

L

- link (RLM), on page 2
- listen-port (SIP), on page 3
- listen-port (tenant), on page 5
- lmr duplex half, on page 7
- lmr e-lead, on page 8
- lmr ip-vad, on page 10
- lmr led-on, on page 11
- lmr m-lead, on page 12
- load-balance, on page 13
- local, on page 14
- localhost, on page 15
- loopback (controller), on page 17
- loop-detect, on page 19
- loss-plan, on page 20
- lrq e164 early-lookup, on page 22
- lrq forward-queries, on page 23
- lrq lrj immediate-advance, on page 26
- lrq reject-resource-low, on page 27
- lrq reject-unknown-circuit, on page 28
- lrq reject-unknown-prefix, on page 29
- lrq timeout blast window, on page 31
- lrq timeout seq delay, on page 32

link (RLM)

To enable a Redundant Link Manager (RLM) link, use the **link** command in RLM configuration mode. To disable this function, use the **no** form of this command.

link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*
no link {**hostname** *name* | **address** *ip-address*} **source** *loopback-source* **weight** *factor*

Syntax Description

hostname name	RLM host name. If host name is used, RLM looks up the DNS server periodically for the host name configured until lookup is successful or the configuration is removed.
address *ip -address*	IP address of the link.
source *loopback -source*	Loopback interface source. We recommend that you use the loopback interface as the source, so that it is independent of the hardware condition. Also, the source interface should be different in every link to avoid falling back to the same routing path. If you intend to use the same routing path for the failover, a single link is sufficient to implement it.
weight *factor*	An arbitrary number that sets link preference. The higher the weighting factor number assigned, the higher priority it gets to become the active link. If all entries have the same weighting factor assigned, all links are treated equally. There is no preference among servers according to the assumption that only one server accepts the connection requests at any given time. Otherwise, preferences are extended across all servers.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

This command is a preference-weighted multiple entries command. Within the same server, the link preference is specified in weighting.

Examples

The following example specifies the RLM group (network access server), device name, and link addresses and their weighting preferences:

```
rlm group 1
 server rl-server
  link address 10.1.4.1 source Loopback1 weight 4
  link address 10.1.4.2 source Loopback2 weight 3
```

listen-port (SIP)

To configure the listen ports used for SIP protocols, use the **listen-port** command in **voice service voip/sip** configuration mode. To reset port use to its default value, use the **no** form of this command.

listen-port [**non-secure** | **secure**] *port-number*
no listen-port [**non-secure** | **secure**]

Syntax Description

secure	Specifies the TLS port value.
non-secure	Specifies the TCP/UDP port value.
port-number	Port number. Range: 1–65535. The default for UDP/TCP is 5060; the default for TLS is 5061.

Command Default

The port number is set to the default value based on the transport layer protocol used.

Command Modes

SIP configuration mode (config-serv-sip)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **listen-port** command is configurable on incoming SIP calls, and is applicable for both TDM-IP gateway and CUBE (IPIPGW). The CUBE gateway port number defined in global configuration will be used for In leg . Before configuring the SIP listen port for TCP/UDP/TLS, SIP service should be shut down using the **shutdown** in SIP configuration mode. If SIP service is not shut down, the **listen-port** command flashes an error message saying "shutdown SIP service before changing SIP listen port". This ensures that there are no active calls when the SIP listen port is changed. The **non-secure** keyword is supported on images, and both the **secure** and **non-secure** keywords are supported on Crypto images.

The following restrictions apply:

- Configuring the SIP listen port on a dial-peer basis is not supported.
- Configuring same listening port for both UDP/TCP and TLS is not allowed.
- Configuring the SIP listen port to a port that is already in use is not supported and results in an error message.
- Changing SIP listen port when Transport services (TCP/UDP/TLS) are shut down, will not close or reopen the port. The result is that only the new port number is updated. The new port will be bound when Transport services (TCP/UDP/TLS) is enabled.

Examples

The following example shows the port number on a Crypto image being changed to port 2000:

```
Router(config-serv-sip)# listen-port secure 2000
```

The following example shows the port number being reset to the TLS default port:

```
Router(config-serv-sip)# no listen-port
```

Related Commands

Command	Description
shutdown	Disables the port.

listen-port (tenant)

To set a specific SIP listen port in a tenant configuration, use the **listen-port** command in voice class tenant configuration mode. By default, tenant level listen port is not set and global level SIP listen port is used. To disable tenant level listen port, use the **no** form of this command.

listen-port { **secure** *port-number* | **non-secure** *port-number* }
no listen-port { **secure** *port-number* | **non-secure** *port-number* }

Syntax Description

secure	Specifies the TLS port value.
non-secure	Specified the TCP/UDP port value.
port-number	• Secure port number range: 1—65535. • Non-secure port number range: 5000—5500. **Note** Port range is restricted to avoid conflicts with RTP media ports that also use UDP transport.

Command Default

The port number will not be set to any default value.

Command Modes

Voice Class Tenant configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	This command is introduced.

Usage Guidelines

Before the introduction of this feature, it was only possible to configure the listen port for SIP signaling at the global level (see listen-port (SIP)) and this value could only be changed if the call processing service was shut down first. It is now possible to specify a listen port for both secure and non-secure traffic within a tenant configuration, allowing SIP trunks to be selected more flexibly. Tenant listen ports may be changed without shutting down the call processing service, provided that there are no active calls on the associated trunk. If the listen port configuration is removed, all active connections associated with the port are closed.

For reliable call processing, ensure that signaling and media interface binding is configured for all tenants that include a listen port and also that interface binding (for VRF and IP address) and listen port combinations are unique across all tenants and global configurations.

Examples

The following is a configuration example for **listen-port***secure*:

```
Router(config)#voice class tenant 1
VOICECLASS configuration commands:
  aaa                  sip-ua AAA related configuration
  authentication       Digest Authentication Configuration
  credentials          User credentials for registration
  ...
  ...
  listen-port         Configure UDP/TCP/TLS SIP listen port (have bind
                      configured under this tenant for the config to take
                      effect)
```

```
  ...

Router(config-class)#listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#listen-port secure ?
  <0-65535>  Port-number

Router(config-class)#listen-port secure 5062
```

The following is a configuration example for **listen-port***non-secure*:

```
Router(config)#voice class tenant 1
VOICECLASS configuration commands:
  aaa                  sip-ua AAA related configuration
  authentication       Digest Authentication Configuration
  credentials          User credentials for registration
  ...
  ...
  listen-port         Configure UDP/TCP/TLS SIP listen port (have bind
                      configured under this tenant for the config to take
                      effect)
 ...

Router(config-class)#listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#listen-port non-secure ?
  <5000-5500>  Port-number

Router(config-class)#listen-port non-secure 5404
```

The following is a configuration example for **no listen-port**:

```
Router(config-class)# no listen-port ?
  non-secure  Change UDP/TCP SIP listen port (have bind configured under this
              tenant for the config to take effect)
  secure      Change TLS SIP listen port (have bind configured under this
              tenant for the config to take effect)

Router(config-class)#no listen-port secure ?
  <0-65535>  Port-number

Router(config-class)#no listen-port secure
```

Related Commands

Command	Description
call service stop	Shutdown SIP service on CUBE.
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

lmr duplex half

To have the voice path for a voice port operate in half duplex mode, use the **lmr duplex half** command in voice-port configuration mode. To return to the default, use the **no** form of this command.

lmr duplex half
no lmr duplex half

Syntax Description

This command has no arguments or keywords.

Command Default

Full duplex mode

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

When a radio system is receiving voice traffic from the radio, operating the voice path in half duplex mode prevents the speaker from being interrupted and prevents the voice stream from being fed back to itself.

Examples

In the following example, the voice path for voice port 1/0/0 on a Cisco 3700 series router is set to operate in half duplex mode:

```
voice-port 1/0/0
 lmr duplex half
```

lmr e-lead

To define the use of the E-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr e-lead**command in voice-port configuration mode. To return to the default use of the E-lead, use the **no** form of this command.

lmr e-lead {**inactive** | **seize** | **voice**}
no lmr e-lead {**inactive** | **seize** | **voice**}

Syntax Description

inactive	Specifies that the router never sends a seize signal on the E-lead to the LMR device. The router sends voice packets to LMR devices.
seize	Specifies that for PLAR and multicast connections, the router sends a seize signal on the E-lead when the LMR port is connected and removes the seize signal from the E-lead when the LMR port is not involved in a VoIP connection. This is the default. Specifies that for connection trunk connections, the router does not send a seize signal when the LMR port is connected. Instead, if the trunk connection is up, the M-lead signal from the far-end router is passed through as the E-lead on the near-end router. When the M-lead is dropped on the far-end router and the trunk connection is still up, the E-lead is dropped on the near-end router.
voice	Specifies that the router sends a seize signal on the E-lead only when it receives voice packets from the network. When no packets are detected on the network, the seize signal is removed from the E-lead.

Command Default

seize

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under E-lead control. Use the **lmr e-lead** command to configure the voice port when using private line, automatic ringdown (PLAR) connections. The E-lead connects to the Push To Talk (PTT) of the LMR system.

Examples

In the following example, packet transmission from the E&M voice port on a Cisco 3745 to an attached LMR radio system is disabled:

```
lmr e-lead inactive
```

Related Commands

Command	Description
lmr m-lead	Defines the use of the M-lead in signaling between the E&M voice port on the router and the attached LMR device.

lmr ip-vad

To configure the Land Mobile Radio (LMR) digital signal processor (DSP) on a Cisco 2800 series integrated services router to report a voice packet arrival event only if the packet contains voice energy, use the **lmr ip-vad** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

lmr ip-vad
no lmr ip-vad

Syntax Description

This command has no arguments or keywords.

Command Default

Any voice packet received from the IP network side triggers the DSP to report a voice packet arrival event to the Cisco IOS software.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **lmr ip-vad** command applies to a voice interface card (VIC) in a Cisco 2800 series integrated services router if the VIC is one of the following types of ear and mouth (E&M) interfaces:

- VIC2-2E/M with signal type LMR
- ds0-group created with signal type e&m-lmr under an E1 or T1 controller

The **lmr ip-vad** command configures the LMR DSP to report voice activity detection (VAD) status change events (rather than voice packet arrival events) for a supported voice interface in a Cisco 2800 series integrated services router.

Examples

The following example shows a sequence of commands that can be used to configure a voice port so that a voice packet arrival event is reported to the Cisco IOS software on the router only if the packet contains voice energy.

```
Router(config)# voice-port 1/1/0

Router(config-voiceport)# signal lmr

Router(config-voiceport)# lmr ip-vad
```

Related Commands

Command	Description
signal	Configures the type of signaling to be used for a voice port.
voice-port	Enters voice-port configuration mode.

lmr led-on

To use the ear and mouth (E&M) LED to indicate the E-lead and M-lead status, use the **lmr led-on** command in voice-port configuration mode. To return to the default use of the E&M LED, use the **no** form of this command.

lmr led-on
no lmr led-on

Syntax Description

This command has no arguments or keywords.

Command Default

The E&M LED indicates voice port activity only.

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr e-lead** command is available on an E&M voice port only if the signal type for that port is Land Mobile Radio (LMR). This command enables the use of the E&M LED to indicate the E-lead and M-lead status as follows:

- Red--E-lead active
- Green--M-lead active
- Yellow--Both E-lead and M-lead active

The default behavior of the E&M LED is to light up when there is activity on the voice port and to turn off when there is no activity.

Examples

The following example specifies that the E&M LED is used to indicate the E-lead and M-lead status:

```
voice-port 1/0/0
 lmr led-on
```

lmr m-lead

To define the use of the M-lead in signaling between the ear and mouth (E&M) voice port on the router and the attached Land Mobile Radio (LMR) device, use the **lmr m-lead**command in voice-port configuration mode. To return to the default use of the M-lead, use the **no** form of this command.

lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}
no lmr m-lead {**inactive** | **audio-gate-in** | **dialin**}

Syntax Description

inactive	The router ignores signals sent by voice on the M-lead. The flow of voice packets is determined by voice activity detection (VAD). The router sends voice received from the LMR device. This is the default.
audio-gate-in	The router generates VoIP packets when a seize signal is detected on the M-lead. The router stops generating VoIP packets when the seize signal is removed from the M-lead.
dialin	When the LMR device is not involved in a VoIP connection, the first seize signal detected on the M-lead triggers the router to set up a VoIP connection. Once the connection is made, the router behaves as in the **audio-gate-in** option.

Command Default

inactive

Command Modes

Voice-port configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

The **lmr m-lead** command has an effect on an ear and mouth (E&M) voice port only if the signal type for that port is LMR. The **lmr e-lead** command is effective only if the attached LMR device operates under M-lead control. The M-lead corresponds to the Carrier Operated Relay (COR) of the LMR system, which indicates receive activity on the LMR system.

Examples

In the following example, an LMR radio system attached to the E&M voice port on a Cisco 3745 is allowed to transmit audio by first raising the E-lead, then transmitting:

```
lmr m-lead dialin
```

Related Commands

Command	Description
lmr e-lead	Defines the use of the E-lead in signaling between the E&M voice port on the router and the attached LMR device.

load-balance

To configure load balancing, use the **load-balance**command ingatekeeper configuration mode. To disable load balancing, use the **no** form of this command.

load-balance [**endpoints** *max-endpoints*] [**calls** *max-calls*] [**cpu** *max-cpu*] [**memory** *max-em-used*]
no load-balance [**endpoints** *max-endpoint* **s**] [**calls** *max-calls*] [**cpu** *max-cpu*] [**memory** *max-mem-used*]

Syntax Description

endpoints *max -endpoints*	(Optional) Maximum number of endpoints.
calls *max-calls*	(Optional) Maximum number of calls.
cpu *max -cpu*	(Optional) Maximum percentage of CPU utilization.
memory *max -mem-used*	(Optional) Maximum percentage of memory used.

Command Default

Load balancing is performed by the gatekeeper.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Usage Guidelines

Load balancing occurs when one gatekeeper reaches the default or the configured load level. Upon reaching the load-level threshold, the gatekeeper begins sending alternate gatekeeper information in Registration, Admission, and Status (RAS) messages, and the gateways then attempt to migrate from the loaded gatekeeper to its least busy alternate. The move is permanent; endpoints are not actively moved back to the original gatekeeper if it stabilizes. However, they may return to that gatekeeper if the new gatekeeper reaches a load threshold and transfers them again. The gatekeepers share the load, but they may not have equal shares. The process of load balancing allows for more effective zone management.

Examples

The following example configures load balancing:

```
load-balance endpoints 200 calls 100 cpu 75 memory 80
```

Related Commands

Command	Description
zone cluster local	Configures alternate gatekeepers for each zone.

local

To define the local domain, including the IP address and port that the border element (BE) should use for interacting with remote BEs, use the **local** command in Annex G configuration mode. To reset to the default, use the no form of this command.

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

Syntax Description

ip *ip -address*	IP address of the local border element.
port *local -port*	(Optional) Port number of the local border element, which is used for exchanging Annex G messages. Default is 2099.

Command Default

Port number: 2099

Command Modes

Annex G configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The local IP address can be a virtual Hot Standby Routing Protocol (HSRP) address for high reliability and availability. You can configure multiple gatekeepers and BEs identically and use HSRP to designate a primary BE and other standby BEs. If the primary BE is down, a standby BE operates in its place.

Examples

The following example sets the IP address and port that the BE should use. (Note that this example uses a nonstandard port number. If you do not want to use a nonstandard port number, use the default value of 2099.)

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# local ip 121.90.10.80 port 2010
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.
show call -router status	Displays the Annex G BE status.

localhost

To globally configure Cisco IOS voice gateways, Cisco Unified Border Elements (Cisco UBEs), or Cisco Unified Communications Manager Express (Cisco Unified CME) to substitute a Domain Name System (DNS) hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **localhost** command in voice service SIP configuration mode or voice class tenant configuration mode. To remove a DNS localhost name and disable substitution for the physical IP address, use the **no** form of this command.

localhost dns: [*hostname.*] *domain* [**preferred**]
no localhost

Syntax Description

dns: [*hostname.*]*domain*	Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages. This value can be the hostname and the domain separated by a period (**dns:** *hostname.domain*) or just the domain name (**dns:** *domain*). In both case, the **dns:** delimiter must be included as the first four characters.
preferred	(Optional) Designates the specified DNS hostname as preferred.

Command Default

The physical IP address of the outgoing dial peer is sent in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages.

Command Modes

Voice service SIP configuration (conf-serv-sip).

Voice class tenant configuration (config-class).

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)XA	This command was modified. The **preferred** keyword was added to specify the preferred localhost if multiple registrars are configured on a SIP trunk.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(1)T	This command was integrated into Cisco IOS Release 5.1(1)T.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **localhost** command in voice service SIP configuration mode to globally configure a DNS localhost name to be used in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on Cisco IOS voice gateways, Cisco UBEs, or Cisco Unified CME. When multiple registrars are configured you can then use the **localhost preferred** command to specify which host is preferred.

To override the global configuration and specify DNS localhost name substitution settings for a specific dial peer, use the **voice-class sip localhost** command in dial peer voice configuration mode. To remove a globally configured DNS localhost name and use the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages, use the **no localhost** command.

Examples

The following example shows how to globally configure a preferred DNS localhost name using only the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:example.com preferred
```

The following example shows how to globally configure a preferred DNS localhost name by specifying the hostname along with the domain for use in place of the physical IP address in outgoing messages on all dial peers:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# localhost dns:MyHostname.example.com preferred
```

Related Commands

Command	Description
authentication (dial peer)	Enables SIP digest authentication on an individual dial peer.
authentication (SIP UA)	Enables SIP digest authentication.
credentials (SIP UA)	Configures a Cisco UBE to send a SIP registration message when in the UP state.
registrar	Enables Cisco IOS SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar.
voice-class sip localhost	Configures settings for substituting a DNS localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers of outgoing messages on an individual dial peer, overriding the global setting.

loopback (controller)

To set the loopback method for testing a T1 or E1 interface, use the **loopback** command in controller configuration mode. To reset to the default, use the **no** form of this command.

loopback {**diagnostic** | **local** {**payload** | **line**} | **remote** {**v54 channel-group** *channel-number* | **iboc** | **esf** {**payload** | **line**}}}
no loopback

Syntax Description

diagnostic	Loops the outgoing transmit signal back to the receive signal.
local	Places the interface into local loopback mode.
payload	Places the interface into external loopback mode at the payload level.
line	Places the interface into external loopback mode at the line level.
remote	Keeps the local end of the connection in remote loopback mode.
v54 channel -group	Activates a V.54 channel-group loopback at the remote end. Available for both T1 and E1 facilities.
channel -number	Channel number for the V.54 channel-group loopback. Range is from 0 to 1.
iboc	Sends an inband bit-oriented code to the far end to cause it to go into line loopback.
esf	T1 or E1 frame type of Extended Super Frame (ESF). Only available under T1 or E1 controllers when ESF is configured on the controller. The following are keywords: • **payload** --Activates remote payload loopback by sending Facility Data Link (FDL) code. FDL is a 4-kbps out-of-band signaling channel in ESF. • **line** --Activates remote line loopback by sending FDL code.

Command Default

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced as a controller configuration command for the Cisco MC3810.
12.0(5)T and 12.0(5)XK	This command was introduced as an ATM interface configuration command for the Cisco 2600 series and Cisco 3600 series.
12.0(5)XE	This command was introduced as an ATM interface configuration command for the Cisco 7200 series and Cisco 7500 series.

Release	Modification
12.0(5)XK and 12.0(7)T	This command was introduced as a controller configuration command for the Cisco 2600 series and Cisco 3600 series.
12.1(1)T	This command was modified as a controller configuration command for the Cisco 2600 series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused either by the line and channel service unit/digital service unit (CSU/DSU) or by the interface. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example sets the diagnostic loopback method on controller T1 0/0:

```
controller t1 0/0
 loopback diagnostic
```

The following example sets the payload loopback method on controller E1 0/0:

```
controller e1 0/0
 loopback local payload
```

loop-detect

To enable loop detection for T1, use the **loop-detect** command in controller configuration mode. To cancel loop detection, use the no form of this command.

loop-detect
no loop-detect

Syntax Description

This command has no arguments or keywords.

Command Default

Loop detection is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM.

Examples

The following example configures loop detection for controller T1 0:

```
controller t1 0
 loop-detect
```

Related Commands

Command	Description
loopback (interface)	Diagnoses equipment malfunctions between an interface and a device.

loss-plan

To specify the analog-to-digital gain offset for an analog Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **loss-plan**command in voice-port configuration mode. To reset to the default, use the **no**form of this command.

loss-plan {**plan1** | **plan2** | **plan3** | **plan4** | **plan5** | **plan6** | **plan7** | **plan8** | **plan9**}
no loss-plan

Syntax Description

plan1	FXO: A-D gain = 0 dB, D-A gain = 0 dB. FXS: A-D gain = -3 dB, D-A gain = -3 dB.
plan2	FXO: A-D gain = 3 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -3 dB.
plan3	FXO: A-D gain = -3 dB, D-A gain = 0 dB. FXS: Not applicable.
plan4	FXO: A-D gain = -3 dB, D-A gain = -3 dB. FXS: Not applicable.
plan5	FXO: Not applicable. FXS: A-D gain = -3 dB, D-A gain = -10 dB.
plan6	FXO: Not applicable. FXS: A-D gain = 0 dB, D-A gain = -7 dB.
plan7	FXO: A-D gain = 7 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -6 dB.
plan8	FXO: A-D gain = 5 dB, D-A gain = -2 dB. FXS: Not applicable.
plan9	FXO: A-D gain = 6 dB, D-A gain = 0 dB. FXS: Not applicable.

Command Default

FXO: A-D gain = 0 dB, D-A gain = 0 dB (loss plan 1) FXS: A-D gain = -3 dB, D-A gain = -3 dB (loss plan 1)

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	The following additional signal level choices were added: plan 3, plan 4, plan 8, and plan 9.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command sets the analog signal level difference (offset) between the analog voice port and the digital signal processor (DSP). Each loss plan specifies a level offset in both directions--from the analog voice port to the DSP (A-D) and from the DSP to the analog voice port (D-A).

Use this command to obtain the required levels of analog voice signals to and from the DSP.

Examples

The following example configures FXO voice port 1/6 for a -3 dB offset from the voice port to the DSP and for a 0 dB offset from the DSP to the voice port:

```
voice-port 1/6
 loss-plan plan3
```

The following example configures FXS voice port 1/1 for a 0 dB offset from the voice port to the DSP and for a -7 dB offset from the DSP to the voice port:

```
voice-port 1/1
 loss-plan plan6
```

Related Commands

Command	Description
impedance	Specifies the terminating impedance of a voice port interface.
input gain	Specifies the gain applied by a voice port to the input signal from the PBX or other customer premises equipment.
output attenuation	Specifies the attenuation applied by a voice port to the output signal toward the PBX or other customer premises equipment.

lrq e164 early-lookup

To start the E.164 registered endpoint matching before via-zone routing is processed in the location request (LRQ) routing process, use the lrq e164 early-lookup command in gatekeeper configuration mode. To return to the default behavior, use the **no** form of this command.

lrq e164 early-lookup
no lrq e164 early-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

The E.164 endpoint matching is done at the last stage of LRQ routing.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The default gatekeeper algorithm for IP-to-IP gateway selection is based on the via-zone prefix and tech-prefix match. Use the **lrq e164 early-lookup**command to start the E.164 matching process before via-zone routing to block nonregistered endpoints.

Examples

The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)#
gatekeeper
Router(config-gk)# lrq e164 early-lookup
```

lrq forward-queries

To enable a gatekeeper to forward location request (LRQ) messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers, use the **lrq forward-queries** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq forward-queries
no lrq forward-queries

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

LRQ forwarding is dependent on a Cisco nonstandard field that first appeared in Cisco IOS Release 12.0(3)T. This means that any LRQ message received from a non-Cisco gatekeeper or any gatekeeper running a Cisco IOS software image prior to Cisco IOS Release 12.0(3)T is not forwarded.

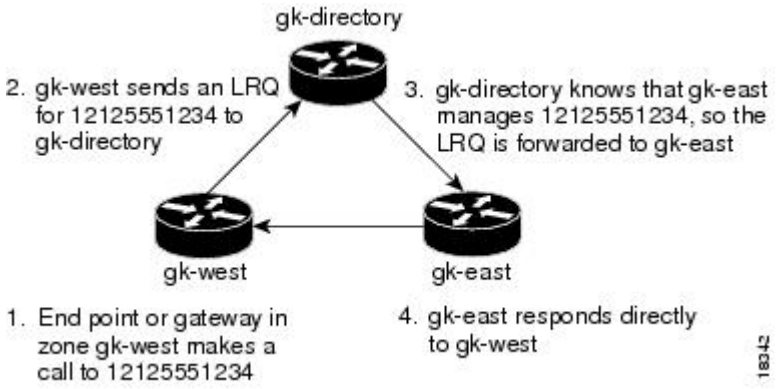
The routing of E.164-addressed calls is dependent on the configuration of zone prefix tables (for example, area code definitions) on each gatekeeper. Each gatekeeper is configured with a list of prefixes controlled by itself and by other remote gatekeepers. Calls are routed to the zone that manages the matching prefix. Thus, in the absence of a directory service for such prefix tables, you, the network administrator, may have to define extensive lists of prefixes on all the gatekeepers in your administrative domain.

To simplify this task, you can select one of your gatekeepers as the "directory" gatekeeper and configure that gatekeeper with the complete list of prefixes and the **lrq forward-queries** command. You can then simply configure all the other gatekeepers with their own prefixes and the wildcard prefix "*" for your directory gatekeeper.

This command affects only the forwarding of LRQ messages for E.164 addresses. LRQ messages for H.323-ID addresses are never forwarded.

Examples

The following example selects one gatekeeper as the directory gatekeeper. See the following figure:



Configuration on gk-directory

On the directory gatekeeper called gk-directory, identify all the prefixes for all the gatekeepers in your administrative domain:

```
zone local gk-directory cisco.com
zone remote gk-west cisco.com 172.16.1.1
zone remote gk-east cisco.com 172.16.2.1
zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......
zone prefix gk-east 1212.......
zone prefix gk-east 1617.......
lrq forward-queries
```

Configuration on gk-west

On the gatekeeper called gk-west, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-west cisco.com
zone remote gk-directory cisco.com 172.16.2.3
zone prefix gk-west 1408.......
zone prefix gk-west 1415.......
zone prefix gk-west 1213.......
zone prefix gk-west 1650.......
zone prefix gk-directory *
```

Configuration on gk-east

On the gatekeeper called gk-east, configure all the locally managed prefixes for that gatekeeper:

```
zone local gk-east cisco.com
zone remote gk-directory cisco.com 172.16.2.3
zone prefix gk-east 1212.......
zone prefix gk-east 1617.......
zone prefix gk-directory *
```

When an endpoint or gateway in zone gk-west makes a call to 12125551234, gk-west sends an LRQ message for that E.164 address to gk-directory, which forwards the message to gk-east. Gatekeeper gk-east responds directly to gk-west.

Related Commands

Command	Description
lrq reject -unknown-prefix	Enables the gatekeeper to reject all LRQ messages for zone prefixes that are not configured.

lrq lrj immediate-advance

To enable the Cisco IOS gatekeeper to immediately send a sequential location request (LRQ) message to the next zone after it receives a location reject (LRJ) message from a gatekeeper in the current zone, use the **lrq lrj immediate-advance** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq lrj immediate-advance
no lrq lrj immediate-advance

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(4)T	This command was introduced. This command does not support the Cisco AS5300, Cisco AS5350, and Cisco AS5400 series in this release.

Usage Guidelines

In a network in which LRQ messages are forwarded through multiple gatekeepers along a single path, a single LRQ message sent from a gatekeeper could solicit multiple LRJ and location confirmation (LCF) responses. If an LRJ response is received first, a potentially unnecessary LRQ message could be sent to the next zone, increasing traffic.

To avoid this problem, perform the following:

- Configure the zone prefix to send sequential LRQ messages rather than to use the **blast** option, using the **zone prefix** command.
- Configure the sequential timer on each gatekeeper along the path, using the **timer lrq seq delay** command.

Examples

The following example enables the gatekeeper to immediately send a sequential LRQ message to the next zone after it receives an LRJ message from a gatekeeper in the current zone.

```
lrq lrj immediate-advance
```

Related Commands

Command	Description
timer lrq seq delay	Defines the time interval between successive sequential LRQ messages.
timer lrq window	Defines the time window during which the gatekeeper collects responses to one or more outstanding LRQ messages.
zone prefix	Adds a prefix to the gatekeeper zone list.

lrq reject-resource-low

To configure a gatekeeper to notify a sending gatekeeper on receipt of a location request (LRQ) message that no terminating endpoints are available, use the **lrq reject-resource-low** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

lrq reject-resource-low
no lrq reject-resource-low

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco 7400 series.

Examples

The following example causes the gatekeeper to notify the sending gatekeeper on receipt of an LRQ message that no terminating endpoints are available:

```
Router(config)#
gatekeeper
Router(config-gk)# lrq reject-resource-low
```

lrq reject-unknown-circuit

To enable the gatekeeper to reject a location request (LRQ) message that contains an unknown destination circuit, use the **lrq reject-unknown-circuit**command in gatekeeper configuration mode. To disable the rejection, use the **no** form of this command.

lrq reject-unknown-circuit
no lrq reject-unknown-circuit

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The gatekeeper checks the destination circuit field in each LRQ message. If the field contains a circuit unknown to the gatekeeper and thiscommandis entered, the gatekeeper rejects the LRQ request. If thiscommand is disabled, the gatekeeper tries to resolve the alias without considering the circuit.

Examples

The following example causes the gatekeeper to reject unknown carriers in an LRQ request:

```
Router(config)# gatekeeper
Router(config-gk)# lrq reject-unknown-circuit
```

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

lrq reject-unknown-prefix

To enable the gatekeeper to reject all location request (LRQ) messages for zone prefixes that are not configured, use the **lrq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming LRQ messages, use the **no** form of this command.

lrq reject-unknown-prefix
no lrq reject-unknown-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

The gatekeeper accepts and processes all incoming LRQ messages.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines

Use this command to configure the gatekeeper to reject any incoming LRQ messages for a destination E.164 address that does not match any of the configured zone prefixes.

Whether or not you use this command, the following is true when the E.164 address matches a zone prefix:

- If the matching zone prefix is local (that is, controlled by this gatekeeper), the LRQ message is serviced.
- If the matching zone prefix is remote (that is, controlled by some other gatekeeper), the LRQ message is rejected.

If you do not use this command and the target address does not match any known local or remote prefix, the default behavior is to attempt to service the call using one of the local zones. If this default behavior is not suitable for your site, use this command on your router to force the gatekeeper to reject such requests.

Examples

Consider the following gatekeeper configuration:

```
zone local gk408 cisco.com
zone local gk415 cisco.com
zone prefix gk408 1408.......
zone prefix gk415 1415.......
lrq reject-unknown-prefix
```

In this sample configuration, the gatekeeper is configured to manage two zones. One zone contains gateways with interfaces in the 408 area code, and the second zone contains gateways in the 415 area code. Then using the **zone prefix** command, the gatekeeper is configured with the appropriate prefixes so that calls to those area codes hop off in the optimal zone.

Now say some other zone has been erroneously configured to route calls to the 212 area code to this gatekeeper. When the LRQ message for a number in the 212 area code arrives at this gatekeeper, the gatekeeper fails to match the area code, and the message is rejected.

If this was your only site that had any gateways in it and you wanted your other sites to route all calls that require gateways to this gatekeeper, you can undo the **lrq reject-unknown-prefix command** by simply using the **no lrq reject-unknown-prefix command.**Now when the gatekeeper receives an LRQ message for the address 12125551234, it attempts to find an appropriate gateway in either one of the zones gk408 or gk415 to service the call.

Related Commands

Command	Description
lrq forward-queries	Enables a gatekeeper to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.

lrq timeout blast window

To configure the timeout window for use when sending multiple location request (LRQ) messages (either sequentially or simultaneously), use the lrq timeout blast window command in gatekeeper configuration mode. To reset to the default, use the no form of this command.

lrq timeout blast window seconds
no lrq timeout blast window

Syntax Description

seconds	Duration of the window, in seconds. Range is from 1 to 10. Default is 6.

Command Default

6 seconds

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the window to 3 seconds:

```
lrq timeout blast window 3
```

Related Commands

Command	Description
gatekeeper gw -type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper's zone list.

lrq timeout seq delay

To configure the delay for use when sending location request (LRQ) messages sequentially, use the lrq timeout seq delay command in gatekeeper configuration mode. To reset to the default, use the no form of this command.

lrq timeout seq delay value
no lrq timeout seq delay

Syntax Description

value	Duration of the delay, in 100-millisecond units.Range is from 1 to 10. The default is 5 (500 ms or 0.5 seconds).

Command Default

Five 100-millisecond units (500 ms or 0.5 seconds)

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(2)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.

Examples

The following example sets the delay to 300 milliseconds:

```
lrq timeout seq delay 3
```

Related Commands

Command	Description
gatekeeper gw-type-prefix	Sets the gatekeepers responsible for each technology prefix.
zone prefix	Adds a prefix to a gatekeeper's zone list.