. If you do not specify the payload-type number, the number defaults to 100. When the payload-type is 100, and you use the show running-config command, the payload-type parameter does not appear.</p> <p>Use the same codec type for both the originating gateway and the terminating gateway. g711ulaw codec is required for T1, and g711alaw codec is required for E1.</p> <p>The redundancy keyword is an optional parameter for sending redundant packets for modem traffic.</p> <p>The maximum-sessions keyword is an optional parameter for the redundancy keyword. This parameter determines the maximum simultaneous modem passthrough sessions with redundancy.</p>
<p>Step 4 <code>exit</code></p> <p>Example:</p> <pre>Router(conf-voi-serv)# exit</pre>	<p>Exits voice-service configuration mode.</p>
<p>Step 5 <code>exit</code></p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>

Configuring Modem Passthrough over VoIP for a Specific Dial Peer

You can configure the Modem Passthrough over VoIP feature on a specific dial peer in two ways, as follows:

- Globally in the voice-service configuration mode
- Individually in the dial-peer configuration mode on a specific dial peer

The default behavior for the voice-service configuration mode is **no modem passthrough**. This default behavior implies that modem passthrough is disabled for all dial peers on the gateway by default.

To enable Modem Passthrough on the VoIP dial peers on both the originating and terminating gateway, configure modem passthrough globally or explicitly on the dial peer.

For modem passthrough to operate, you must define VoIP dial peers on both gateways to match the call, for example, by using a destination pattern or an incoming called number. The modem passthrough parameters associated with those dial peers then will apply to the call.

**Note**

When modem passthrough is configured individually for a specific dial peer, that configuration for the specific dial peer takes precedence over the global configuration.

To configure the Modem Passthrough over VoIP feature for a specific dial peer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **dial-peer voice** *number* **voip**
3. **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}
4. **exit**
5. **exit**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 dial-peer voice <i>number</i> voip</p> <p>Example:</p> <pre>Router(config)# dial-peer voice 5 voip</pre>	<p>Enters dial-peer configuration mode.</p> <p>Configures a specific dial peer in dial-peer configuration mode.</p>

Command or Action	Purpose
<p>Step 3 <code>modem passthrough {system nse [payload-type number] codec {g711ulaw g711alaw}[redundancy]}</code></p> <p>Example:</p> <pre>Router(config-dial-peer)# modem passthrough nse payload-type 97 codec g711alaw redundancy</pre>	<p>Configures the Modem Passthrough over VoIP feature for a specific dial peer. The default behavior for the Modem Passthrough for VoIP feature in dial-peer configuration mode is modem passthrough system. As required, the gateway defaults to no modem passthrough.</p> <p>When the system keyword is enabled, the following parameters are not available: nse, payload-type, codec, and redundancy. Instead the values from the global configuration are used.</p> <p>The payload type is an optional parameter for the nse keyword. Use the same payload-type number for both the originating gateway and the terminating gateway. The payload-type number can be set from 96 to 119. If you do not specify the payload-type number, the number defaults to 100. When the payload-type is 100, and you use the show running-config command, the payload-type parameter does not appear.</p> <p>Use the same codec type for both the originating gateway and the terminating gateway. g711ulaw codec is required for T1, and g711alaw codec is required for E1.</p> <p>The redundancy keyword is an optional parameter for sending redundant packets for modem traffic.</p>
<p>Step 4 <code>exit</code></p> <p>Example:</p> <pre>Router(config-dial-peer)# exit</pre>	<p>Exits dial-peer configuration mode and returns to the global configuration mode.</p>
<p>Step 5 <code>exit</code></p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>

Verifying Modem Passthrough over VoIP

To verify that the Modem Passthrough over VoIP feature is enabled, perform the following steps:

SUMMARY STEPS

1. Enter the **show run** command to verify the configuration.
2. Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

DETAILED STEPS

-
- Step 1** Enter the **show run** command to verify the configuration.
- Step 2** Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

Troubleshooting Tips

To troubleshoot the Modem Passthrough over VoIP feature, perform the following steps:

- Make sure that you can make a voice call.
- Make sure that Modem Passthrough over VoIP is configured on both the originating gateway and the terminating gateway.
- Make sure that both the originating gateway and the terminating gateway have the same named signaling event (NSE) **payload-type number**.
- Make sure that both the originating gateway and the terminating gateway have the same **maximum-sessions value** when the two gateways are configured in the voice-service configuration mode.
- Use the **debug vtsp dsp** and **debug vtsp session** commands to debug a problem.

Monitoring and Maintaining Modem Passthrough over VoIP

To monitor and maintain the Modem Passthrough over VoIP feature, use the following commands in privileged EXEC mode:

Command	Purpose
Router# show call active { voice fax } [brief]	Displays information for the active call table or displays the voice call history table. The brief option displays a truncated version of either option.
Router# show dial-peer voice [<i>number</i> summary]	Displays configuration information for dial peers. The <i>number</i> argument specifies a specific dial peer from 1 to 32767. The summary option displays a summary of all dial peers.

Configuration Examples

The following is sample configuration for the Modem Passthrough over VoIP feature:

```

version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
    modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
!
resource-pool disable
!
!
!
!
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
    
```

```

!
isdn switch-type primary-5ess
cns event-service server
!
!
!
!
mta receive maximum-recipients 0
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 shutdown
 clock source line secondary 1
!
controller T1 2
 shutdown
!
controller T1 3
 shutdown
!
!
!
interface Ethernet0
 ip address 1.1.2.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no peer default ip address
 no fair-queue
 no cdp enable
 no ppp lcp fast-start
!
interface FastEthernet0
 ip address 26.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 duplex full
 speed auto
 no cdp enable
!
ip classless
ip route 17.18.0.0 255.255.0.0 1.1.1.1
no ip http server
!
!
!
!
voice-port 0:D
!
dial-peer voice 1 pots
 incoming called-number 55511..
 destination-pattern 020..
 direct-inward-dial
 port 0:D
 prefix 020
!
dial-peer voice 2 voip
 incoming called-number 020..

```



```

destination-pattern 55511..
modem passthrough nse codec g711ulaw redundancy
session target ipv4:26.0.0.2
!
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
  login
!
!
end

```

Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 *Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers for the Cisco Unified Border Element.*

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	12.4(6)T	<p>The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs).</p> <p>The following commands were introduced or modified: modem passthrough (dial-peer); modem passthrough (voice-service); show call active voice voice; show call history voice voice; show dial-peer voice; voice service.</p>

Table 2 *Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers for the Cisco Unified Border Element (Enterprise).*

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	Cisco IOS XE Release 3.1S, Cisco IOS XE Release 3.3S	<p>The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs).</p> <p>The following commands were introduced or modified: modem passthrough (dial-peer); modem passthrough (voice-service); show call active voice; show call history voice; show dial-peer voice; voice service.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



SIP RFC 2782 Compliance with DNS SRV Queries

Effective with Cisco IOS XE Release 2.5, the Domain Name System Server (DNS SRV) query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore "_" character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.

- [Finding Feature Information, page 15](#)
- [Prerequisites SIP RFC 2782 Compliance with DNS SRV Queries, page 15](#)
- [Information SIP RFC 2782 Compliance with DNS SRV Queries, page 16](#)
- [How to Configure SIP-RFC 2782 Compliance with DNS SRV Queries, page 16](#)
- [Verifying, page 17](#)
- [Feature Information for SIP RFC 2782 Compliance with DNS SRV Queries, page 18](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites SIP RFC 2782 Compliance with DNS SRV Queries

Cisco Unified Border Element

- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information SIP RFC 2782 Compliance with DNS SRV Queries

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses the DNS SRV query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style originated in RFC 2052. Beginning with Cisco IOS XE Release 2.5, a second style, in compliance with RFC 2782, prepends the protocol label with an underscore "_"; for example, "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style.

How to Configure SIP-RFC 2782 Compliance with DNS SRV Queries

- [Configuring DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries, page 16](#)

Configuring DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries

Compliance with RFC 2782 changes the DNS SVR protocol label style. RFC 2782 updates RFC 2052 by prepending the protocol label with an underscore character. The prefix format compliant with RFC 2782 is the default format. However, backward compatibility is available, allowing newer versions of Cisco IOS software to work with older networks that support only RFC 2052 DNS SVR prefix style.

To configure the format of DNS SRV queries to comply with RFC 2782, complete this task.

**Note**

You do not have to perform this task if you want to use the default RFC 2782 format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **sip-ua**
5. **srv version** {1 | 2}
6. **exit**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>interface type number</code></p> <p>Example:</p> <pre>Router(config)# interface gigabitethernet 0/0/0</pre>	<p>Configures an interface type and enters interface configuration mode</p>
<p>Step 4 <code>sip-ua</code></p> <p>Example:</p> <pre>Router(config-if)# sip-ua</pre>	<p>Enters SIP UA configuration mode.</p>
<p>Step 5 <code>srv version {1 2}</code></p> <p>Example:</p> <pre>Router(config-sip-ua)# srv version 2</pre>	<p>Generates DNS SRV queries in either RFC 2782 or RFC 2052 format.</p> <ul style="list-style-type: none"> 1 --The query is set to the domain name prefix of protocol.transport. (RFC 2052 style). 2 --The query is set to the domain name prefix of _protocol._transport. (RFC 2782 style). This is the default.
<p>Step 6 <code>exit</code></p> <p>Example:</p> <pre>Router(config-sip-ua)# exit</pre>	<p>Exits the current configuration mode.</p>

Verifying

The following example shows sample is output from the **show sip-ua status** command used to verify the style of DNS server queries:

```
Router# show sip-ua status
SIP User Agent Status
```

```

SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)

```

Feature Information for SIP RFC 2782 Compliance with DNS SRV Queries

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

ISR feature history table entry

Table 3 Feature Information for SIP: RFC 2782 Compliance with DNS SRV Queries

Feature Name	Releases	Feature Information
SIP: RFC 2782 Compliance of DNS SRV Queries	12.2(8)T, 12.2(11)T, 12.2(15)T	<p>Effective with Cisco IOS XE Release 2.5, the DNS SRV query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore "_" character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.</p> <p>The following command was introduced or modified: srv version.</p>

ASR feature history table entry

Table 4 **Feature Information for SIP: RFC 2782 Compliance with DNS SRV Queries**

Feature Name	Releases	Feature Information
SIP: RFC 2782 Compliance of DNS SRV Queries	Cisco IOS XE Release 2.5	<p>Effective with Cisco IOS XE Release 2.5, the DNS SRV query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore "_" character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.</p> <p>The following command was introduced or modified: srv version.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



Additional References

The following sections provide references related to the Cisco Unified Border Element (Enterprise) Configuration Guide.

- [Related Documents, page 21](#)
- [Standards, page 22](#)
- [MIBs, page 22](#)
- [RFCs, page 23](#)
- [Technical Assistance, page 24](#)

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Voice commands	<i>Cisco IOS Voice Command Reference</i>
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooting information--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
Cisco IOS Release 15.0	Cisco IOS Release 15.0 Configuration Guides
Cisco IOS Release 12.2	Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <p>http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_ovrvw.html</p> <ul style="list-style-type: none"> Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <p>http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_config.html</p>
Related Application Guides	<ul style="list-style-type: none"> <i>Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</i> <i>Cisco IOS SIP Configuration Guide</i> Cisco Unified Communications Manager (CallManager) Programming Guides
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> Cisco IOS Debug Command Reference, Release 12.4 at <p>http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</p> <ul style="list-style-type: none"> <i>Troubleshooting and Debugging VoIP Call Basics</i> at http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml <i>VoIP Debug Commands</i> at <p>http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</p>

Standards

Standard	Title
ITU-T G.711	--

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-PROCESS MIB • CISCO-MEMORY-POOL-MIB • CISCO-SIP-UA-MIB • DIAL-CONTROL-MIB • CISCO-VOICE-DIAL-CONTROL-MIB • CISCO-DSP-MGMT-MIB • IF-MIB • IP-TAP-MIB • TAP2-MIB • USER-CONNECTION-TAP-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 1889	<i>RTP: A Transport Protocol for Real-Time Applications</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>
RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>
RFC 2198	<i>RTP Payload for Redundant Audio Data</i>
RFC 2327	<i>SDP: Session Description Protocol</i>
RFC 2543	<i>SIP: Session Initiation Protocol</i>
RFC 2543-bis-04	<i>SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt</i>
RFC 2782	<i>A DNS RR for Specifying the Location of Services (DNS SRV)</i>
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3203	<i>DHCP reconfigure extension</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>
RFC 3262	<i>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</i>
RFC 3323	<i>A Privacy Mechanism for the Session Initiation Protocol (SIP)</i>

RFC	Title
RFC 3325	<i>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</i>
RFC 3515	<i>The Session Initiation Protocol (SIP) Refer Method</i>
RFC 3361	<i>Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers</i>
RFC 3455	<i>Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)</i>
RFC 3608	<i>Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration</i>
RFC 3711	<i>The Secure Real-time Transport Protocol (SRTP)</i>
RFC 3925	<i>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</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>	<p>http://www.cisco.com/cisco/web/support/index.html</p>



Glossary

AMR-NB --Adaptive Multi Rate codec - Narrow Band.

Allow header --Lists the set of methods supported by the UA generating the message.

bind -- In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.

call --In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.

call leg --A logical connection between the router and another endpoint.

CLI --command-line interface.

Content-Type header --Specifies the media type of the message body.

CSeq header --Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.

delta --An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred. **dial peer**--An addressable call endpoint.

dial peer --An addressable call endpoint.

DNS --Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNS SRV --Domain Name System Server. Used to locate servers for a given service.

DSP --Digital Signal Processor.

DTMF --dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).

EFXS --IP phone virtual voice ports.

FQDN --fully qualified domain name. Complete domain name including the host portion; for example, *serverA.companyA.com*.

FXS --analog telephone voice ports.

gateway --A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H.323 --An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the

conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

iLBC --internet Low Bitrate Codec.

INVITE--A SIP message that initiates a SIP session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP-- Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ISDN --Integrated Services Digital Network.

Minimum Timer --Configured minimum value for session interval accepted by SIP elements (proxy, UAC, UAS). This value helps minimize the processing load from numerous INVITE requests.

Min-SE --Minimum Session Expiration. The minimum value for session expiration.

multicast --A process of transmitting PDUs from one source to many destinations. The actual mechanism (that is, IP multicast, multi-unicast, and so forth) for this process might be different for LAN technologies.

originator --User agent that initiates the transfer or Refer request with the recipient.

PDU --protocol data units. Used by bridges to transfer connectivity information.

PER --Packed Encoding Rule.

proxy --A SIP UAC or UAS that forwards requests and responses on behalf of another SIP UAC or UAS.

proxy server --An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.

recipient --User agent that receives the Refer request from the originator and is transferred to the final recipient.

redirect server --A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request or accept calls.

re-INVITE --An INVITE request sent during an active call leg.

Request URI --Request Uniform Resource Identifier. It can be a SIP or general URL and indicates the user or service to which the request is being addressed.

RFC --Request For Comments.

RTP --Real-Time Transport Protocol (RFC 1889)

SCCP --Skinny Client Control Protocol.

SDP--Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

session --A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

session expiration --The time at which an element considers the call timed out if no successful INVITE transaction occurs first.

session interval --The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this

value from the Session-Expires header of a 2xx INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2xx INVITE response they receive.

SIP --Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

SIP URL --Session Initiation Protocol Uniform Resource Locator. Used in SIP messages to indicate the originator, recipient, and destination of the SIP request. Takes the basic form of *user@host*, where *user* is a name or telephone number, and *host* is a domain name or network address.

SPI --service provider interface.

socket listener -- Software provided by a socket client to receives datagrams addressed to the socket.

stateful proxy --A proxy in keepalive mode that remembers incoming and outgoing requests.

TCP --Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TDM --time-division multiplexing.

UA --user agent. A combination of UAS and UAC that initiates and receives calls. See **UAS** and **UAC**.

UAC --user agent client. A client application that initiates a SIP request.

UAS --user agent server. A server application that contacts the user when a SIP request is received and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

UDP -- User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URI --Uniform Resource Identifier. Takes a form similar to an e-mail address. It indicates the user's SIP identity and is used for redirection of SIP messages.

URL --Universal Resource Locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

User Agent --A combination of UAS and UAC that initiates and receives calls. See **UAS** and **UAC**.

VFC --Voice Feature Card.

VoIP --Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based approach (for example, H.323) to IP voice traffic.

