Cisco Unified CME Commands: I

ica

To specify the audio file used for the isolated code announcement, use the **ica** command in voice MLPP configuration mode. To disable use of this audio file, use the **no** form of this command.

ica *audio-url*
no ica

Syntax Description

audio-url	Location of the announcement audio file in URL format. Valid storage locations are TFTP, FTP, HTTP, and flash memory.

Command Default

No announcement is played.

Command Modes

Voice MLPP configuration (config-voice-mlpp)

Command History

Cisco IOS Release	Cisco Product	Modification
15.0(1)XA	Cisco Unified CME 8.0	This command was introduced.
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command specifies the G.711 a-law or u-law 8-KHz encoded audio file (.wav or .au format) for the announcement that plays to callers when service or equipment problems prevent completion of their call.

The **mlpp indication** command must be enabled (default) for a phone to play precedence announcements.

This command is not supported by Cisco IOS help. If you type **?** , Cisco IOS help does not display a list of valid entries.

Examples

The following example shows that the audio file played for the isolated code announcement is named ica.au located in flash:

```
Router(config)# voice mlpp
Router(config-voice-mlpp)# ica flash:ica.au
```

Related Commands

Command	Description
bnea	Specifies the audio file used for the busy station not equipped for preemption announcement.
upa	Specifies the audio file used for the unauthorized precedence announcement.
vca	Specifies the audio file used for the vacant code announcement.
mlpp indication	Enables MLPP indication on an SCCP phone or analog FXS port.
mlpp preemption	Enables preemption capability on an SCCP phone or analog FXS port.

id (voice register pool)

To explicitly identify a locally available individual Cisco SIP IP phone, or when running Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST), set of Cisco SIP IP phones, use the **id** command in voice register pool configuration mode. To remove local identification, use the **no** form of this command.

id {**[network** *address* **mask** *mask* **|** *address* **mask** *mask* **] | [ip** *address* **mask** *mask address* **mask** *mask* **] | [mac** *address***]}[device-id-name** *devicename***]**
no id {**[network** *address* **mask** *mask* **|** *address* **mask** *mask* **] | [ip** *address* **mask** *mask address* **mask** *mask* **] | [mac** *address***]}[device-id-name** *devicename***]**

Syntax Description

network *address* **mask** *mask* **|** *address* **mask** *mask*	This keyword/argument combination is used to accept SIP Register messages for the indicated phone numbers from any IP phone within the specified IPv4 and IPv6 subnets. *ipv6 address* can only be configured with an IPv6 address or a dual-stack mode.
ip *address* **mask** *mask* **|** *address* **mask** *mask*	This keyword/argument combination is used to identify an individual phones IPv4 or IPv6 address. *ipv6 address* can only be configured with an IPv6 address or a dual-stack mode.
mac *address*	The **mac** *address* keyword/argument combination is used to identify the MAC address of a particular Cisco IP phone.
device-id-name *devicename*	Defines the device name to be used to download the phone's configuration file.

Command Default

No SIP IP phone is configured.

Command Modes

Voice register pool configuration (config-register-pool)

Command History

Release	Cisco Product	Modification
12.2(15)ZJ	Cisco SIP SRST 3.0	This command was introduced.
12.3(4)T	Cisco SIP SRST 3.0	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)T	Cisco CME 3.4 Cisco SIP SRST 3.4	This command was added to Cisco CME.
15.3(3)T	Cisco Unified CME 10.0	This command was modified to add the **device-id-name** *devicename* keyword-argument combination.
Cisco IOS XE Everest 16.6.1	Unified SRST 12.0	This command was modified to add the following keyword-argument combinations for **network** and **ip** to include support for IPv6 address: *address* **mask** *mask*.

Usage Guidelines

Configure this command before configuring any other command in voice register pool configuration mode.

This command allows explicit identification of an individual Cisco SIP IP phone to support a degree of authentication, which is required to accept registrations, based upon the following:

- Verification of the local Layer 2 MAC address using the router's Address Resolution Protocol (ARP) cache.
- Verification of the known single static IP address (or DHCP dynamic IP address within a specific subnet) of the Cisco SIP IP phone.

When the **mac** *address* keyword and argument are used, the IP phone must be in the same subnet as that of the router's LAN interface, such that the phone's MAC address is visible in the router's ARP cache. Once a MAC address is configured for a specific voice register pool, remove the existing MAC address before changing to a new MAC address.

Note For Cisco Unified SIP SRST, this command also allows explicit identification of locally available set of Cisco SIP IP phones.

Examples

The following is partial sample output from the **show running-config** command. The **id** command identifies the MAC address of a particular Cisco IP phone. The output shows that voice register pool 1 has been set up to accept SIP Register messages from a specific IP phone through the use of the **id** command.

```
voice register pool 1
 id mac 0030.94C2.A22A
 preference 5
 cor incoming call91 1 91011
 translate-outgoing called 1
 proxy 10.2.161.187 preference 1 monitor probe icmp-ping
 alias 1 94... to 91011 preference 8
 voice-class codec 1
```

The following is sample output from the **show running-config** command after configuring IPv6 address on Cisco Unified SRST router.

```
voice register pool 1
 id network 2001:420:54FF:13::312:0/117
```

Related Commands

Command	Description
mode (voice register global)	Enables the mode for provisioning SIP phones in a Cisco Unified CallManager Express (Cisco Unified CME) system.

import certificate

To import a trusted certificate in PEM format from flash memory to the CTL file of an IP phone, use the **import certificate** command in ctl-client configuration mode. To return to the default, use the **no** form of this command.

import certificate *tag description***flash:***cert_name*
no import certificate

Syntax Description

tag	Identifier for the trusted certificate.
description	Descriptive name of the trusted certificate.
flash:*cert_name*	Specifies the filename of the trusted certificate stored in flash memory.

Command Default

None

Command Modes

CTL-client configuration (config-ctl-client)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

A CTLFile.tlv file should appear in the flash location after using the **regenerate** command in ctl-client configuration mode. If the file is missing, use the **debug ctl-client** command, followed by the **regenerate** command.

Examples

The following is an example of how the **import certificate** command is used to import the WebServer certificate with filename web_cer.cer from flash memory:

```
Router(config)# ctl-client
Router(config-ctl-client)# sast1 trustpoint primary-cme
Router(config-ctl-client)# sast2 trustpoint sast-secondary
Router(config-ctl-client)# import certificate 1 WebServer flash:web_cert.cer
Router(config-ctl-client)# regenerate
```

Related Commands

Command	Description
ctl-client	Enters CTL-client configuration mode to set parameters for the CTL client.

index (lpcor ip-phone)

To add a logical partitioning class of restriction (LPCOR) group to the IP-phone subnet table, use the **index** command in LPCOR ip-phone subnet configuration mode. To remove a resource, use the **no** form of this command.

index *index-number lpcor-group* {*ipv4-address network-mask* [**vrf** *vrf-name*] | **dhcp-pool** *pool-name*}
no index *index-number*

Syntax Description

index-number	Number of the LPCOR subnet index entry. Range: 1 to 50.
lpcor-group	Name of a LPCOR resource-group policy.
ipv4-address	IPv4 address of the LPCOR policy.
network-mask	Subnet mask for the associated IPv4 address.
vrf *vrf-name*	(Optional) Dynamic Host Configuration Protocol (DHCP) server uses the VPN routing and forwarding (VRF) table that is associated with the access point name (APN).
dhcp-pool *pool-name*	User-defined name of the DHCP pool. The pool name can be a symbolic string (such as Sales) or an integer (such as 0).

Command Default

No index entry is configured.

Command Modes

LPCOR ip-phone subnet configuration (cfg-lpcor-ipphone-subnet)

Command History

Cisco IOS Release	Cisco Product	Modification
15.0(1)XA	Cisco Unified CME 8.0	This command was introduced.
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command is used for mobility-type phones only, which can include Extension Mobility phones, teleworker remote phones, and Cisco IP Communicator softphones.

Two IP-phone subnet tables, containing up to 50 index entries, can be defined on each Cisco Unified CME router. One table is for incoming calls and the other table is for outgoing calls.

A LPCOR policy is dynamically associated with calls to and from a mobility-type phone by matching its current IP address or DHCP pool in the IP-phone subnet table. If the LPCOR policy cannot be provisioned from the IP-phone subnet table, the default LPCOR policy for mobility-type phones is used.

Entries in the IP-phone subnet tables are indexed in ascending order. The lookup of entries is in sequential ascending order. After Cisco Unified CME finds a matching entry, the corresponding LPCOR policy is associated with the call. Even if there are other entries that are a better match, only the first match is used.

For instance, in the example below, if a call originates from an IP phone with IP address 10.1.10.3, LPCOR policy local_g4 is associated with the incoming call instead of LPCOR policy local_g5 even though local_g5 is a better match.

Examples

The following example shows an IP-phone subnet table for incoming calls that has four entries:

```
voice lpcor ip-phone subnet incoming
 index 1 local_g4 10.1.10.0 255.255.255.0
 index 2 remote_g4 171.19.0.0 255.255.0.0
 index 3 local_g5 10.1.10.2 255.255.255.255
 index 4 local_g5 10.1.10.3 255.255.255.255
```

Related Commands

Command	Description
lpcor type	Specifies the LPCOR type for an IP phone.
voice lpcor ip-phone mobility	Sets the default LPCOR policy for mobility-type phones.
voice lpcor policy	Creates a LPCOR policy for a resource group.

index (lpcor ip-trunk)

To add a logical partitioning class of restriction (LPCOR) resource group to the IP trunk subnet table, use the **index** command in LPCOR IP-trunk subnet configuration mode. To remove a resource, use the **no** form of this command.

index *number* *lpcor-group* {*ipv4-address* *network-mask* | **hostname** *host-name*}
no index *number*

Syntax Description

number	Number of the LPCOR subnet index entry. Range: 1 to 50.
lpcor-group	Name of a LPCOR resource-group policy.
ipv4-address	IPv4 address of the LPCOR policy.
network-mask	Subnet mask of the associated IPv4 address.
hostname *host-name*	User-defined IP host name.

Command Default

No index entry is configured.

Command Modes

LPCOR IP-trunk subnet configuration (cfg-lpcor-iptrunk-subnet)

Command History

Cisco IOS Release	Cisco Product	Modification
15.0(1)XA	Cisco Unified CME 8.0	This command was introduced.
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

One IP-trunk subnet table, containing up to 50 index entries, can be defined on each Cisco Unified CME router for incoming VoIP trunk calls (H.323 or SIP).

An incoming VoIP trunk call is associated with a LPCOR policy by matching the remote IP address to an entry in the incoming IP-trunk subnet table. If that is not successful, the LPCOR policy in voice service configuration mode is applied.

Entries in the IP-trunk subnet table are indexed in ascending order. The lookup of entries is in sequential ascending order. After Cisco Unified CME finds a matching entry, it associates the corresponding LPCOR policy with the call. Even if there are other entries that are a better match, only the first match is used.

In the following example, an incoming VoIP call with a remote IP address of 172.19.22.25 is associated with sip_group1 even though voip_group2 is a better match.

Examples

The following example shows an IP-trunk subnet table with six index entries:

```
voice lpcor ip-trunk subnet incoming
 index 1 h323_group1 172.19.33.0 255.255.255.0
 index 2 sip_group1 172.19.22.0 255.255.255.0
 index 3 voip_group2 172.19.33.25 255.255.255.255
 index 4 voip_group3 172.19.22.26 255.255.255.255
```

```
index 5 sip_s1 hostname sipserver1
index 6 sip_s2 hostname sipserver2
```

Related Commands

Command	Description
lpcor incoming	Associates an incoming call with a LPCOR resource-group policy.
voice lpcor policy	Ccreates a LPCOR policy for a resource group.

intercom (ephone-dn)

To create an intercom by programming a pair of extensions (ephone-dns) to automatically call and answer each other, use the **intercom** command in ephone-dn configuration mode. To remove an intercom, use the **no** form of this command.

intercom *extension-number* **[[barge-in [no-mute] |no-auto-answer | no-mute] [label***label***]] | label***label***]|[***paging number***ptt]**
no intercom

Syntax Description

extension-number	Extension or telephone number to which calls are placed.
barge-in	(Optional) Allows inbound intercom calls to force an existing call into the call-hold state and the intercom call to be answered immediately.
label *label*	(Optional) Defines an alphanumeric label for the intercom, of up to 30 characters.
no-auto-answer	(Optional) Disables the intercom auto-answer feature.
no-mute	(Optional) Allows an intercom call to be answered without deactivating a speaker's mute key.
paging number ptt	(Optional) Allows to set a paging number for push-to-talk (PTT) feature.

Command Default

Intercom functionality is disabled.

Command Modes

Ephone-dn configuration (config-ephone-dn)

Command History

Cisco IOS Release	Cisco Product	Modification
12.2(2)XT	Cisco ITS 2.0	This command was introduced.
12.2(8)T	Cisco ITS 2.0	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(11)XL	Cisco CME 3.2.1	The **no-mute** keyword was added.
12.3(14)T	Cisco CME 3.3	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(20)T	Cisco Unified CME 7.0	The paging number and ptt keywords and argument was added.

Usage Guidelines

This command is used to dedicate a pair of Cisco ephone-dns for use as a "press to talk" two-way intercom between Cisco IP phones. Intercom lines cannot be used in shared-line configurations. If an ephone-dn is configured for intercom operation, it must be associated with one Cisco IP phone only. The intercom attribute causes an IP extension (ephone-dn) to operate in autodial fashion for outbound calls and autoanswer-with-mute for inbound calls.

The **barge-in** keyword allows inbound intercom calls to force an existing call on the called phone into the call-hold state to allow the intercom call to be answered immediately. The **no-auto-answer** keyword creates for the IP phone line a connection that resembles a private line, automatic ringdown (PLAR). The **label** keyword defines a text label for the intercom.

Following this command, the intercom ephone-dns are assigned to ephones using the **button** command. Following the **button** command, the **restart** command must be used to initiate a quick reboot of the phones to which this intercom is assigned.

The default **intercom** command behavior is speakers are set to mute automatically when phones receive intercom calls. For example, if phone user 1 places an intercom call and connects to phone user 2, user 2 will hear user 1, but user 1 will not hear user 2. To be heard, user 2 must first disable the speaker's mute function. The benefit is people who receive intercom calls can use the mute button to control when they will be heard initially.

The **no-mute** keyword deactivates the speaker mute function when IP phones receive intercom calls. For example, if phone user 1 makes an intercom call to phone user 2, both users will hear each other upon connection. The benefit is that people who receive intercom calls do not have to disable their speaker's mute function to be heard, *but* their conversations and nearby background sounds will be heard the moment an intercom call to them is connected—regardless of whether they are ready to take a call or not.

The intercom command allows you to add a paging number to behave as a push-to-talk (ptt) feature. More information on the push-to-talk feature is available at this link:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmelabel.html#wpmkr1048855

Examples

The following example sets the intercom on Cisco IP phone directory number 1:

```
Router(config)# ephone-dn 1
Router(config-ephone-dn) number A5001
Router(config-ephone-dn) name "intercom"
Router(config-ephone-dn) intercom A5002 barge-in
```

The following example shows intercom configuration between two Cisco IP phones:

```
ephone-dn 18
 number A5001
 name "intercom"
 intercom A5002 barge-in
ephone-dn 19
 number A5002
 name "intercom"
 intercom A5001 barge-in
ephone 4
 button 1:2 2:4 3:18
 ephone 5
 button 1:3 2:6 3:19
```

In the example, ephone-dn 18 and ephone-dn 19 are set as an intercom pair. Ephone-dn 18 is associated with button 3 of Cisco IP phone (ephone) 4, and ephone-dn 19 is associated with button number 3 of Cisco IP phone (ephone) 5. Button 3 on Cisco IP phone 4 and button 3 on Cisco IP phone 5 are set as a pair to provide intercom service to each other.

The intercom feature acts as a combination speed-dial PLAR and autoanswer with mute. If the **barge-in** keyword is set on the ephone-dn that receives the intercom call, the existing call is forced into the hold state, and the intercom call is accepted. If the phone user has the handset off hook (that is, not in speakerphone mode), the user hears a warning beep, and the intercom call is immediately connected with two-way audio. If the phone user is using speakerphone mode, the intercom connects with the microphone mute activated.

Note Any caller can dial in to an intercom extension, and a call to an intercom extension that is originated by a nonintercom caller triggers an automatic answer exactly like a legitimate intercom call. To prevent nonintercom originators from manually dialing an intercom destination, you can use alphabetic characters when you assign numbers to intercom extensions using the **number** command. These characters cannot be dialed from a normal phone but can be dialed by preprogrammed intercom extensions whose calls are made by the router.

Related Commands

Command	Description
button	Associates ephone-dns with individual buttons on Cisco IP phones and specifies ring behavior per button.
number	Associates a telephone or extension number with an extension (ephone-dn).
restart (ephone)	Performs a fast reboot of a single phone associated with a Cisco CME router.
restart (telephony-service)	Performs a fast reboot of one or all phones associated with a Cisco CME router.

intercom (voice register dn)

To enable the intercom call option on a Cisco Unified SIP IP phone, use the **intercom** command in voice register dn configuration mode. To prevent a Cisco Unified SIP IP phone from making an intercom call, use the **no** form of this command.

intercom [**speed-dial** *digit-string*] [**label** *label-text*]
no intercom [**speed-dial** *digit-string*] [**label** *label-text*]

Syntax Description

speed-dial	(Optional) Enables the intercom line user to place a call to a pre-configured destination. If the speed-dial is not configured, it simply initiates a new call on the intercom line and waits for the user to dial the destination number.
digit-string	Digits to be dialed when the speed-dial button is pressed on a Cisco Unified SIP IP phone. For Cisco Unified SIP IP phones, if the first character of the string is a plus sign (+), the speed-dial number is locked and cannot be changed at the phone. If the only character in the string is a pound sign (#), the user-programmable speed-dial button with no speed-dial number attached is defined.
label *label-text*	(Optional) String that contains identifying text to be displayed next to the speed-dial button. Enclose the string in quotation marks if the string contains a space.

Command Default

The Cisco Unified SIP IP phone cannot make or receive an intercom call.

Command Modes

Voice register dn configuration (config-register-dn)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The intercom line cannot be the primary line of a Cisco Unified SIP IP phone and cannot be shared among Cisco Unified SIP IP phones.

When the intercom speed-dial option is not configured, the intercom line waits for the user to dial the destination number.

Examples

The following example shows SIP intercom configured on extension 1001:

```
Router(config)# voice register dn  1
Router(config-register-dn) number 1001
Router(config-register-dn) intercom [speed-dial 1002] [label intercom1001]
Router(config)# voice register pool 1
Router(config-register-pool) id mac 001D.452D.580C
Router(config-register-pool) type 7962
Router(config-register-pool) number 1 dn 2
Router(config-register-pool) number 2 dn 1
```

Related Commands

Command	Description
voice register dn	Enters voice register dn configuration mode.
voice register pool	Enters voice register pool configuration mode.

internal-call

To assign an MOH group for calls from an internal directory number, use the **internal-call** command in telephony-service configuration mode. To disable the internal-call command, use the **no** form of this command.

internal-call moh-group-tag
no internal-call

Syntax Description

moh-group-tag	Specifies a MOH-group number to be used for calls from an internal directory number. Range is from 0 to 5, where 0 represents MOH configuration in telephony-service configuration mode.

Command Default

No internal-call is configured.

Command Modes

Telephony-service configuration (config-telephony-service)

Command History

Cisco IOS Release	Cisco Product	Modification
15.0(1)XA	Cisco Unified CME 8.0	This command was introduced.
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Before using this command make sure you have MOH-groups configured under voice-moh-group configuration mode. This command allows you to assign a MOH-group for all calls from an internal directory number. MOH group tag identifies the unique number assigned to a MOH group. Range for MOH group tag is from 0 to 5, where 0 represents MOH configuration in telephony service.

Examples

The following example shows MOH-group 4 assigned for an internal directory number:

```
telephony-service
 internal-call moh-group 4
 em logout 0:0 0:0 0:0
 max-ephones 58
 max-dn 192
 ip source-address 15.1.0.161 port 2000
 max-conferences 8 gain -6
 moh music-on-hold.au
 multicast moh 239.1.1.1 port 2000
 transfer-system full-consult
```

Related Commands

Command	Description
voice-moh-group	Enter voice-moh-group configuration mode.
moh filename	Enables music on hold from a flash audio feed
multicast moh	Enables multicast of the music-on-hold audio stream.
extension-range	Specifies the extension range for a clients calling a voice-moh-group.

ip address trusted authenticate

To enable ip address trusted authentication for incoming VoIP (H.323/SIP) calls, use the **ip address trusted authenticate** command in voice service voip mode. To disable ip address trusted authentication, use the no form of this command.

ip address trusted authenticate
no ip address trusted authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

IP address trusted list authenticate is enabled.

Command Modes

Voice Service Voip

Command History

Cisco IOS Release	Cisco Product	Modification
15.1(2)T	Cisco Unified CME 8.1	This command was introduced.

Usage Guidelines

Use this command to enable the ip address trusted authentication for incoming H.323 or SIP trunk calls for toll fraud prevention on Cisco Unified CME.

Examples

The following is a sample output from this command displaying IP address trusted authentication enabled for incoming calls:

```
IP Address Trusted Authentication
 Administration State: UP
 Operation State:      UP
IP Address Trusted Call Block Cause: call-reject (21)
VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1
IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
```

Related Commands

Command	Description
ip address trusted list	Allows to manually add additional valid IP addresses.
ip address trusted call- block cause	Allows to issues a cause-code when the incoming call is rejected by the IP address trusted authentication.

ip address trusted call-block cause

To issues a cause-code when the incoming call is rejected by the IP address trusted authentication, use the **ip address trusted call-block cause** command in voice service voip mode. To stop the IP address trusted authentication process from sending a call-block cause, use the no form of this command.

ip-address trusted call-block cause code-id
no ip-address trusted call-block cause code-id

Syntax Description

code-id	Q.850 call-disconnect cause code. Range is from 1 to 127.

Command Default

A call-reject (21) cause-code is issued to disconnect the incoming VoIP calls.

Command Modes

Voice Service voip.

Command History

Cisco IOS Release	Cisco Product	Modification
15.1(2)T	Cisco Unified CME 8.1	This command was introduced.

Usage Guidelines

Use this command to issue a cause-code when the incoming call is rejected by the IP address trusted authentication. You can issue a specific call-block cause code using any one of the Q.850 call reject cause codes.

Examples

The following is a sample output from this command displaying the default call block cause code:

```
Router #show ip address trusted list
IP Address Trusted Authentication
 Administration State: UP
 Operation State:      UP
IP Address Trusted Call Block Cause: call-reject (21)
VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1
```

Related Commands

Command	Description
ip address trusted list	Allows to manually add additional valid IP addresses.
ip address trusted authenticate	Enables IP address trusted authentication for incoming VoIP calls.

ip address trusted list

To manually add multiple IP addresses for incoming VoIP (H.323/SIP) calls, use the **ip address trusted list** command in voice service voip mode. To turn off the list, use the no form of this command.

ip address trusted list ipv4 ipv4 address network mask
no ip address trusted list ipv4 ipv4 address network mask

Syntax Description

ipv4-address	IPv4 address of the incoming H.323 or SIP calls.
network mask	Subnet IP address.

Command Default

IP address trusted list is disabled.

Command Modes

Voice Service Voip.

Command History

Cisco IOS Release	Cisco Product	Modification
15.1(2)T	Cisco Unified CME 8.1	This command was introduced.

Usage Guidelines

Use this command to manually add unique and multiple IP addresses to a list of trusted IP addresses. You can add up to 100 IPv4 addresses in the ip address trusted list. No duplicate IP addresses are allowed.

Examples

The following is a sample output from this command displaying a list of trusted IP addresses:

```
Router #show ip address trusted list
IP Address Trusted Authentication
 Administration State: UP
 Operation State:      UP
IP Address Trusted Call Block Cause: call-reject (21)
VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1
IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
```

Related Commands

Command	Description
IP address trusted authenticate	Enables IP address trusted authentication for incoming VoIP calls.
IP address trusted code-block cause	Allows to issues a cause-code when the incoming call is rejected by the IP address trusted authentication.

ip qos dscp (telephony-service and voice register global)

To set the Differentiated Services Code Point (DSCP) for marking the quality of service (QoS) requirements for each packet, use the **ip qos dscp** command in telephony-service or voice register global configuration mode. To reset to the default value, use the **no** form of this command.

ip qos dscp {*numberafcs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}
no ip qos dscp {*numberafcs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}

Syntax Description

number	DSCP value. Range: 0 to 63.
af	Sets DSCP to assured forwarding bit pattern. • **af11**—bit pattern 001010 • **af12**—bit pattern 001100 • **af13**— bit pattern 001110 • **af21**— bit pattern 010010 • **af22**— bit pattern 010100 • **af23**— bit pattern 010110 • **af31**— bit pattern 011010 • **af32**— bit pattern 011100 • **af33**— bit pattern 011110 • **af41**—bit pattern 100010 • **af42**—bit pattern 100100 • **af43**—bit pattern 100110
cs	Sets DSCP to class-selector codepoint. • **cs1**—codepoint 1 (precedence 1) • **cs2**—codepoint 2 (precedence 2) • **cs3**—codepoint 3 (precedence 3) • **cs4**—codepoint 4 (precedence 4) • **cs5**—codepoint 5 (precedence 5) • **cs6**—codepoint 6 (precedence 6) • **cs7**—codepoint 7 (precedence 7)
default	Sets DSCP to default bit pattern of 000000.
ef	Sets DSCP to expedited forwarding bit pattern 101110.
media	Applies DSCP to media payload packets.
service	Applies DSCP to phone service including HTTP traffic.
signaling	Applies DSCP to signaling packets.
video	Applies DSCP to video stream.

Command Default

DSCP for media is **ef**. DSCP for service is **0**. DSCP for signaling is **cs3**. DSCP for video is **af41**.

Command Modes

Telephony-service configuration (config-telephony)
Voice register global configuration (config-register-global)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(22)YB	Cisco Unified CME 7.1	This command was introduced.
12.4(24)T	Cisco Unified CME 7.1	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command allows you to set different priority levels for different types of network traffic sent by the Cisco Unified CME router. Differentiated Services is a method of prioritizing specific network traffic based on the QoS specified by each packet. You can set different DSCP values, for example, for video and audio streams.

Cisco Unified CME downloads the configured DSCP value to the phones in their configuration files and all control messages and RTP streams are marked with the preferred DSCP value. Use this command in telephony-service mode to set the DSCP for SCCP phones. Use the command in voice register global mode to set the value for SIP phones.

If the DSCP is configured for the gateway interface using the **service-policy** command or in the dial peer using the **ip qos dscp** command, the value set with those commands takes precedence over the DSCP value configured with this command.

Examples

The following examples show the configuration of DSCP for different types of packets .

```
voice register global
 mode cme
 ip qos dscp af11 media
 ip qos dscp cs2 signal
 ip qos dscp af43 video
 ip qos dscp 25 service

telephony-service
 load 7960-7940 P00308000500
 max-ephones 100
 max-dn 240
 ip source-address 10.7.0.1 port 2000
 ip qos dscp af11 media
 ip qos dscp cs2 signal
 ip qos dscp af43 video
 ip qos dscp 25 service
```

Related Commands

Command	Description
ip qos dscp	Sets the DSCP for QoS in a dial peer.
service-policy	Assigns a policy map to an interface that will be used as the service policy for the interface.

ip source-address (credentials)

To enable the Cisco Unified CME or Cisco Unified SRST router to receive credential service messages through the specified IP address and port, use the **ip source-address** command in credentials configuration mode. To disable the router from receiving messages, use the **no** form of this command.

ip source-address *ip-address* [**port** [*port*]]
no ip source-address

Syntax Description

ip-address	Router IP address, typically one of the addresses of the Ethernet port of the local router.
port *port*	(Optional) TCP port for credentials service communication. Range is from 2000 to 9999. Cisco Unified CME default is 2444. SRST default is 2445.

Command Default

Default port number in Cisco Unified CME is 2444. Default port number in Cisco Unified SRST is 2445.

Command Modes

Credentials configuration (config-credentials)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(14)T	Cisco SRST 3.3	This command was introduced for Cisco SRST.
12.4(4)XC	Cisco Unified CME 4.0	This command was introduced for Cisco Unified CME.
12.4(9)T	Cisco Unified CME 4.0	This command for Cisco Unified CME was integrated in Cisco IOS Release 12.4(9)T.

Usage Guidelines

Cisco Unified CME

This command is used with Cisco Unified CME phone authentication to identify a Cisco Unified CME router on which a CTL provider is being configured.

Cisco Unified SRST

The **ip source-address** command is a mandatory command to enable secure SRST. If the port number is not provided, the default value (2445) is used. The IP address is usually the IP address of the secure SRST router.

Examples

Cisco Unified CME

The following example creates a CTL provider on a Cisco Unified CME router that is not running the CTL client.

```
Router(config)# credentials
Router(config-credentials)# ip source-address 172.19.245.1 port 2444
Router(config-credentials)# trustpoint ctlpv
Router(config-credentials)# ctl-service admin user4 secret 0 c89L8o
```

Cisco Unified SRST

The following example enters credentials configuration mode and sets the IP source address and port:

```
Router(config)# credentials
Router(config-credentials)# ip source-address 10.6.21.4 port 2445
```

Related Commands

Command	Description
ctl-service admin	Specifies a user name and password to authenticate the CTL client during the CTL protocol.
debug credentials	Sets debugging on the credentials service that runs between a Cisco Unified CME CTL provider and the CTL client or between an SRST router and Cisco Unified CallManager.
show credentials	Displays the credentials settings on a Cisco Unified CME or SRST router.
trustpoint (credentials)	Specifies the name of the trustpoint to be associated with a Cisco Unified CME CTL provider certificate or with an SRST router certificate.

ip source-address (telephony-service)

To identify the IP address and port through which IP phones communicate with a Cisco Unified CME router, use the **ip source-address** command in telephony-service or group configuration mode. To disable the router from receiving messages from Cisco Unified IP phones, use the **no** form of this command.

ip { *ipv4_address*| *ipv6_address*} [port*port*] [secondary {*ipv4 address* |*ipv6 address*} [rehome*seconds*]] [any-match | strict-match]
no ip source-address

Syntax Description

ipv4_address	IPv4 address of the router, typically one of the addresses of the Ethernet port of the router.
ipv6_address	In Cisco Unified CME 8.0 and later versions: IPv6 address of the router, typically one of the addresses of the Ethernet port of the router.
port *port*	(Optional) TCP/IP port number to use for Skinny Client Control Protocol (SCCP). Default is 2000. For IPv4 only: Range is from 2000 to 9999. **Note** For IPv6, do not configure the port number to change from the default value (2000).
secondary	(Optional) Second Cisco Unified CME router with which phones can register if the primary Cisco Unified CME router fails. **Note** For dual-stack (IPv4 and IPv6) mode: Only an IPv4 address can be configured for a secondary router.
rehome *seconds*	(Optional) Used only by Cisco Unified IP phones that have registered with a Cisco Unified Survivable Remote Site Telephony (SRST) router. This keyword defines a delay that is used by phones to verify the stability of their primary SCCP controller (Cisco Unified Communications Manager or Cisco Unified CME) before the phones reregister with it. This parameter is ignored by phones unless they are registered to a secondary Cisco Unified SRST router. The range is from 0 to 65535 seconds. The default is 120 seconds. The use of this parameter is a phone behavior and is subject to change, based on the phone type and phone firmware version.
strict-match	(Optional) Requires strict IP address checking for registration.

Command Default

The IP address for communicating with phones is not defined.

Command Modes

Telephony-service configuration (config-telephony)
Group configuration (conf-tele-group)

Command History

Cisco IOS Release	Cisco Product	Modification
12.1(5)YD	Cisco ITS 1.0	This command was introduced.
12.2(8)T	Cisco ITS 2.0	This command was integrated into Cisco IOS Release 12.2(8)T.

Cisco IOS Release	Cisco Product	Modification
12.4(4)XC	Cisco Unified CME 4.0	The **secondary** *ip-address* and **rehome** *seconds* keyword-argument pairs were added.
12.4(9)T	Cisco Unified CME 4.0	The **secondary** *ip-address* and **rehome** *seconds* keyword-argument pairs were added.
12.4(22)T	Cisco Unified CME 7.0(1)	This command was added to VRF group mode.
15.0(1)XA	Cisco Unified CME 8.0	This command was modified. Support for IPv6 was added and the *ipv4-address* and ipv6-*address arguments replaced the generic ip-address argument.*
15.1(1)T	Cisco Unified CME 8.0	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command enables a router to receive messages from Cisco Unified IP phones through the specified IP address and port.

The Cisco Unified CME router cannot communicate with Cisco Unified CME phones if the IP address of the port to which they are attached is not configured. In Cisco Unified CME 8.0 and later versions, the Cisco Unified CME router can receive messages from IPv6-enabled or IPv4-enabled IP phones or from phones in dual-stack (both IPv6 and IPv4) mode.

- In Cisco Unified CME 8.0 and later versions: If the IP phones connected to Cisco Unified CME were configured for dual-stack mode by using **dual-stack** keyword with the **protocol mode** command, configure this command with the IPv6 address.
- In Cisco Unified CME 8.0 and later versions: If the IP phones to be connected to the port to be configured are IPv4-enabled only *or* IPv6-enabled only, configure this command with the corresponding IPv4 or IPv6 address.

For IPv6: Do not configure the **port** *port* keyword argument combination in this command to change the value from the default (2000). If you change the port number, IPv6 CEF packet switching engine will not be able to handle the IPv6 SCCP phones and various packet handling problems may occur when more than a dozen (approximately) calls in IPv6 are going on.

Use the **strict-match** keyword to instruct the router to reject IP phone registration attempts if the IP server address used by the phone does not match the source address.

Prior to Cisco IOS Telephony Services (Cisco ITS) V2.1, this command helped the router to autogenerate the SEPDEFAULT.cnf file, which was stored in the flash memory of the router. The SEPDEFAULT.cnf file contains the IP address of one of the Ethernet ports of the router to which the phone should register.

In ITS V2.1 and in Cisco CME 3.0 and later versions, the configuration files were moved to system:/its/. The file named Flash:SEPDEFAULT.cnf that was used with previous Cisco ITS versions is obsolete, but is retained as system:/its/SEPDEFAULT.cnf to support upgrades from older phone firmware.

For systems using Cisco ITS V2.1 or later versions, the IP phones receive their initial configuration information and phone firmware from the TFTP server associated with the router. In most cases, the phones obtain the IP address of their TFTP server using the **option 150** command and Dynamic Host Configuration Protocol (DHCP). For Cisco ITS or Cisco CME operation, the TFTP server address obtained by the Cisco Unified IP phones should point to the router IP address. The Cisco IP phones attempt to transfer a configuration file called XmlDefault.cnf.xml. This file is automatically generated by the router through the **ip source-address** command and is placed in router memory. The XmlDefault.cnf.xml file contains the IP address that the phones

use to register for service, using the SCCP. This IP address should correspond to a valid Cisco CME router IP address (and may be the same as the router TFTP server address).

Similarly, when an analog telephone adapter (ATA) such as the ATA-186 is attached to the Cisco Unified CME router, the ATA receives very basic configuration information and firmware from the TFTP server XmlDefault.cnf.xml file. The XmlDefault.cnf.xml file is automatically generated by the Cisco Unified CME router with the **ip source-address** command and is placed in the router's flash memory.

By specifying a second Cisco Unified CME router in the **ip source-address** command, you improve the failover time for phones.

Examples

The following example sets the IP source address and port:

```
Router(config)# telephony-service
Router(config-telephony)# ip source-address 10.6.21.4 port 2000 strict-match
```

The following example establishes the router at 10.5.2.78 as a secondary router:

```
Router(config)# telephony-service
Router(config-telephony)# ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78
```

Cisco Unified CME 8.0 and Later Versions

The following example shows how to configure this command with an IPv6 address. Do not change the port number from the default value (2000) when you configure an IPv6 address.

```
Router(config)# telephony-service
Router(config-telephony)#protocol mode ipv6
Rounter(config-telephony)ip source-address 2001:10:10:10::3
```

The following example shows how to configure an IP address for dual-stack mode. When the IP phones are configured for dual-stack mode, the IP address of the router port to which the IP phones are connected must be an IPv6 address. For dual-stack mode, the address of the secondary router must be an IPv4 address.

```
Router(config)# telephony-service
Router(config-telephony)# protocol mode dual-stack
Router(config-telephony)# ip source address
2001:10:10:10::3 secondary 10.5.2.78
Router(config-telephony)#
```

Related Commands

Command	Description
option	Configures DHCP server options.
protocol mode	Configures a preferred IP-address mode for SCCP IP phones in Cisco Unified CME.