Cisco Unified Communications Trusted Firewall Control

First Published: December 15, 2008

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. Firewall traversal is accomplished using Session Traversal Utilities for NAT(STUN) on a TRP colocated with a Cisco Unified Communications Manager Express (Cisco Unified CME) or a Cisco Unified Border Element.

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 for Cisco Unified Communications Trusted Firewall Control" section on page 13.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE 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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Cisco Unified Communications Trusted Firewall Control

- Be sure that you have the correct platform to support this feature. Cisco Unified Communications Trusted Firewall Control is supported on the Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 platforms.
- Cisco IOS Release 12.4(22)T.
- TRP colocated with Cisco IOS firewall
  - TRP + Cisco IOS firewall on the same box as Cisco Unified CME and Cisco Unified Border Element
  - c28xx, c1861, and c38xx and platforms
  - **adventerprisek9** and **advipservicesk9** packages

Restrictions for Cisco Unified Communications Trusted Firewall Control

Cisco IOS Release 12.4(22)T implements firewall traversal for media using STUN on TRP and is only supported on:

- Cisco Unified CME colocated with TRP
- Cisco Unified Border Element colocated with TRP (limited call flows)

TRP is only supported for the following control agents:

- Cisco Unified CME and Cisco Unified Border Element which are STUN-aware
- Cisco Unified CME for SIP trunks

  Supported:
  - SCCP/SIP line to SIP trunk audio calls
  - Cisco IOS firewall on the SIP trunk side
  - SIP over UDP/TCP
  - RTP and SRTP

  Not Supported:
  - Cisco IOS firewall on line side
  - Video, RSVP, IPv6
- Cisco Unified Border Element for SIP to SIP call flows

  Supported:
  - SIP to SIP flow-through audio calls
  - SIP over UDP/TCP
  - REFER-based supplementary services
  - SIP to SIP DTMF inter-working
  - In-box transcoding

Not Supported:

- High density transcoding (transcoder optimization)
- Re-INVITE based supplementary services
- Video, RSVP, IPv6

Other restrictions:

- Unauthenticated Keepalives
  - When a pinhole is opened, the Cisco IOS firewall expects only UDP packets.
  - TRP sends periodic STUN binding indications containing only the STUN header.
  - Keepalives do not contain any token and are not authenticated by the Cisco IOS firewall.
- No explicit close pinhole message
  - There is no explicit *close pinhole* message from TRP.
  - The pinhole times out at the Cisco IOS firewall when no UDP packets are received.
- No prering support
  - No guarantee that STUN open pinhole packet reaches the Cisco IOS firewall before the first RTP packet.
  - Possible initial RTP packet drops at the Cisco IOS firewall.
- Cisco IOS firewall control session timeout
  - ACLs must be configured on the Cisco IOS firewall to allow SIP signaling.
  - The Cisco IOS firewall control sessions timeout if no SIP messages are exchanged.
  - Timed out SIP over UDP sessions are re-established with the next SIP message (for example, BYE).
  - Timed out SIP over TCP sessions are not re-established, causing subsequent SIP messages (for example, BYE) to be dropped.

Information About Cisco Unified Communications Trusted Firewall Control

Firewall traversal for end-to end VoIP calls poses several problem:

- VoIP protocols use many ports for a single communication session. It is not possible to configure static rules for a large range of ports.
- Limiting the RTP port range is not supported by most endpoints.
- An application layer gateway (ALG) can be costly in terms of system resources and maintenance.

Cisco Unified Communications Trusted Firewall Control builds intelligence into the firewall so that it can open a pinhole (a port that is opened through a firewall to allow a particular application access to the protected network) dynamically when it receives a STUN request for a media flow. This request is authenticated/authorized by the firewall to ensure that it opens pinholes only for genuine calls.

Cisco Unified Communications Trusted Firewall Control provides:

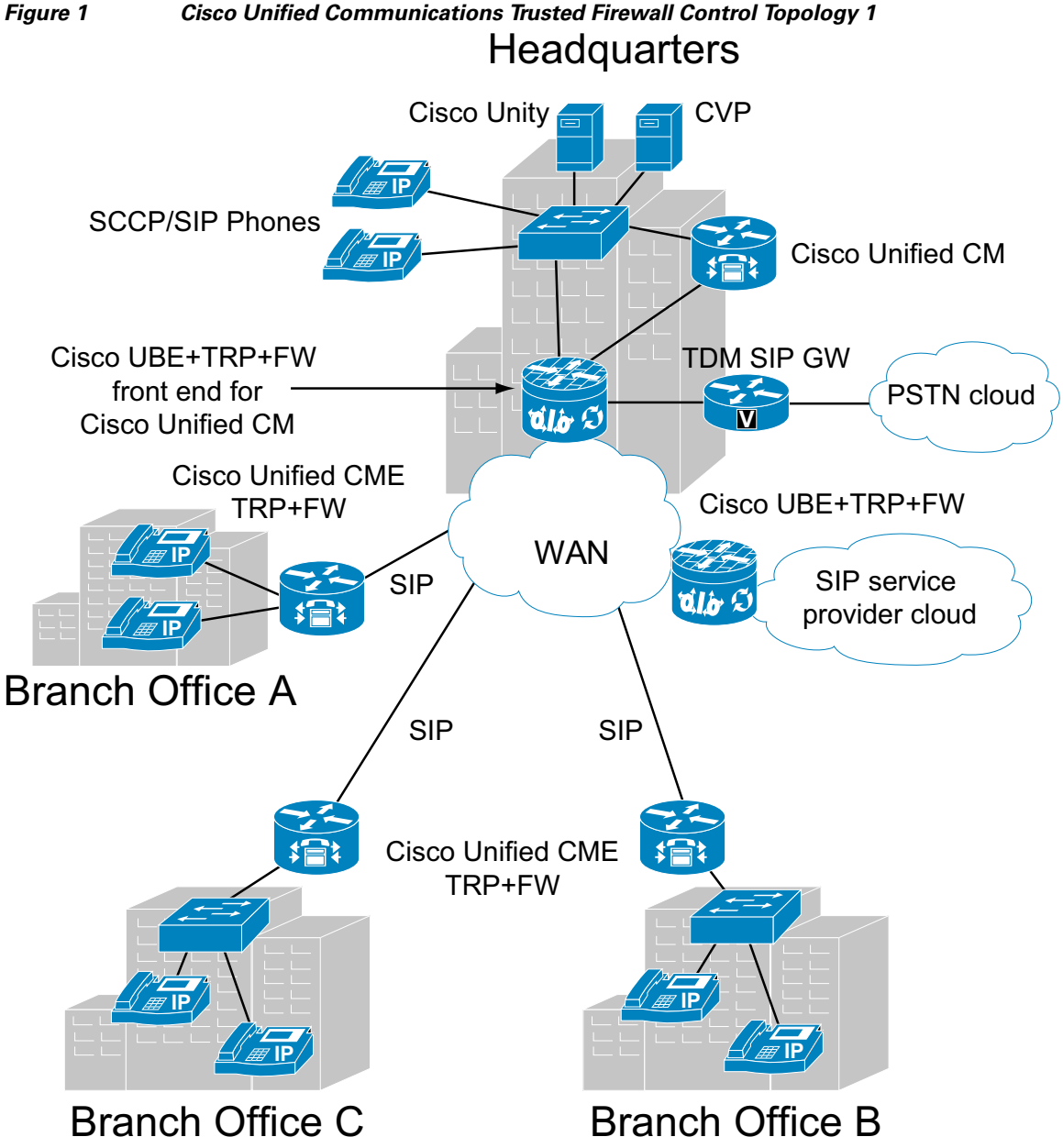
- Increased firewall performance while opening firewall ports in the media path dynamically when a VoIP call is made between two endpoints.

- Simplification of firewall policy configuration and integration of firewall policy generation with call control.
- No compromising on network security
- Firewall traversal

Flowdata refers to CISCO-STUN-FLOWDATA, a comprehension-optional Cisco proprietary STUN attribute. If a STUN agent does not understand the attribute, the agent must ignore it. This attributes identifies an RTP or RTCP flow to the firewall and contains a Crypto Acceptance Token (CAT), which the firewall uses to authenticate the sender of the STUN message—the TRP. See RFC 5389 for more information.

Figure 1 shows a topology for Cisco Unified Communications Trusted Firewall Control.

Figure 1 Cisco Unified Communications Trusted Firewall Control Topology 1



How to Configure Cisco Unified Communications Trusted Firewall Control

To configure firewall traversal, perform the following steps:

Prerequisites

- The firewall must be configured with an agent ID and shared secret, which must be the same as those configured on the call agent.

```
!
parameter-map type protocol-info stun-ice stun-params
 authorization agent-id 15 shared-secret ciscopasswd1234 cat-window 10
!
```

- Zone security configuration on the interface locks the interface. Only the traffic specified in the policy is allowed. To allow ICMP pings between the two interfaces, configure a new class map as follows:

```
!
class-map type inspect icmp-class
    match protocol icmp
!
```

Add the class to the policy map as follows:

```
!
policy-map type inspect stun-policy
    class type inspect stun-class
    inspect
    class type inspect icmp-class
    pass
!
```

- Configure a policy to allow SIP traffic through the firewall.

For information on configuring zone-based Cisco IOS firewalls, see: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **stun**
5. **stun flowdata agent-id** *tag*
6. **stun flowdata shared-secret** *string*
7. **stun flowdata keepalive** *seconds*
8. **exit**
9. **voice class stun-usage** *tag*
10. **stun usage firewall-traversal flowdata**

11. **exit**
12. **dial-peer voice** *tag* **voip**
13. **voice-class stun-usage** *tag*
14. **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 service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode and specifies a voice-encapsulation type.
Step 4	**stun** **Example:** `Router(config-voi-serv)# stun`	Enters STUN configuration mode.
Step 5	**stun flowdata agent-id** *tag* **Example:** `Router(config-serv-stun)# stun flowdata agent-id 35`	Configure the STUN flowdata agent ID. • *tag*—Must match agent ID on the firewall
Step 6	**stun flowdata shared-secret** *string* **Example:** `Router(config-serv-stun)# stun flowdata shared-secret 123abc123abc`	Configures a secret shared on a call control agent. • *string*—Must match shared secret on the firewall.

Step 7	**stun flowdata keepalive** *seconds*
	
	Example:
	`Router(config)# voice service voip`
	`Router(config-serv-stun)# stun flowdata keepalive 5`
		(Optional) Changes the keepalive interval from the default value.
		• *seconds*—Range is 1 to 65535 seconds. Default is 10 seconds.

Step 8	**exit** **Example:** `Router(config-serv-stun)# exit`	Exits STUN configuration mode.

	Command or Action (continued)	Purpose (continued)
Step 9	**voice class stun-usage** *tag* **Example:** `Router(config)# voice-class stun-usage 10000`	Assigns identification tag to a voice class and enters voice class configuration mode.
Step 10	**stun usage firewall-traversal flowdata** **Example:** `Router(config-class)# stun usage firewall-traversal flowdata`	Enables firewall traversal using STUN.
Step 11	**exit** **Example:** `Router(config-class)# exit`	Exits voice class configuration mode.
Step 12	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial peer configuration mode to define a VoIP dial peer for firewall traversal.
Step 13	**voice-class stun-usage** *tag* **Example:** `Router(config-dial-peer)# voice-class stun-usage 10000`	Enables firewall traversal for VoIP communications on this dial peer.
Step 14	**end** **Example:** `Router(config-dial-peer)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying Firewall Traversal

Use the **show policy-map type inspect zone-pair sessions** command to display information about policy maps.

Configuration Examples for Cisco Unified Communications Trusted Firewall Control

The following is a sample configuration for Cisco Unified Communications Trusted Firewall Control:

```
CUBE2-3825#show running config
Building configuration...

Current configuration : 3594 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
```

```
service internal
!
hostname CUBE2-3825
!
boot-start-marker
boot system flash:c3825-ipvoice-mz.stun_stack_dt
boot-end-marker
!
logging message-counter syslog
logging buffered 9999999
no logging console
!
no aaa new-model
clock timezone IST 5
no network-clock-participate slot 1
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
!
!
voice dsp waitstate 0
!
voice service voip
 address-hiding
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
 stun
  stun flowdata agent-id 35
  stun flowdata shared-secret 123xyz123xyz
  stun flowdata keepalive 5
 sip
!
!
voice class codec 1
!
!
voice class stun-usage 10
stun usage firewall-traversal flowdata
!
!
!
voice iec syslog
!
no memory lite
archive
 log config
  hidekeys
```

```
!
!
ip ftp username test
ip ftp password test123
!
!
interface Loopback0
 no ip address
!
interface GigabitEthernet0/0
 ip address 9.13.23.6 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 9.13.23.1
ip route 1.1.1.0 255.255.255.0 9.13.24.7
ip route 9.13.24.0 255.255.255.0 9.13.23.7
ip http server
no ip http secure-server
!
!
tftp-server flash:P0S3-08-4-00.sb2
tftp-server flash:P0S3-08-4-00.loads
tftp-server flash:P003-08-4-00.sbn
tftp-server flash:P003-08-4-00.bin
tftp-server flash:OS79XX.TXT
!
control-plane
!
call treatment on
!
!
voice-port 1/0/0
!
voice-port 1/0/1
 shutdown
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
dial-peer voice 1 voip
 destination-pattern 2...
 session protocol sipv2
 session target ipv4:9.13.23.5
 codec g711ulaw
!
dial-peer voice 11 voip
voice-class stun-usage 10
 session protocol sipv2
 session transport udp
 incoming called-number 2...
```

```
 codec g711ulaw
!
sip-ua
 protocol mode ipv4
!
!
gatekeeper
 irq global-request
 shutdown
!
alias exec t test stun
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 no login
 transport input none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp server 9.13.0.10
end
```

Additional References

The following sections provide references related to Cisco Unified Communications Trusted Firewall Control.

Related Documents

Related Topic	Document Title
IP Application Services Configuration	*Cisco IOS IP Application Services Configuration Guide 12.4*
IP Application Services Command Reference	*Cisco IOS IP Application Services Command Reference 12.4*
Cisco Unified CME Command Reference	*Cisco Unified Communications Manager Express Command Reference*
All other Cisco IOS Command Reference guides	Various titles located at http://www.cisco.com/en/US/customer/products/ps6350/prod_command_reference_list.html
Routers Support Resources	*Technical Support and Documentation for Routers*

Standards

Standard	Title
No new or modified standards are supported, and support for existing RFCs has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
5389	Session Traversal Utilities for NAT (STUN)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Cisco Unified Communications Trusted Firewall Control

Table 1 lists the release history for this feature.

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

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE 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 Cisco Unified Communications Trusted Firewall Control

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control	12.4(22)T	Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following sections provide information about this feature: • "Information About Cisco Unified Communications Trusted Firewall Control" section on page 3 • "How to Configure Cisco Unified Communications Trusted Firewall Control" section on page 6 The following commands were introduced: **stun**; **stun flowdata agent-id**; **stun flowdata keepalive**; **stun flowdata shared-secret**; **stun usage firewall-traversal flowdata**; **voice class stun-usage**; **voice-class stun-usage**.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

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

© 2008 Cisco Systems, Inc. All rights reserved.

Command Reference

This section documents only commands that are new or modified.

- **stun**
- **stun flowdata agent-id**
- **stun flowdata keepalive**
- **stun flowdata shared-secret**
- **voice class stun-usage**
- **stun usage firewall-traversal flowdata**
- **voice-class stun-usage**

stun

To enter STUN configuration mode for configuring firewall traversal parameters, use the **stun** command in voice-service voip configuration mode. To remove STUN parameters, use the **no** form of this command.

stun *stun*

Syntax Description

stun	Stun configuration parameters: • **stun flowdata agent-id** • **stun flowdata keepalive** • **stun flowdata shared-secret**

Command Default

No default behavior or values.

Command Modes

Voice-service voip configuration (config-voi-serv)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use this command to enter the configuration mode to configure firewall traversal parameters for VoIP communications.

Examples

The following example shows how to enter STUN configuration mode.

```
Router(config)# voice service voip
Router(config-voi-serv)# stun
```

Related Commands

Command	Description
stun flowdata agent-id	Configures the agent ID.
stun flowdata keepalive	Configures the keepalive interval
stun flowdata shared-secret	Configures a secret shared between Call Control Agent and Firewall
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.
voice-class stun-usage	Enables firewall traversal for VoIP communications.

stun flowdata agent-id

To configure the STUN flowdata agent ID, use the **stun flowdata agent-id** command in STUN configuration mode. To return to the default value for agent ID, use the **no** form of this command.

stun flowdata agent-id *tag*

no stun flowdata agent-id

Syntax Description

tag	Unique identifier in the range 0 to 255. Default is -1.

Command Default

No firewall traversal is performed.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use the **stun flowdata agent-id** command to configure call control agents which authorize the flow of traffic to the firewall. The **show run all** command displays the default value as -1.

Examples

The following example shows how to set stun flowdata agent ID to 35.

```
Router(config)# voice service voip
Router(config-voi-serv)# stun
Router(config-serv-stun)# stun flowdata agent-id 35
Router(config-serv-stun)# stun flowdata shared-secret 123abc123abc
Router(config-serv-stun)# stun flowdata keepalive 5
```

Related Commands

Command	Description
stun	Enters STUN configuration mode.
stun flowdata keepalive	Configures the keepalive interval
stun flowdata shared-secret	Configures a secret shared between Call Control Agent and Firewall

stun flowdata keepalive

To configure the keepalive interval, use the **stun flowdata keepalive** command in STUN configuration mode. To return to the default keepalive value, use the **no** form of this command.

stun flowdata keepalive *seconds*

no stun flowdata keepalive

Syntax Description.

seconds	Keepalive interval in seconds. Range is 1 to 65535. Default is 10.

Command Default

The default keepalive value is 10 seconds.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Keepalives are application connections TRP generates to keep firewall pinholes open.

Examples

The following example shows how to change the stun flowdata keepalive interval from the default value (10) to 5 seconds.

```
Router(config)# voice service voip
Router(config-voi-serv)# stun
Router(config-serv-stun)# stun flowdata agent-id 35
Router(config-serv-stun)# stun flowdata shared-secret 123abc123abc
Router(config-serv-stun)# stun flowdata keepalive 5
```

Related Commands

Command	Description
stun	Enters STUN configuration mode.
stun flowdata shared-secret	Configures a secret shared between Call Control Agent and Firewall.
stun flowdata agent-id	Configures the agent ID.

stun flowdata shared-secret

To configure a secret shared on a call control agent, use the **stun flowdata shared-secret** command in STUN configuration mode. To return the shared secret to the default value, use the **no** form of this command.

stun flowdata shared-secret *string*

no stun flowdata shared-secret

Syntax Description

string	12 to 80 ASCII characters. Default is an empty string.

Command Default

The default value of this command sets the shared secret to an empty string. No firewall traversal is performed when the shared-secret has the default value.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

A shared secret on a call control agent is a string that is used between a call control agent and the firewall for authentication purposes. The shared secret value on the call control agent and the firewall must be the same.

Examples

The following example shows how to set the shared secret to 123abc123abc.

```
Router(config)# voice service voip
Router(config-voi-serv)# stun
Router(config-serv-stun)# stun flowdata agent-id 35
Router(config-serv-stun)# stun flowdata shared-secret 123abc123abc
Router(config-serv-stun)# stun flowdata keepalive 5
```

Related Commands

Command	Description
stun	Enters STUN configuration mode.
stun flowdata agent-id	Configures the agent ID.
stun flowdata keepalive	Configures the keepalive interval.

voice class stun-usage

To configure voice class and enter voice class configuration mode, called stun-usage, use the **voice-class stun-usage command** in global configuration mode. To disable the voice class, use the **no** form of this command

voice class stun-usage *tag*

no voice class stun-usage *tag*

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

The voice class is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the voice-class stun-usage is removed, the same is removed automatically from the dial-peer configurations.

Examples

The following example shows how to set the **voice class stun-usage** tag to 10000:

```
Router(config)# voice class stun-usage 10000
```

Related Commands

Command	Description
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
stun flowdata agent-id	Configures the agent ID.

stun usage firewall-traversal flowdata

To enable firewall traversal using STUN, use the **stun usage firewall-traversal flowdata** command in voice class stun-usage configuration mode. To disable firewall traversal with STUN, use the **no** form of this command.

stun usage firewall-traversal flowdata

no stun usage firewall-traversal flowdata

Syntax Description

This command has no parameters.

Command Default

Firewall traversal using STUN is not enabled.

Command Modes

Voice-class configuration (config-class)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows how to enable firewall traversal using STUN:

```
Router(config)# voice class stun-usage 10
Router(config-class)# stun usage firewall-traversal flowdata
```

Related Commands

Command	Description
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.

voice-class stun-usage

To enable firewall traversal for VoIP communications, use the **voice-class stun-usage** command in dial-peer voice configuration mode. To disable firewall traversal, use the **no** form of this command.

voice-class stun-usage *tag*

no voice-class stun-usage

Syntax Description

tag	Unique identifier in the range 1 to 10000.

Command Default

Firewall traversal is not enabled.

Command Modes

Dial-peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the voice-class stun-usage command is removed, the same is removed automatically from dial-peer configurations.

Examples

The following example shows how to set the **voice-class stun-usage** tag to 10.

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# voice-class stun-usage 10
```

Related Commands

Command	Description
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.