ss7 mtp2-variant through switchover method

ss7 mtp2-variant

To configure a Signaling System 7 (SS7) signaling link, use the **ss7 mtp2-variant** command in global configuration mode. To restore the designated default, use the **no** form of this command.

ss7 mtp2-variant [{**bellcore** *channel* | **itu-white channel** | **ntt** *channel* | **ttc** *channel*}] [*parameters*]
no ss7 mtp2-variant

Syntax Description

bellcore	Configures the router for Telcordia Technologies (formerly Bellcore) standards.
channel	Message Transfer Part Layer 2 (MTP2) serial channel number. Range is from 0 to 3.
itu white	Configures the SS7 channel with the ITU-white protocol variant.
ntt	Configures the router for NTT (Japan) standards. **Note** This keyword is not available with the PCR feature.
ttc	Configures the router for Japanese Telecommunications Technology Committee (TTC) standards. **Note** This keyword is not available with the PCR feature.
parameters	(Optional) Configures a particular standard. See the tables in the "Usage Guidelines" section for accepted parameters.

Command Default

bellcore

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	This command was modified to include all possible variants: **bellcore**, **itu white**, **ntt**, **ttc**.

Usage Guidelines

The MTP2 variant has timers and parameters that can be configured using the values listed in the following tables. To restore the designated default, use the **no** or the **default** form of the command (see the "Examples" section below).

Note When the **bellcore** or **itu white** variant is selected, this command enters a new configuration mode for setting MTP2 parameters: ITU configuration mode. See the **error correction**command reference for information about setting MTP2 parameters from this mode.

Table 1: Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	1600	1000 to 65535
T4 Normal Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending status indication busy (SIB) timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535
lssu len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	127	16 to 127
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM number octets	SUERM octet-counting mode	16	8 to 32
SUERM number signal units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie AERM Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tie AERM Normal	AERM normal error-rate threshold	4	1 to 8

Table 2: ITU-white Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4 Normal Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535

Parameter	Description	Default	Range
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
msu len	message signal unit (MSU) length	1	1 to 2
unacked MSUs	Maximum number of MSUs awaiting acknowledgment (ACK)	127	16 to 127
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM number octets	SUERM octet counting mode	16	8 to 32
SUERM - number - signal - units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie AERM Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin AERM Normal	AERM normal error-rate threshold	4	1 to 8

Table 3: NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	Fill-in Signal Unit (FISU) interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) e error-rate threshold	64	32 to 128
SUE RM - number - octets	SUERM octet counting mode	16	8 to 32
SUERM - number - signal - units	Signal Unit Error Rate Monitor (SUERM) units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie - AERM - Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8

Table 4: TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error - rate threshold	64	32 to 128
SUERM number octets	SUERM octet counting mode	16	8 to 32

Parameter	Description	Default	Range
SUERM number signal units	Signal units (good or bad) needed to decrement ERM	256	128 to 512
Tie AERM Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example configures an SS7 channel (link) for Preventive Cyclic Retransmission (PCR) with forced retransmission initiated. In this example, SS7 channel 0 is configured with the ITU-white protocol variant using the PCR error correction method.

```
Router# configure terminal
Router(config)# ss7 mtp2-variant itu-white 0

Router(config-ITU)# error-correction pcr forced-retransmission enabled N2 1000
Router(config-ITU)# end
```

The following example disables error-correction:

```
Router(config-ITU)# no error-correction
```

Related Commands

Command	Description
error correction	Sets the error correction method for the SS7 signaling link when the SS7 MTP2 variant is Bellcore or ITU-white.
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

ss7 mtp2-variant bellcore

To configure the router for Telcordia Technologies (formerly Bellcore) standards, use the **ss7 mtp2-variant bellcore** command in global configuration mode.

ss7 mtp2-variant bellcore [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for default parameters.

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see example below).

Note Timer durations are converted to 10-millisecond units. For example, a T1 value of 1005 is converted to 100, which results in an actual timeout duration of 1000 ms. This is true for all timers and all variants.

Table 5: Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	600	1000 to 65535
T4 -Normal-Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535

Parameter	Description	Default	Range
lssu -len	1- or 2-byte LSSU format	1	1 to 2
unacked -MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error-rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet-counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tie -AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the aligned/ready timer duration on channel 0 to 30,000 ms:

```
ss7 mtp2-variant bellcore 0 T1 30000
```

The following example restores the aligned/ready timer default value of 13,000 ms:

```
ss7 mtp2-variant bellcore 0 no T1
```

Related Commands

Command	Description
ss7 mtp2 -variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2 -variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2 -variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant itu

To configure the router for ITU (International Telecom United) standards, use the **ss7 mtp2-variant itu** command in global configuration mode.

ss7 mtp-variant itu [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for ITU default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 6: ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4 -Normal-Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu -len	1- or 2-byte LSSU format	1	1 to 2
msu -len			

Parameter	Description	Default	Range
unacked -MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tin -AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the emergency proving period on channel 1 to 10,000 ms:

```
ss7 mtp2-variant itu 1
 t4-Emergency-Proving 10000
```

The following example restores the emergency proving period default value of 5,000 ms:

```
ss7 mtp2-variant itu 1
 default t4-Emergency-Proving
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ntt

To configure the router for NTT (Japan) standards, use the **ss7 mtp2-variant ntt** command in global configuration mode.

ss7 mtp-variant ntt [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for NTT default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The NTT MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 7: NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked -MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the SUERM error rate threshold on channel 2 to 100:

```
ss7 mtp2-variant ntt 2
 SUERM-threshold 100
```

The following example restores the SUERM error rate threshold default value of 64:

```
ss7 mtp2-variant ntt 2
 no SUERM-threshold
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ttc

To configure the router for TTC (Japan Telecom) standards, use the **ss7 mtp2-variant ttc** command in global configuration mode.

ss7 mtp-variant ttc [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for TTC default parameters.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The TTC MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 8: TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked -MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the maximum number of proving attempts for channel 3 to 3:

```
ss7 mtp2-variant ttc 3
 proving-attempts 3
```

The following example restores the maximum number of proving attempts to the default value:

```
ss7 mtp2-variant ttc 3
 default proving-attempts
```

Related Commands

Command	Description
ss7 mtp2 -variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2 -variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2 -variant ntt	Specifies the MTP2-variant as NTT.

ss7 mtp2-variant itu-white

To configure the router for International Telecommunications Union (ITU) standards, use the **ss7 mtp2-variant itu-white** command in global configuration mode.

ss7 mtp2-variant itu-white [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Message Transfer Part 2 (MTP2) serial channel number. The range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for ITU default parameters.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command.

Table 9: ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds [ms])	40000	1000 to 65535
T2	Not aligned timer (ms)	5000	1000 to 65535
T3	Aligned timer (ms)	1000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (ms)	500	1000 to 65535
T4-Normal-Proving	Normal proving timer (ms)	8200	1000 to 65535
T5	Sending SIB timer (ms)	100	80 to 65535
T6	Remote congestion timer (ms)	6000	1000 to 65535
T7	Excessive delay timer (ms)	1000	1000 to 65535
lssu-len	1- or 2-byte Links Status Signal Unit (LSSU) format	1	1 to 2
msu-len	--	--	--

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of Message Signal Units (MSUs) waiting acknowledgement	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal unit error monitor (SUERM) error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal- units	Signal units (good or bad) needed to dec Embedded Resource Manager (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Unit Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example shows how to set the emergency proving period on channel 1 to 10,000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# t4-Emergency-Proving 10000
```

The following example shows how to restore the emergency proving period default value of 5000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# default t4-Emergency-Proving 5000
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2 variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2 variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2 variant as TTC.

ss7 session

To create a Reliable User Datagram Protocol (RUDP) session and explicitly add an RUDP session to a Signaling System 7 (SS7) session set, use the **ss7 session** command in global configuration mode. To delete the session, use the **no** form of this command.

ss7 session *session-id* **address** *destination-address destinaion-port local-address local-port* [**session-set** *session-number*]
no ss7 session *session-id*

Syntax Description

session -id	SS7 session number. Valid values are 0 and 1. You must enter a hyphen with no space following it after the **session** keyword.
address *destination -address*	Specifies the SS7 session IP address.
destination -address	The local IP address of the router in four-part dotted-decimal format. The local IP address for both sessions, 0 and 1, must be the same.
destination -port	The number of the local UDP port on which the router expects to receive messages from the media gateway controller (MGC) . Specify any UDP port that is not used by another protocol as defined in RFC 1700 and that is not otherwise used in your network. The local UDP port must be different for session 0 and session 1. Valid port ranges are from 1024 to 9999.
local -address	The remote IP address of the MGC in four-part dotted-decimal format.
local -port	The number of the remote UDP port on which the MGC is configured to listen. This UDP port cannot be used by another protocol as defined in RFC 1700 and cannot be otherwise used in the network. Valid port ranges are from 1024 to 9999.
session -setsession - number	(Optional) Assigns an SS7 session to an SS7 session set.

Command Default

No session is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(15)T	The **session-set** keyword and thesession - number argument were added.

Usage Guidelines

For the Cisco 2600-based SLT, you can configure a maximum of four sessions, two for each Cisco SLT. In a redundant VSC configuration, session 0 and session 2 are configured to one VSC, and session 1 and session 3 are configured to the other. Session 0/1 and session 2/3 run to the Cisco SLT.

The VSC must be configured to send messages to the local port, and it must be configured to listen on the remote port. You must also reload the router whenever you remove a session or change the parameters of a session.

This command replaces the **ss7 session-0 address** and **ss7 session-1 address** commands, which contain hard-coded session numbers. The new command is used for the new dual Ethernet capability.

The new CLI supports both single and dual Ethernet configuration by being backward compatible with the previous **session-0** and **session-1** commands so that you can configure a single Ethernet instead of two, if needed.

For the Cisco AS5350 and Cisco AS5400-based SLT, you can configure a maximum of two sessions, one for each signaling link. In a redundant MGC configuration, session 0 is configured to one MGC and session 1 is configured to the other.

The MGC must be configured to send messages to the local port, and the MGC must be configured to listen on the remote port.

You must reload the router whenever you remove a session or change the parameters of a session.

By default, each RUDP session must belong to SS7 session set 0. This allows backward compatibility with existing SS7 configurations.

If the **session-set** keyword is omitted, the session is added to the default SS7 session set 0. This allows backward compatibility with older configurations. Entering the no form of the command is still sufficient to remove the session ID for that RUDP session.

If you want to change the SS7 session set to which a session belongs, you have to remove the entire session first. This is intended to preserve connection and recovery logic.

Examples

The following example sets up two sessions on a Cisco 2611 and creates session set 2:

```
ss7 session-0 address 172.16.1.0 7000 172.16.0.0 7000 session-set 2
ss7 session-1 address 172.17.1.0 7002 172.16.0.0 7001 session-set 2
```

Note The example above shows how the local IP addresses in session-0 and session-1 must be the same.

Related Commands

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.

Command	Description
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session cumack_t

To set the Reliable User Datagram Protocol (RUDP) cumulative acknowledgment timer for a specific SS7 signaling link session, use the **ss7 session cumack_t**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session *session-number* **cumack_t** *milliseconds*
no ss7 session *session-number* **cumack_t**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the RUDP waits before it sends an acknowledgment after receiving a segment. Range is from 100 to 65535. The value should be less than the value configured for the retransmission timer by using the ss7 session-*session number* **retrans_t**command.

Command Default

300 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The cumulative acknowledgment timer determines when the receiver sends an acknowledgment. If the timer is not already running, it is initialized when a valid data, null, or reset segment is received. When the cumulative acknowledgment timer expires, the last in-sequence segment is acknowledged. The RUDP typically tries to "piggyback" acknowledgments on data segments being sent. However, if no data segment is sent in this period of time, it sends a standalone acknowledgment.

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Examples

The following example sets up two sessions and sets the cumulative acknowledgment timer to 320 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 cumack_t 320
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 cumack_t 320
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session kp_t

To set the null segment (keepalive) timer for a specific SS7 signaling link session, use the **ss7 session kp_t**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **kp_t milliseconds**
no ss7 session-session *number* **kp_t milliseconds**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the Reliable User Datagram Protocol (RUDP) waits before sending a keepalive to verify that the connection is still active. Valid values are 0 and from100 to 65535. Default is 2000.

Command Default

2000 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The null segment timer determines when a null segment (keepalive) is sent by the client Cisco 2600 series router. On the client, the timer starts when the connection is established and is reset each time a data segment is sent. If the null segment timer expires, the client sends a keepalive to the server to verify that the connection is still functional. On the server, the timer restarts each time a data or null segment is received from the client.

The value of the server's null segment timer is twice the value configured for the client. If no segments are received by the server in this period of time, the connection is no longer valid.

To disable keepalive, set this parameter to 0.

Examples

The following example sets up two sessions and sets a keepalive of 1,800 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 kp_t 1800
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 kp_t 1800
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_cumack

To set the maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_cumack**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_cumack** *segments*
no ss7 session-session *number* **m_cumack** *segments*

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment. Range is from 0 to 255. Default is 3.

Command Default

3 segments

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The cumulative acknowledgment counter records the number of unacknowledged, in-sequence data, null, or reset segments received without a data, null, or reset segment being sent to the transmitter. If this counter reaches the configured maximum, the receiver sends a standalone acknowledgment (a standalone acknowledgment is a segment that contains only acknowledgment information). The standalone acknowledgment contains the sequence number of the last data, null, or reset segment received.

If you set this parameter to 0, an acknowledgment is sent immediately after a data, null, or reset segment is received.

Examples

The following example sets up two sessions and in each session sets a maximum of two segments for receipt before acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_cumack 2
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_cumack 2
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_outseq

To set the maximum number of out-of-sequence segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an extended acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_outseq**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_outseq** *segments*
no ss7 session-session *number* **m_outseq**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment. If the specified number of segments are received out of sequence, an Extended Acknowledgment segment is sent to inform the sender which segments are missing. Range is from 0 to 255. Default is 3.

Command Default

3 segments

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The out-of-sequence acknowledgment counter records the number of data segments that have arrived out of sequence. If this counter reaches the configured maximum, the receiver sends an extended acknowledgment segment that contains the sequence numbers of the out-of-sequence data, null, and reset segments received. When the transmitter receives the extended acknowledgment segment, it retransmits the missing data segments.

If you set this parameter to 0, an acknowledgment is sent immediately after an out-of-sequence segment is received.

Examples

The following example sets up two sessions and sets a maximum number of four out-of-sequence segments for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_outseq 4
```

```
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_outseq 4
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_rcvnum

To set the maximum number of segments that the remote end can send before receiving an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_rcvnum**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_rcvnum** *segments*
no ss7 session-session *number* **m_rcvnum**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that the remote (Cisco IOS software) end can send before receiving an acknowledgment. Range is from 1 to 64. Default is 32.

Command Default

32 segments

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The outstanding segments counter is the maximum number of segments that the Cisco IOS software end of the connection can send without getting an acknowledgment from the receiver. The receiver uses the counter for flow control.

Examples

The following example sets up two sessions and for each session sets a maximum of 36 segments for receipt before an acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_rcvnum 36
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_rcvnum 36
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_retrans

To set the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid in a specific SS7 signaling link session, use the **ss7 session m_retrans** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_retrans** *number*
no ss7 session-session *number* **m_retrans**

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
number	Maximum number of times that the RRUDP attempts to resend a segment before declaring the connection broken. Range is from 0 to 255. Default is 2.

Command Default

2 times

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The retransmission counter is the number of times a segment has been retransmitted. If this counter reaches the configured maximum, the transmitter resets the connection and informs the upper-layer protocol.

If you set this parameter to 0, the RUDP attempts to resend the segment continuously.

Examples

The following example sets up two sessions and for each session sets a maximum number of three times to resend before a session becomes invalid:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_retrans 3
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_retrans 3
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session retrans_t

To set the amount of time that the Reliable User Datagram Protocol (RUDP) waits to receive an acknowledgment for a segment in a specific SS7 signaling link session, use the **ss7 session retrans_t**command in global configuration mode. If the RUDP does not receive the acknowledgment in this time period, the RUDP retransmits the segment. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **retrans_t** *milliseconds*
no ss7 session-session *number* **retrans_t**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Amount of time, in milliseconds, that the RUDP waits to receive an acknowledgment for a segment. Range is from 100 to 65535. Default is 600.

Command Default

600 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The retransmission timer is used to determine whether a packet must be retransmitted and is initialized each time a data, null, or reset segment is sent. If an acknowledgment for the segment is not received by the time the retransmission timer expires, all segments that have been transmitted--but not acknowledged--are retransmitted.

This value should be greater than the value configured for the cumulative acknowledgment timer by using the **ss7 session cumack_t**command.

Examples

The following example sets up two sessions and specifies 550 ms as the time to wait for an acknowledgment for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 retrans_t 550
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 retrans_t 550
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.

ss7 set

Note Effective with Cisco IOS Release 12.2(15)T, the **ss7 set** command replaces the ss7 set failover-timer command.

To independently select failover-timer values for each session set and to specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session, use the **ss7 set**command in global configuration mode. To restore the failover timer to its default value of 5, use the **no** form of this command.

ss7 set [**session-set** *session-id*] **failover-timer** *ft-value*
no ss7 set [**session-set** *session-id*] **failover-timer**

Syntax Description

session-set *session-id*	(Optional) Selects failover timer values for each SS7 session set. Valid values are from 1 to 5. Default is 0.
failover -timer *ft-value*	Time, in seconds, that the Session Manager waits for a session to recover. Valid values range from 1 to 10. Default is 5.

Command Default

The failover timer is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced. This command replaces the **ss7 set failover-timer**command.

Usage Guidelines

The failover-timer keyword and the ft-value argument specify the number of seconds that the Session Manager waits for the active session to recover or for the standby MGC to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the failover timer expires without recovery of the original session or if the system fails to get an active message from the standby MGC, the signaling links are taken out of service.

The no form of this command restores the failover timer to its default value of 5. Omitting the optional session-set keyword implicitly selects SS7 session set 0, which is the default.

Examples

The following example sets the failover timer to four seconds without using the session-set option:

```
ss7 set failover-timer 4
```

The following example sets the failover timer to 10 seconds and sets the SS7 session set value to 5:

```
ss7 set session-set 5 failover-timer 10
```

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

ss7 set failover-timer

To specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby Media Gateway Controller to indicate that the SLT should switch traffic to the standby session, use the **ss7 set failover-timer**command in global configuration mode. To reset ti the default, use the **no** form of this command.

ss7 set failover-timer [*seconds*]
no ss7 set failover-timer

Syntax Description

seconds	Time, in seconds, that the session manager waits for a session to recover. Range is from 1 to 10. Default is 3.

Command Default

3 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command specifies the number of seconds that the session manager waits for the active session to recover or for the standby media gateway controller to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the timer expires without a recovery of the original session or an active message from the standby media gateway controller, the signaling links are taken out of service.

Examples

The following example sets the failover timer to 4 seconds:

```
ss7 set failover-timer 4
```

Related Commands

Command	Description
show ss7 sm set	Displays the current failover timer setting.
ss7 session	Establishes a session.

station-id name

To specify the name that is to be sent as caller ID information and to enable caller ID, use the **station-id name** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the name, use the **no** form of this command.

station-id name *name*
no station-id name *name*

Syntax Description

name	Station-id name. Must be a string of 1 to 15 characters.

Command Modes

The default is no station-id name.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

Do not use this command when the caller ID standard is dual-tone multifrequency (DTMF). DTMF caller ID can carry only the calling number.

If the **station-id name**, **station-id number**, or a **caller-id alerting**command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable**command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
```

```
 station-id number 4085550111
Router(config-voiceport)#station-id
 ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller -id enable	Enables caller ID operation.
station-id number	Enables caller ID operation and specifies the number sent from the originating station-id or network FXO port for caller ID purposes.

station-id number

To specify the telephone or extension number that is to be sent as caller ID information and to enable caller ID, use the **station-id number** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the number, use the **no** form of this command.

station-id number *number*
no station-id number *number*

Syntax Description

number	Station-id number. Must be a string of 1 to 15 characters.

Command Default

The default is no station-id number.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Within the network, if an originating station-id does not include configured number information, Cisco IOS software determines the number by using reverse dial-peer search.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

If the **station-id name**, **station-id number**, or a **caller-id alerting**command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable**command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
```

```
 station-id number 4085550111
Router(config-voiceport)#station-id
 ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller -id enable	Enables caller ID operation.
station-id name	Enables caller ID operation and specifies the name sent from the originating station-id or network FXO port for caller ID purposes.

stats

To enable statistics collection for voice applications, use the **stats** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

stats
no stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application stats** command.

Usage Guidelines

To display the application statistics, use the **show call application session-level**, **show call application app-level**, or **show call application gateway-level**command. To reset the application counters in history to zero, use the **clear call application stats** command.

Examples

The following example enables statistics collection for voice applications:

```
application
monitor
stats
```

Related Commands

Command	Description
call application interface stats	Enables statistics collection for application interfaces.
call application stats	Enables statistics collection for voice applications.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
interface stats	Enables statistics collection for application interfaces.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.

stcapp

To enable the SCCP Telephony Control Application (STCAPP), use the **stcapp** command in global configuration mode. To disable the STCAPP, use the **no** form of this command.

stcapp
no stcapp

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco CallManager does not control Cisco IOS gateway-connected analog and BRI endpoints.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **stcapp**command to enable basic Skinny Client Call Control (SCCP) call control features for BRI and foreign exchange stations (FXS) analog ports within Cisco IOS voice gateways. The **stcapp**command enables the Cisco IOS gateway application to support the following features:

- Line-side support for the Multilevel Precedence and Preemption (MLPP) feature
- Cisco CallManager registration of analog and Basic Rate Interface BRI endpoints
- Cisco CallManager endpoint autoconfiguration support
- Modem pass-through support
- Cisco Survivable Remote Site Telephony (SRST) support

Examples

The following example shows that STCAPP is enabled:

```
Router(config)# stcapp
```

Related Commands

Command	Description
ccm-manager config server	Specifies the TFTP server for SCCP gateway downloads.
ccm-manager sccp local	Specifies the SCCP local interface for Cisco CallManager registration.
sccp	Enables the SCCP protocol.
show stcapp device	Displays configuration information about STCAPP) voice ports.
show stcapp statistics	Displays call statistics for STCAPP voice ports.
stcapp ccm-group	Configures the Cisco CallManager group number for use by the STCAPP.

Command	Description
stcapp timer	Enables STCAPP timer configuration.

stcapp call-control mode

To configure call control mode for Skinny Client Control Protocol (SCCP) gateway supplementary features, use the **stcapp call-control mode** command in global configuration mode. To disable call control mode, use the **no** form of this command

stcapp call-control mode [{**feature** | **standard**}]
no stcapp call-control mode [{**feature** | **standard**}]

Syntax Description

feature	(Optional) Feature mode call control.
standard	(Optional) Standard mode call control. This is the default.

Command Default

Standard mode call control is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

This command enables feature mode call control, which allows SCCP analog phone users to invoke a feature by dialing a feature access code (FAC). The following table lists the features and FACs that you can use in feature mode.

Feature	FAC
Drop Last Active Call	#1
Call Transfer	#2
Call Conference	#3
Drop Last Conferee	#4
Toggle Between Two Calls	#5

Examples

The following partial output from the **show running-config** command shows feature call control mode enabled:

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

The following partial output from the **show running-config** command shows standard call control mode enabled:

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

Related Commands

Command	Description
show stcapp feature codes	Displays current values for SCCP telephony control (STC) application feature access codes.

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback
no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application:

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp ccm-group

To configure the Cisco CallManager group number for use by the SCCP Telephony Control Application (STCAPP), use the **stcapp ccm-group** command in global configuration mode. To disable STCAPP Cisco CallManager group number configuration, use the **no** form of this command.

stcapp ccm-group *group-id*
no stcapp ccm-group *group-id*

Syntax Description

group-id	Cisco CallManager group number.

Command Default

No Cisco CallManager group number is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The Cisco CallManager group identifier must have been configured for the service provider interface (SPI) using the **sccp ccm-group** *group-id*command.

Examples

The following example configures the STCAPP to use Cisco CallManager group 2:

```
Router(config)# stcapp ccm-group 2
```

Related Commands

Command	Description
show stcapp device	Displays configuration information about SCCP Telephony Control Application (STCAPP) voice ports.
show stcapp statistics	Displays call statistics for SCCP Telephony Control Application (STCAPP) voice ports.
stcapp	Enables the SCCP Telephony Control Application (STCAPP).
stcapp timer	Enables SCCP Telephony Control Application (STCAPP) timer configuration.

stcapp feature access-code

To enable feature access codes (FACs) in the STC application and enter the STC application feature access-code configuration mode, use the **stcapp feature access-code** command in global configuration mode. To disable the use of all STC application feature access codes, use the **no** form of this command.

stcapp feature access-code
no stcapp feature access-code

Syntax Description

This command has no arguments or keywords.

Command Default

All feature access codes are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command enables feature access codes (FACs) in the SCCP telephony control (STC) application and enters the STC application feature access-code configuration mode to modify the default values of the prefix and feature codes for FACs.

The **no** form of this command blocks the use of FACs on all analog ports.

Use the **show stcapp feature codes** command to display a list of all FACs.

Examples

The following example shows how to enable FACs in the STC application.

```
Router(config)# stcapp feature access-code
Router(stcapp-fac)#
```

Related Commands

Command	Description
call forward all	Defines the feature code in the feature access code (FAC) for forwarding all calls.
call forward cancel	Defines the feature code in the feature access code (FAC) for cancelling Call Forward All.
pickup direct	Defines the feature code in the feature access code (FAC) for Directed Call Pickup.
pickup group	Defines the feature code in the feature access code (FAC) for call pickup from another group.
pickup local	Defines the feature code in the feature access code (FAC) for call pickup from the local group.

Command	Description
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback
no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application:

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp feature speed-dial

To enable STC application feature speed-dial codes and enter their configuration mode, use the **stcapp feature speed-dial** command in global configuration mode. To disable the use of all STC application feature speed-dial codes, use the **no** form of this command.

stcapp feature speed-dial
no stcapp feature speed-dial

Syntax Description

This command has no arguments or keywords.

Command Default

All feature speed-dial codes are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the SCCP telephony control (STC) application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Although feature speed-dial (FSD) prefixes and codes for analog FXS ports are configured on the voice gateway that has the FXS ports, the actual numbers that are dialed using these codes are configured on Cisco CallManager or the Cisco CallManager Express system.

The **no** form of this command blocks the use of FSD codes on all analog ports.

Note that all the STC FSD codes have defaults. To return codes under this configuration mode to their defaults, you must use the **no** form of the individual commands one at a time.

Examples

The following example sets an FSD prefix of three asterisks (***) and speed-dial codes from 2 to 7. After these values are configured, a phone user presses ***2 on the keypad to speed-dial the telephone number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ***
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# redial 9
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

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

```
stcapp feature speed-dial
  prefix ***
  redial ***9
  voicemail ***8
  speeddial1 ***2
  speeddial2 ***3
  speeddial3 ***4
  speeddial4 ***5
  speeddial5 ***6
  speeddial6 ***7
```

Related Commands

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show stcapp feature codes	Displays configured and default STC application feature codes.
speed dial	Designates a range of STC application feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

stcapp register capability

To specify modem capability for SCCP Telephony Control Application (STCAPP) devices, use the **stcapp register capability**command in global configuration mode. To disable modem capability, use the **no** form of this command.

stcapp register capability *voice-port* [{**both** | **modem-passthrough** | **modem-relay**}]
no stcapp register capability *voice-port*

Syntax Description

voice-port	Voice interface slot number 1 through 4
both	Specifies support for both modem-relay and modem pass-through.
modem - passthrough	Specifies support for modem pass-through.
modem - relay	Specifies support for V.150.1 modem relay.

Command Default

No voice port modem capability is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **stcapp register capability** *command to specify modem transport methods for STCAPP-controlled devices registering with Cisco Call-Manager. If this command is applied while the voice port is idle, the port automatically reregisters with the Cisco CallManager. If there is an active call on the voice port when this command is applied, the port does not reregister.*Although Cisco does not recommend the procedure, to force device reregistration you must either manually shut down the device using the **shutdown** command in voice-port configuration mode, or reset it from the Cisco CallManager.

Use the voice service configuration command **modem passthrough** to globally enable modem pass-through capability, thereby providing fallback to voice band data (modem pass-through) when the voice gateway communicates with a Secure Telephone Unit (STU) or nonmodem-relay capable gateway.

Examples

The following example configures the device connected to voice port 1/1/0 to support both modem capabilities:

```
Router(config)# stcapp register capability 1/1/0 both
```

Related Commands

Command	Description
modem passthrough	Globally enables modem pass-through over VoIP.
show stcapp device voice-port	Displays configuration information for STCAPP devices.

Command	Description
shutdown	Disables voice ports on the VIC.

stcapp security mode

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the security mode to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security mode** command in global configuration mode. To disable security for the endpoint, use the no form of this command.

stcapp security mode [{**authenticated** | **encrypted** | **none**}]
no stcapp security

Syntax Description

mode	Sets the global security mode for all STCAPP endpoints.
authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME through the secure TLS connection on TCP port 2443.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
none	Sets the security mode to none (Default).

Command Default

Security is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode**and **stcapp security trustpoint** commands to enable security for the STCAPP end point. The **stcapp security trustpoint** command must be configured for the STCAPP service to start.

SCCP signaling security mode can be set for each dial peer using the **security mode** command in dial peer configuration mode. If you use both the **stcapp security mode** and the **security mode**commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
security mode	Sets the security mode for a specific dial peer using STCAPP services in a secure Cisco Unified CME network.
stcapp	Enables the STCAPP.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.
stcapp security trustpoint	Enables security for STCAPP endpoints and specifies the trustpoint for setting up the TLS connection.

stcapp security trustpoint

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the trustpoint to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security** command in global configuration mode. To disable security for the endpoint and delete all identity information and certificates associated with the trustpoint, use the no form of this command.

stcapp security trustpoint *line*
no stcapp security

Syntax Description

trustpoint	Security trustpoint label for all STCAPP endpoints.
line	Text description that identifies the trustpoint.

Command Default

Security is not enabled and no trustpoint is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode**and **stcapp security trustpoint** commands to enable security for the STCAPP endpoint. The **stcapp security trustpoint** command must be configured for the STCAPP service to start. The trustpoint configured by this command contains the device certificate and must match the trustpoint configured on the router using the **crypto pki trustpoint** command. All analog phones use the same certificate. Cisco Unified Communications Manager Express does not require a different certificate for each phone.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.
stcapp	Enables the STCAPP.

Command	Description
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

stcapp supplementary-services

To enter supplementary-service configuration mode for configuring STC application supplementary-service features on an FXS port, use the **stcapp supplementary-services** command in global configuration mode. To remove the configuration, use the **no** form of this command.

stcapp supplementary-services
no stcapp supplementary-services

Syntax Description

This command has no arguments or keywords.

Command Default

No configuration for STC application supplementary-service features exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enters the supplementary-service configuration mode for configuring STC application supplementary-service features for analog FXS ports on a Cisco IOS voice gateway, such as a Cisco integrated services router (ISR) or Cisco VG224 Analog Phone Gateway.

Examples

The following example shows how to enable the Hold/Resume STC application supplementary-service feature for analog phones connected to port 2/0 on a Cisco VG224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
port (supplementary-service)	Specifies analog FXS port on which STC application supplementary-service features are to be supported.

stcapp timer

To enable SCCP Telephony Control Application (STCAPP) timer configuration, use the **stcapp timer**command in global configuration mode. To disable STCAPP timer configuration, use the **no** form of this command.

stcapp timer roh *seconds*
no stcapp timer

Syntax Description

roh	Receiver off hook (ROH) tone timeout.
seconds	Duration, in seconds, that the receiver off-key tone is played. Range is 0 to 120 seconds.

Command Default

seconds: 45 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure the STCAPP ROH timer for the maximum time that ROH tone is played. ROH tone signals a subscriber that the phone remains off hook when there is no active call.

Examples

The following example configures the receiver off hook timer for 30 seconds:

```
Router(config)# stcapp timer roh 30
```

Related Commands

Command	Description
show call application voice stcapp	Displays information about the STCAPP.
stcapp	Enables the STCAPP.

stream-service profile

To associate details specific to stream service with the media class on CUBE, use the **stream-service profile** *tag* command in media class configuration mode. To revert the stream service association, use the **no** form of this command.

stream-service profile *tag*
no stream-service profile *tag*

Syntax Description

tag	The stream-service profile tag. Range is 1–10000.

Command Default

Stream service profile isn't associated with the media class by default.

Command Modes

Media Class configuration mode (cfg-mediaclass)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

The **stream-service profile** *tag* command associates a stream service profile with a media class. This profile is then configured in **media profile stream-service** *tag* command to enable stream-service in CUBE.

Examples

The following is a sample configuration for stream-service profile in CUBE:

```
router(config)#media class 9
csr(cfg-mediaclass)#stream-service ?
profile select media profile stream-service

csr(cfg-mediaclass)#stream-service profile ?
<1-10000> media profile stream-service tag

csr(cfg-mediaclass)#stream-service profile 99
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
source-ip (media-profile)	Configures local source IP address of a WebSocket connection.
media class	Applies the media class at the dial peer level.

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
no stun

Syntax Description

This command has no arguments or keywords.

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.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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	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* [*boot-count*]
no stun flowdata agent-id *tag* [*boot-count*]

Syntax Description

tag	Unique identifier in the range 0 to 255. Default is -1.
boot-count	(Optional) Value of boot-count. Range is 0 to 65535. Default is zero.

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 the agent id and the boot count to configure call control agents which authorize the flow of traffic.

Configuring the boot-count keyword helps to prevent anti-replay attacks after the router is reloaded. If you do not configure a value for boot count, the boot-count is initialized to 0 by default. After it is initialized, it is incremented by one automatically upon each reboot and the value saved back to NVRAM. The value of boot count is reflected in **show running** configuration command.

Examples

The following example shows how the **stun flowdata agent-id** command is used at the router prompt.

```
Router#enable
Router#configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata agent-id 35 100
```

Related Commands

Command	Description
stun flowdata keepalive	Configures the keepalive interval.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.

stun flowdata catlife

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

stun flowdata catlife *liftetime* **keepalive** *interval*
no stun flowdata catlife *liftetime* **keepalive** *interval*

Syntax Description

liftetime	Lifetime of the CAT in seconds. The default value is 1270 (21 min 10 sec).
interval	Keepalive interval time in seconds. Range is 10 to 30. Default is 10.

Command Default

The default keepalive value is 10 seconds.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **stun flowdata catlife**command to configure call control agents which authorize the flow of traffic.

Examples

The following example shows how the **stun flowdata catlife** command is used at the router prompt.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata catlife 150 keepalive 30
```

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 keepalive

Note Effective with Cisco IOS Release 15.0(1)M, the **stun flowdata keepalive** command is replaced by the command **stun flowdata catlife**.

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.

stunflowdata keepalive *seconds*
no stunflowdata keepalive *seconds*

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.
15.0(1)M	This command was replaced. The call application **stun flowdata keepalive** command was replaced by the commands **stun flowdata catlife**. The **stun flowdata keepalive** command is hidden and depreciated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

You can use the **stun flowdata keepalive** command to decide how often to send keepalives. Keepalives are application mechanisms for maintaining alive the firewall traversal mappings associated with firewalls.

TRP works with a Call Agent which supports firewall traversal. In this mode, the Call Agent sends a request to TRP to open the pinhole. The request contains local, remote IP /Port, token, and other Cisco-flow data parameters.

TRP sends a STUN indication message to the firewall with Cisco-flow data, after processing the request. The message contains the STUN header, STUN username, and Cisco-flow data. The firewall validates the token in Cisco-flow data after receiving the STUN packet, and opens the pinhole if validation is successful.

Keepalives in STUN flow between the UDP peers to ensure that the firewall keeps the pinholes open.

This command is hidden and depreciated in Cisco IOS Release 15.0(1)M release because the keepalive interval is configured along with stun flowdata catlife command. When this command is configured or present in start-up configuration during reload, the following command will be nvgen'ed and displayed in **show run** command.

In addition, the following message will be printed during the configuration/reload:

```
Deprecated command. Setting catlife=1270 sec and keepalive=30 sec.
Use the following command to configure non-default values:
stun flowdata catlife <lifetime> keepalive <interval>
```

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 tag *string*
no stun flowdata shared-secret

Syntax Description

tag	0--Defines the password in plaintext and will encrypt the password. 6-- Defines secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES). **Note** Requires AES primary key to be preconfigured. 7-- Defines the password in hidden form and will validate the (encrypted) password before accepting it.
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.
15.0(1)M	This command was modified. The encryption values zero and seven was added to this command.
IOS XE 16.11.1a	Secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES) was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

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. This is a string of 12 to 80 characters. The **no** form of this command will remove the previously configured shared-secret if any. The default form of this command will set the shared-secret to NULL. The password can be encrypted and validated before it is accepted. Firewall traversal is not performed when the shared-secret is set to default.

It is mandatory to specify the encryption type for the shared secret. If a clear text password (type **0**) is configured, it is encrypted as type **6** before saving it to the running configuration.

If you specify the encryption for the shared secret as type **6** or **7**, the entered password is checked against a valid type **6** or **7** password format and saved as type **6** or **7** respectively.

Type-6 passwords are encrypted using AES cipher and a user-defined primary key. These passwords are comparatively more secure. The primary key is never displayed in the configuration. Without the knowledge of the primary key, type **6** shared secret passwords are unusable. If the primary key is modified, the password that is saved as type 6 is re-encrypted with the new primary key. If the primary key configuration is removed, the type **6** shared secret passwords cannot be decrypted, which may result in the authentication failure for calls and registrations.

Note When backing up a configuration or migrating the configuration to another device, the primary key is not dumped. Hence the primary key must be configured again manually.

To configure an encrypted preshared key, see Configuring an Encrypted Preshared Key.

Note The encryption type **7** is supported in IOS XE Release 16.11.1a, but will be deprecated in the later releases. Following warning message is displayed when encryption type **7** is configured.

```
Warning: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password type 6.
```

Examples

The following example shows how the **stun flowdata shared-secret** command is used.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(config-serv-stun)#stun flowdata shared-secret 6 123cisco123cisco
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata agent-id	Configures the agent ID.
stun flowdata catlife	Configures the lifetime of the CAT.

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 arguments or keywords.

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.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

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.

stun usage ice lite

To enable ICE-lite using stun, use the **stun usage ice-lite** command in voice class stun-usage configuration mode. To disable ICE-lite with stun, use the **no** form of this command.

stun usage ice lite
no stun usage ice lite

Syntax Description

This command has no arguments or keywords.

Command Default

ICE-lite is not enabled by default.

Command Modes

Voice-class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE 3.15S Cisco IOS 15.5(3)M	This command was introduced.

Examples

The following example shows how to enable ICE-lite using STUN:

```
Router(config)#voice class stun-usage 25
Router(config-class)#stun usage ice lite
```

subaddress

To configure a subaddress for a POTS port, use the **subaddress** command in dial-peer voice configuration mode. To disable the subaddress, use the **no** form of this command.

subaddress *number*
no subaddress *number*

Syntax Description

number	Actual subaddress of the POTS port.

Command Default

No subaddress is available for a POTS port.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines

You can use this command for any dial-peer voice POTS port. You can configure only one subaddress for each of the POTS ports. The latest entered subaddress on the dial-peer voice port is stored. To check the status of the subaddress configuration, use the **show running-config** command.

Examples

The following examples show that a subaddress of 20 has been set for POTS port 1 and that a subaddress of 10 has been set for POTS port 2:

```
dial-peer voice 1 pots
 destination-pattern 5555555
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 1111111 ring 3
 caller-number 2222222 ring 1
 caller-number 3333333 ring 1
 subaddress 20
dial-peer voice 2 pots
 destination-pattern 4444444
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 6666666 ring 2
 caller-number 7777777 ring 3
 subaddress 10
```

subcell-mux

To enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing on a Cisco router, use the **subcell-mux** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

subcell-mux *time*
no subcell-mux *time*

Syntax Description

time	Timer value, in milliseconds. Range is from 5 to 1000 (1 second). Default is 10.

Command Default

10 ms Subcell multiplexing is off

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)XB	The *time* argument was implemented on the Cisco 3660.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use thiscommand to enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing when the Cisco router interoperates with other equipment that uses subcell multiplexing.

Examples

The following example sets AAL2 CPS subcell multiplexing to 15 ms:

```
Router(conf-voi-serv-sess)# subcell-mux 15
```

Related Commands

Command	Description
voice -service	Specifies the voice encapsulation type and enters voice-service configuration mode.

subscription asnl session history

To specify how long to keep Application Subscribe/Notify Layer (ASNL) subscription history records and how many history records to keep in memory, use the subscription asnl session history command in global configuration mode. To reset to the default, use the no form of this command.

subscription asnl session history {**count** *number* | **duration** *minutes*}
no subscription asnl session history {**count** | **duration**}

Syntax Description

count *number*	Number of records to retain in a session history.
duration *minutes*	Duration, in minutes, for which to keep the record.

Command Default

Default duration is 10 minutes. Default number of records is 50.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The ASNL layer maintains subscription information. Active subscriptions are retained in the active subscription table in system memory. When subscriptions are terminated, they are moved to the subscription table in system memory.

This command controls the ASNL history table. Use this command to specify how many minutes the history record is retained after the subscription is removed, and to specify how many records are retained at any given time.

Examples

The following example specifies that a total of 100 records are to be kept in the RTSP client history:

```
subscription asnl session history count 100
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

subscription maximum

To specify the maximum number of outstanding subscriptions to be accepted or originated by a gateway, use the subscription maximum command in voice service voip sip configuration mode. To remove the maximum number of subscriptions specified, use the **no** form of this command.

subscription maximum {**accept** | **originate**} *number*
no subscription maximum {**accept** | **originate**}

Syntax Description

accept	Subscriptions accepted by the gateway.
originate	Subscriptions originated by the gateway.
number	Maximum number of outstanding subscriptions to be accepted or originated by the gateway.

Command Default

The default number of subscriptions is equal to twice the number of dial-peers configured on the platform.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to configure the maximum number of concurrent SIP subscriptions, up to twice the number of dial-peers configured.

Examples

The following example configures subscription maximums:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# subscription maximum originate 10
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
retry timer	Configures the retry interval for resending SIP messages.
show subscription	Displays active SIP subscriptions.

supervisory answer dualtone

To enable answer supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory answer dualtone command in**voice-port configuration mode. To disable answer supervision on a voice port, use the **no** form of this command.

supervisory answer dualtone [**sensitivity** {**high** | **medium** | **low**}]
no supervisory answer dualtone

Syntax Description

sensitivity	(Optional) Specific detection sensitivity for answer supervision.
high	Increased level of detection sensitivity.
medium	Default level of detection sensitivity.
low	Decreased level of detection sensitivity.

Command Default

Answer supervision is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.2(2)T	This command was introduced on the following platforms: Cisco 1750, Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

This command configures the FXO voice port to detect voice, fax, and modem traffic when calls are answered. If answer supervision is enabled, calls are not recorded as connected until answer supervision is triggered.

This command enables a ring-no-answer timeout that drops calls after a specified period of ringback. The period of ringback can be configured using the **timeouts ringing** command.

This command automatically enables disconnect supervision in the preconnect mode on the voice port if disconnect supervision is not already enabled with the **supervisory disconnect dualtone**command.

This command is applicable to analog FXO voice ports with loop-start signaling.

If false answering is detected, decrease the **sensitivity** setting. If answering detection is failing, increase the **sensitivity** setting.

Examples

The following example enables answer supervision on voice port 0/1/1:

```
voice-port 0/1/1
 supervisory answer dualtone
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.

Command	Description
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts ringing	Specifies the time that the calling voice port allows ringing to continue if a call is not answered.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory custom-cptone

To associate a class of custom call-progress tones with a voice port, use the **supervisory custom-cptone command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory custom-cptone *cptone-name*
no supervisory custom-cptone

Syntax Description

cptone -name	Descriptive identifier of the class of custom call-progress tones to be detected by a voice port. This name must match the *cptone-name* of a class of tones defined by the **voice class custom-cptone** command.

Command Default

U.S. standard call-progress tones are associated with a voice port.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a class of custom call-progress tones, defined by the **voice class custom-cptone** command, with a voice port.

You can associate the same custom call-progress tones to multiple voice ports.

You can associate only one class of custom call-progress tones with a voice port. If you associate a second class of custom call-progress tones with a voice port, the second class of custom tones replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of custom call-progress tones named country-x with voice ports 1/4 and 1/5:

```
voice-port 1/4
 supervisory custom-cptone country-x
 exit
voice-port 1/5
 supervisory custom-cptone country-x
 exit
```

Related Commands

Command	Description
dualtone	Defines a call-progress tone to be detected.
supervisory answer dualtone	Enables answer supervision on an FXO voice port.

Command	Description
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

supervisory disconnect

To enable a supervisory disconnect signal on Foreign Exchange Office (FXO) ports, use the **supervisory disconnect** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect
no supervisory disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Voice-port configuration (config-voiceport)

Command History

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

Usage Guidelines

This command indicates whether supervisory disconnect signaling is available on the FXO port. Supervisory disconnect signaling is a power denial from the switch lasting at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call.

You should configure no supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch.

Note If there is no disconnect supervision on the voice port, the interface could be left active if the caller abandons the call before the far end answers. After the router collects the dialed digits but before the called party answers, the router starts a tone detector. Within this time window, the tone detector listens for signals (such as a fast busy signal) that occur if the originating caller hangs up. If this occurs, the router interprets those tones as a disconnect indication and closes the window.

Examples

The following example configures supervisory disconnect on a voice port:

```
voice-port 2/1/0
 supervisory disconnect
```

supervisory disconnect anytone

To configure a Foreign Exchange Office (FXO) voice port to go on-hook if the router detects any tone from a PBX or the PSTN before an outgoing call is answered, use the **supervisory disconnect anytone command in**voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect anytone
no supervisory disconnect anytone

Syntax Description

This command has no arguments or keywords.

Command Default

The supervisory disconnect function is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

Use this command to provide disconnect if the PBX or PSTN does not provide a supervisory tone. Examples of tones that trigger a disconnect include busy tone, fast busy tone, and dial tone.

This command is enabled only during call setup (before the call is answered).

You must enable echo cancellation; otherwise, ringback tone from the router can trigger a disconnect.

This command replaces the **no supervisory disconnect signal**command. If you enter thiscommand, the supervisory disconnect anytone feature is enabled, and the message supervisory disconnect anytoneis displayed when **show** commands are entered.

If you enter either the **supervisory disconnect anytone**command or the **no supervisory disconnect signal**command, answer supervision is automatically disabled.

Examples

The following example configures voice ports 1/4 and 1/5 to go on-hook if any tone from the PBX or PSTN is detected before the call is answered:

```
voice-port 1/4
 supervisory disconnect anytone
 exit
voice-port 1/5
 supervisory disconnect anytone
 exit
```

The following example disables the disconnect function on voice port 1/5:

```
voice-port 1/5
```

```
no supervisory disconnect anytone
exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.

supervisory disconnect dualtone

To enable disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory disconnect dualtone command in**voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**}
no supervisory disconnect dualtone

Syntax Description

mid -call	Disconnect supervision operates throughout the duration of the call.
pre -connect	Disconnect supervision operates during call setup and stops when the called telephone goes off-hook.

Disconnect supervision is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command configures an FXO voice port to disconnect calls when the router detects call-progress tones from a PBX or the PSTN. Disconnection occurs after the wait-release time specified on the voice port.

Disconnect supervision is automatically enabled in the preconnect mode on the voice port if the **supervisory answer dualtone**command is entered.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples

The following example specifies tone detection during the entire call duration:

```
voice-port 1/5
 supervisory disconnect dualtone mid-call
 exit
```

The following example specifies tone detection only during call setup:

```
voice-port 0/1/1
 supervisory disconnect dualtone pre-connect
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.

Command	Description
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.
timeouts wait-release	Specifies the timeout value for releasing a voice port when an outgoing call is not answered.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory disconnect dualtone voice-class

To assign a previously configured voice class for Foreign Exchange Office (FXO) supervisory disconnect tone to a voice port, use the **supervisory disconnect dualtone voice-class** command in voice port configuration mode. To remove a voice class from a voice-port, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**} **voice-class** *tag*
no supervisory disconnect dualtone voice-class *tag*

Syntax Description

mid -call	Tone detection operates throughout the duration of a call.
pre -connect	Tone detection operates during call setup and stops when the called telephone goes off-hook.
tag	Unique identification number assigned to one voice class. The tag number maps to the tag number assigned using the **voice class dualtone** global configuration command. Range is from 1 to 10000.

Command Default

No voice class is assigned to a voice port.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

You can apply an FXO supervisory disconnect tone voice class to multiple voice ports. You can assign only one FXO supervisory disconnect tone voice class to a voice port. If a second voice class is assigned to a voice port, the second voice class replaces the one previously assigned. You cannot assign separate FXO supervisory disconnect tone commands directly to the voice port.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples

The following example assigns voice class 70 to FXO voice port 0/1/1 and specifies tone detection during the entire call duration:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone mid-call voice-class 70
```

The following example assigns voice class 80 to FXO voice port 0/1/1 and specifies tone detection only during call setup:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone pre-connect voice-class 80
```

Related Commands

Command	Description
channel-group	Defines the time slots of each T1 or E1 circuit.
mode	Sets the mode of the T1/E1 controller and enters specific configuration commands for each mode type in VoATM.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

supervisory disconnect lcfo

To enable a supervisory disconnect signal on an FXS port, use the **supervisory disconnect lcfo** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect lcfo
no supervisory disconnect lcfo

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)YD	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(2)T	Support was added for SCCP Telephony Control Application (STCAPP) analog voice ports.

Usage Guidelines

This command enables a disconnect indication by triggering a power denial using a loop current feed open (LCFO) signal on FXS ports with loop-start signaling. Third-party devices, such as an interactive voice response (IVR) system, can detect a disconnect and clear the call when it receives the power denial signal. To disable the power denial during the disconnect stage, use the **no supervisory disconnect lcfo** command. The duration of the power denial is set with the **timeouts power-denial** command.

Examples

The following example disables the power denial indication on voice port 2/0:

```
voice-port 2/0
 no supervisory disconnect lcfo
```

Related Commands

Command	Description
timeouts power-denial	Sets the duration of the power denial timeout for a specified FXS voice port.

supervisory dualtone-detect-params

To associate a class of modified tone-detection tolerance limits with a voice port, use the **supervisory dualtone-detect-params command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory dualtone-detect-params *tag*
no supervisory dualtone-detect-params

Syntax Description

tag	Tag number of the set of modified tone-detection tolerance limits to be associated with the voice port. The tag number must match the tag number of a voice class configured by the **voice class dualtone-detect-params**command. Range is from 1 to 10000.

Command Default

The default tone-detection tolerance limits are associated with voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a specific set of modified tone-detection tolerance limits, defined by the **voice class dualtone-detect-params**command, with a voice port.

You can associate the same class of modified tone-detection tolerance limits to multiple voice ports.

You can associate only one class of modified tone-detection tolerance limits to a voice port. If you associate a second class of modified tone-detection tolerance limits with a voice port, the second class replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of modified tone-detection tolerance limits that has tag 70 with voice ports 1/5 and 1/6.

```
voice-port 1/5
 supervisory dualtone-detect-params 70
 exit
voice-port 1/6
 supervisory dualtone-detect-params 70
 exit
```

The following example restores the default tone-detection parameters to voice port 1/5.

```
voice-port 1/5
 no supervisory dualtone-detect-params
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class dualtone-detect-params	Creates a voice class for call-progress tone-detection tolerance parameters.

supervisory sit us

To provide detection of eight standard U.S. special information tones (SITs) and certain nonstandard tones (including the AT&T SIT), and to report the detected tone with a preassigned disconnect cause code for disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory sit us**command in voice-port configuration mode. To turn off the detection and disconnect activity, use the **no** form of this command.

supervisory sit us [**all-tones**] [**tone-selector** *value*] [**immediate-release**]
no supervisory sit us

Syntax Description

all-tones	(Optional) Disconnects the call when a SIT or a nonstandard tone is detected.
tone-selector	(Optional) Defines a specific response for call-disconnect when a standard SIT or a nonstandard tone is detected on the incoming or outgoing call.
value	Acceptable values are 0, 1, 2, or 3: • 0--Detection of a standard SIT drops the call, but an AT&T SIT or a nonstandard tone does not cause a disconnect. • 1--Detection of either a standard SIT or nonstandard tone drops the call, but the AT&T SIT does not cause a disconnect. • 2--Detection of a standard SIT or an AT&T SIT results in a call disconnect, but any other nonstandard tone does not cause a disconnect. • 3--Detection of a standard SIT, AT&T SIT, or another nonstandard tone results in a disconnect.
immediate-release	(Optional) Disconnects the call immediately when a SIT is detected on the incoming or outgoing call. Nonstandard tones are ignored.

Command Default

No detection or disconnect occurs for the eight standard U.S. SITs, nonstandard tones, or the AT&T SIT on the FXO voice port for incoming and outgoing calls.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
12.4(24)T	The **all-tones** and **tone-selector**keywords and the *value* argument were added.

Usage Guidelines

This command configures an FXO voice port to detect and disconnect calls when the router detects call-progress tones from a PBX or the PSTN.

Prior to Cisco IOS Release 12.4(24)T, this command specifically detected eight standard U.S. SITs, but not nonstandard tones or the AT&T SIT. Beginning in Cisco IOS Release 12.4(24)T, the **tone-selector***value* option can be configured to detect nonstandard tones played by the service provider when the called number is invalid.

Disconnection occurs after the wait-release time specified on the voice port. Calls are disconnected immediately after a SIT is detected from the PSTN when the **immediate-release** keyword is configured. To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release**command on the voice port.

The SIT reporting complies with standard Q.850 messages in order for fax servers to uniquely identify each condition. This capability is supported for analog FXO trunk and T1/E1 channel-associated signaling (CAS) FXO loop-start.

Note The SIT detection and reporting feature enabled by the **supervisory sit us** command is supported on c5510 and LSI digital signal processors (DSPs). No other DSPs support this feature.

The table below identifies eight standard U.S. SITs and their associated disconnect cause codes.

Note These eight tones are referred to as standard tones based on the tone frequencies and durations shown in the table. These tones are defined in the Telcordia Technologies specification GR-1162-CORE (which is specific to North America). There are other nonstandard SITs that can occur. The AT&T SIT is one of the more common examples of the other variations. The nonstandard SITs can have durations and frequencies comparable to the nominal values for the eight tone segments shown in the table below or the nonstandard SITs can deviate significantly from these nominal values. The **supervisory sit us** command has been modified in Cisco IOS Release 12.4(24)T to provide flexibility in handling these variations.

Table 10: Eight U.S. SITs and Associated Disconnect Cause Codes

Name	First Tone (Hz)	ms	Second Tone (Hz)	ms	Third Tone (Hz)	ms	Disconnect Cause Code
IC	913.8	274	1370.6	274	1776.7	380	8
VC	985.2	380	1370.6	274	1776.7	380	1
RO	985.2	274	1370.6	380	1776.7	380	86
RO	913.8	274	1428.5	380	1776.7	380	86
NC	913.8	380	1370.6	380	1776.7	380	34
NC	985.2	380	1428.5	380	1776.7	380	34
#1	913.8	380	1428.5	274	1776.7	274	21
#2	985.2	274	1428.5	274	1776.7	380	21

Examples

The following example shows how to enable SIT detection for the eight standard U.S. tones and provide for immediate disconnect on the voice port:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us immediate-release
```

The following example shows how to enable SIT detection for all eight standard U.S. tones and configure the delay timeout for 10 seconds:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us
Router(config-voiceport)# timeouts wait-release 10
```

The following example shows how to enable detection for a standard SIT or the AT&T SIT and to provide for immediate disconnect on the voice port (in this case, a nonstandard SIT does not cause a disconnect):

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us tone-selector 2 immediate-release
```

Related Commands

Command	Description
timeouts wait-release	Configures the delay timeout before the system starts the process for releasing voice ports.

supplementary-service h225-notify cid-update (dal peer)

To enable individual dial peers to send H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in dal peer configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update
no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

dal peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies that an individual dial peer should provide caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode to specify this capability globally.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no
 supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.

Command	Description
supplementary-service h225-notify cid-update (voice-service)	Globally enables the sending of H.225 messages with caller-ID updates.

supplementary-service h225-notify cid-update (voice-service)

To globally enable the sending of H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update
no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command globally provides caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in dial-peer configuration mode to specify this capability for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no
 supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
supplementary-service h225-notify cid-update (dial-peer)	Enables the sending of H.225 messages with caller-ID updates for individual dial peers.

Command	Description
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.2 (dial peer)

To enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.2** command in dial peer configuration mode. To disable H.450.2 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450 . 2
no supplementary-service h450 . 2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies the use of the H.450.2 standard protocol for call transfers across a VoIP network for the calls handled by an individual dial peer. Use the **supplementary-service h450.2** command in voice-service configuration mode to specify H.450.2 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.2 services for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# no supplementary-service h450.2

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.2 (voice-service)	Globally enables H.450.2 capabilities for call transfers.

supplementary-service h450.2 (voice-service)

To globally enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.2**command in voice-service configuration mode. To disable H.450.2 capabilities globally, use the **no** form of this command.

supplementary-service h450 . 2
no supplementary-service h450 . 2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.2 standard protocol for call transfers for all calls across a VoIP network. Use the **no supplementary-service h450.2** command in dial-peer configuration mode to disable H.450.2 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.2 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.2

Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.2 (dial-peer)	Enables H.450.2 call transfer capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.3 (dial peer)

To enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network for an individual dial peer, use the **supplementary-service h450.3**command in dial peer configuration mode. To disable H.450.3 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450 . 3
no supplementary-service h450 . 3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.3 standard protocol for call forwarding for calls handled by an individual dial peer. Use the **supplementary-service h450.3** command in voice-service configuration mode to specify H.450.3 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.3 capabilities for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# no
 supplementary-service h450.3

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.

supplementary-service h450.3 (voice-service)

To globally enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network, use the **supplementary-service h450.3** command in voice-service configuration mode. To disable H.450.3 capabilities globally, use the **no** form of this command.

supplementary-service h450 . 3
no supplementary-service h450 . 3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.3 standard protocol for call forwarding across a VoIP network. Use the **no supplementary-service h450.3**command in dial-peer configuration mode to disable H.450.3 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.3 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.3

Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.3 (dial-peer)	Enables H.450.3 call forwarding capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.7

To globally enable H.450.7 supplementary services capabilities exchange for message-waiting indication (MWI) across a VoIP network, use the **supplementary-service h450.7** command in voice-service or dial-peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service h450 . 7
no supplementary-service h450 . 7

Syntax Description

There are no keywords or arguments.

Command Default

H.450.7 supplementary services are disabled.

Command Modes

Voice service configuration (config-voi-serv)
Dial-peer configuration (config-dial-peer)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use this command when you are implementing QSIG supplementary service features that use the H.450.7 standard.

Use this command in voice-service configuration mode to affect all dial peers globally. Use this command in dial-peer configuration mode to affect an individual dial peer:

If the **supplementary-service h450.7** command is not in use, the services are globally disabled by default.

If the **supplementary-service h450.7** command is not in use in voice-service configuration mode, you can use this command in dial-peer configuration mode to enable the services on individual dial peers.

If the **supplementary-service h450.7** command is in use in voice-service configuration mode, the services are globally enabled and you cannot disable the services on individual dial peers.

Examples

The following example shows how to globally enable H.450.7 supplemental services:

```
voice service voip
 supplementary-service h450.7
```

The following example shows how to enable H.450.7 supplemental services on dial peer 256:

```
dial-peer voice 256 voip
 supplementary-service h450.7
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.

Command	Description
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.12 (dial peer)

To enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.12** command in dial peer configuration mode. To disable H.450.12 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450 . 12
no supplementary-service h450 . 12

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.12 standard protocol for call transfers across a VoIP network for calls handled by an individual dial peer. Use the **supplementary-service h450.12** command in voice-service configuration mode to specify H.450.12 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Examples

The following example enables H.450.12 capabilities on dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# supplementary-service h450.12

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.12 (voice-service)	Globally enables H.450.12 capabilities.

supplementary-service h450.12 (voice-service)

To globally enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.12**command in voice-service configuration mode. To disable H.450.12 capabilities globally, use the **no** form of this command.

supplementary-service h450 . 12 [**advertise-only**]
no supplementary-service h450 . 12 [**advertise-only**]

Syntax Description

advertise-only	(Optional) Advertises H.450 capabilities to the remote end but does not require H.450.12 responses.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The H.450.12 standard provides a means to advertise and discover H.450.2 call transfer and H.450.3 call forwarding capabilities in voice gateway endpoints on a call-by-call basis. When H.450.12 is enabled, use of H.450.2 and H.450.3 standards is disabled for call transfers and call forwards unless a positive H.450.12 indication is received from all the other VoIP endpoints involved in the call. If positive H.450.12 indications are received, the router uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding. If a positive H.450.12 indication is not received, the router uses the alternative method that you have configured for call transfers and forwards, which, for Cisco CallManager Express (Cisco CME) 3.1 systems, may be either hairpin call routing or an H.450 tandem gateway. This command is useful when you have a mixed network with some endpoints that support H.450.2 and H.450.3 standards and other endpoints that do not support those standards.

This command specifies the global use of the H.450.12 standard protocol for all calls across a VoIP network. Use the **supplementary-service h450.12** command in dial-peer configuration mode to specify H.450.12 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Use the **advertise-only** keyword on a Cisco CME 3.1 system when you have only Cisco CME 3.0 systems in your network in addition to Cisco CME 3.1 systems. Cisco CME 3.0 systems can use H.450.2 and H.450.3 standards, but are unable to respond to H.450.12 queries. The **advertise-only** keyword enables a Cisco CME 3.1 system to bypass the requirement that a system respond to an H.450.12 query in order to use H.450.2 and H.450.3 standards for transferring and forwarding calls.

Examples

The following example enables H.450.12 capabilities at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12

Router(config-voi-serv)# exit
```

The following example enables H.450.12 capabilities at a global level in advertise-only mode on a Cisco CME 3.1 system to enable call transfers using the H.450.2 standard and call forwards using the H.450.3 standard with Cisco CME 3.0 systems in the network.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12
 advertise-only
Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.12 (dial-peer)	Enables H.450.12 capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service media-renegotiate

To globally enable midcall media renegotiation for supplementary services, use the **supplementary-service media-renegotiate** command in voice-service configuration mode. To disable midcall media renegotiation for supplementary services, use the **no** form of this command.

supplementary-service media-renegotiate
no supplementary-service media-renegotiate

Syntax Description

This command has no arguments or keywords.

Command Default

Midcall media renegotiation for supplementary services is disabled.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

This command enables midcall media renegotiation, or key renegotiation, for all calls across a VoIP network. To implement media encryption, the two endpoints controlled by Cisco Unified Communications Manager Express (Cisco Unified CME) need to exchange keys that they will use to encrypt and decrypt packets. Midcall key renegotiation is required to support interoperation and supplementary services among multiple VoIP suites in a secure media environment using Secure Real-Time Transport Protocol (SRTP).

Note The video part of a video stream will not play if the **supplementary-service media-renegotiate** command is configured in voice-service configuration mode.

Examples

The following example enables midcall media renegotiation for supplementary services at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service media-renegotiate
Router(config-voi-serv)# exit
```

supplementary-service qsig call-forward

To specify that calls are using QSIG and require supplementary services for call forwarding, use the **supplementary-service qsig call-forward**command in voice-service or dial-peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service qsig call-forward
no supplementary-service qsig call-forward

Syntax Description

This command has no keywords or arguments.

Command Default

The functionality is disabled.

Command Modes

Voice service configuration (config-voi-serv)
Dial-peer configuration (dial-peer-config)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command provides QSIG call-forwarding supplementary services (ISO 13873) when necessary to forward calls to another number.

Use this command in voice-service configuration mode, which is enabled by the **voice service pots**command, to affect all POTS dial peers globally. Use this command in dial-peer configuration mode, which is enabled by the **dial-peer voice** command, to affect a single POTS dial peer.

If you are not using the **supplementary-service qsig call-forward**command, the services are globally disabled by default.

If you are not using the **supplementary-service qsig call-forward** command in voice-service configuration mode, you can use this command in dial-peer configuration mode to enable the services on individual POTS dial peers.

If you are using the **supplementary-service qsig call-forward** command in voice-service configuration mode, this feature is globally enabled and you cannot disable the services on individual POTS dial peers.

Examples

The following example shows how to enable QSIG call-forwarding treatment for all POTS calls:

```
Router(config)# voice service pots
Router(conf-voi-serv)# supplementary-service qsig call-forward
```

The following example shows how to enable QSIG call-forwarding treatment for calls on POTS dial-peer 23:

```
Router(config)# dial-peer voice 23 pots
Router(config-dial-peer)# supplementary-service qsig call-forward
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
voice service voip	Enters voice-service configuration mode.

supplementary-service sip

To enable SIP supplementary service capabilities for call forwarding and call transfers across a SIP network, use the **supplementary-service sip** command in dial peer voice or voice service VOIP configuration mode. To disable supplementary service capabilities, use the **no** form of this command.

supplementary-service sip {**handle-replaces** | **moved-temporarily** | **refer**}
no supplementary-service sip {**handle-replaces** | **moved-temporarily** | **refer**}

Syntax Description

handle-replaces	Replaces the Dialog-ID in the Replaces Header with the peer Dialog-ID.
moved-temporarily	Enables SIP Redirect response for call forwarding.
refer	Enables SIP REFER message for call transfers.

Command Default

SIP supplementary service capabilities are enabled globally.

Command Modes

Dial peer voice configuration (config-dial-peer)

Voice service configuration (conf-voi-serv)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.2(2)T1	This command was modified. The **handle-replaces** keyword was introduced.
15.3(1)T	This command was modified. With CSCub47586, if an INVITE (incoming call or incoming forward) with a diversion header is received while the **no supplementary-service sip moved-temporarily** form of this command is enabled, on either an inbound call leg or an outbound call leg, the call is disconnected.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The **supplementary-service sip refer** command enables REFER message pass-through on a router.

The **no** form of the **supplementary-service sip** command allows you to disable a supplementary service feature (call forwarding or call transfer) if the destination gateway does not support the supplementary service. You can disable the feature either globally or for a specific SIP trunk (dial peer).

- The **no supplementary-service sip handle-replaces** command replaces the Dialog-ID in the Replaces Header with the peer Dialog-ID.
- The **no supplementary-service sip moved-temporarily** command prevents the router from sending a redirect response to the destination for call forwarding. SDP Passthrough is not supported in 302-consumption mode or Refer-consumption mode. With CSCub47586, if an INVITE (incoming call

or incoming forward) with a diversion header is received while SDP Pass through is enabled on either an inbound call leg or an outbound call leg, the call is disconnected.

- The **no supplementary-service sip refer** command prevents the router from forwarding a REFER message to the destination for call transfers. The router instead attempts to initiate a hairpin call to the new target.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

On Cisco Unified Communications Manager Express (CME), this command is supported for calls between SIP phones and for calls between SCCP phones. It is not supported for a mixture of SCCP and SIP phones; for example, it has no effect for calls from an SCCP phone to a SIP phone. On the Cisco UBE, this command is supported for SIP trunk-to-SIP trunk calls.

Examples

The following example shows how to disable SIP call transfer capabilities for dial peer 37:

```
Device(config)# dial-peer voice 37 voip
Device(config-dial-peer)# destination-pattern 555....
Device(config-dial-peer)# session target ipv4:10.5.6.7

Device(config-dial-peer)# no supplementary-service sip refer
```

The following example shows how to disable SIP call forwarding capabilities globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip moved-temporarily
```

The following example shows how to enable a REFER message pass-through on the Cisco UBE globally and how to disable the Refer-To header modification:

```
Device(config)# voice service voip
Device(conf-voi-serv)# supplementary-service sip refer
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# referto-passing
```

The following example shows how to enable a REFER message consumption on the Cisco UBE globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip refer
```

The following example shows how to enable REFER message consumption on the Cisco UBE for dial peer 22:

```
Device(config)# dial-peer voice 22 voip
Device(config-dial-peer)# no supplementary-service sip refer
```

The following example shows how to enable a REFER message to replace the Dialog-ID in the Replaces Header with the peer Dialog-ID on the Cisco UBE for dial peer:

```
Device(config)# dial-peer voice 34 voip
Device(config-dial-peer)# no supplementary-service sip handle-replaces [system]
```

The following example shows how to enable a REFER message to replace the Dialog-ID in the Replaces Header with the peer Dialog-ID on the Cisco UBE globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip handle-replaces
```

Related Commands

Command	Description
supplementary-service h450.2 (voice-service)	Globally enables H.450.2 capabilities for call transfer.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.
referto-passing	Disables dial peer lookup and modification of the Refer-To header while passing across REFER message on the Cisco UBE during a call transfer.

supported language

To configure Session Initiation Protocol (SIP) Accept-Language header support, use the **supported-language**command in voice service or dial-peer voice configuration mode. To disable Accept-Language header support, use the **no** form of this command.

supported-language *language-code* **language-param** *qvalue*
no **supported-language** *language-code*

Syntax Description

language -code	Any of 139 languages designated by a two-letter ISO-639 country code.
qvalue	The priority of the language, with languages sorted in descending order according the assigned parameter value. Valid values include zero, one, or a decimal fraction in the range .001 through .999. Default is 1, the highest priority.
language -param	Specifies language preferences by associating a parameter with the language being configured.

Command Default

qvalue: 1

Command Modes

Dial-peer voice configuration (config-dial-peer)
Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

To include the Accept-Language header in outgoing SIP INVITE messages, and enable Accept-Language header support on specific trunk groups with different language requirements, use dial-peer voice configuration mode, which is enabled by the dial-peer voice command . To enable Accept-Language headers to be included in both SIP INVITE messages and OPTIONS responses, use voice service configuration mode, enabled by the voice service pots command. If both voice service and dial-peer voice mode accept-language support are configured, and there are no dial-peer matches, the outgoing INVITE message contains the voice service specified languages. Otherwise, the INVITE contains the dial-peer configured languages.

The SIP Accept-Language Header Support feature supports 139 languages which are designated by a two-letter ISO-639 country code. The following is a partial list of supported language codes and languages. To display a complete listing use the help command supported-language ?.

- • **AR** --Arabic
  • **ZH** --Chinese
  • EN--English
  • EO--Esperanto
  • DE--German
  • EL--Greek
  • HE--Hebrew
  • GA--Irish
  • IT--Italian

- JA--Japanese
- KO--Korean
- RU--Russian
- ES--Spanish
- SW--Swahili
- SV--Swedish
- VI--Vietnamese
- YI--Yiddish
- ZU--Zulu

Examples

The following example configures Italian to be the preferred language, followed by Greek:

```
s
upported-language IT language-param .9
supported-language EL language-param .8
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers.

suppress

To suppress accounting for a specific call leg, use the **suppress** command in gateway accounting AAA configuration mode. To reenable accounting for that leg, use the **no** form of this command.

suppress [{**pots** | **rotary** | **voip**}]
no suppress [{**pots** | **rotary** | **voip**}]

Syntax Description

pots	(Optional) POTS call leg.
rotary	(Optional) Rotary dial peer.
voip	(Optional) VoIP call leg.

Command Default

Accounting is enabled.

Command Modes

Gateway accounting AAA configuration (config-gw-accounting-aaa)

Command History

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

Usage Guidelines

Use this command to turn off accounting for a specific call leg.

If both incoming and outgoing call legs are of the same type, no accounting packets are generated.

Use the **rotary** keyword to suppress excess start and stop accounting records. This causes only one pair of records to be generated for every connection attempt through a dial peer.

Examples

The following example suppresses accounting for the POTS call leg.

```
suppress pots
```

Related Commands

Command	Description
debug suppress rotary	Displays connection attempt statistics.
gw-accounting aaa	Enables VoIP gateway accounting.

survivability single-register

To enable survivability for phones that register with Nano CUBE using single register request, execute **survivability single-register** command in voice service voip >> sip configuration mode. To disable, use **no** form of this command.

survivability single-register
no survivability single-register

Syntax Description

This command has no arguments or keywords.

Command Default

Survivability is not enabled for phones that send single register request.

Command Modes

voice service voip >> sip

Command History

Release	Modification
Cisco IOS 15.6(1)T	This command was introduced.

Usage Guidelines

When this command is configured, Nano CUBE always checks for the response from remote side. Request timeout on WAN side or response other than 200, 4XX, and 3XX received by Nano CUBE from SBC enables the survivability.

Example

```
Device> enable
Device# configure terminal
Device(config)#  voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# survivability single-register
```

suspend-resume (SIP)

To enable SIP Suspend and Resume functionality, use the **suspend-resume** command in SIP user agent configuration mode. To disable SIP Suspend and Resume functionality, use the **no** form of this command.

suspend-resume
no suspend-resume

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Session Initiation Protocol (SIP) gateways are now enabled to use Suspend and Resume. Suspend and Resume are basic functions of ISDN and ISDN User Part (ISUP) signaling procedures. A Suspend message temporarily halts communication (call hold), and a Resume message is received after a Suspend message and continues the communication.

Examples

The following example disables Suspend and Resume functionality:

```
Router(config)# sip-ua
Router(config-sip-ua)# no suspend-resume
```

Related Commands

Command	Description
show sip -ua status	Displays SIP UA status.
sip -ua	Enables the SIP user-agent configuration commands.

switchback interval

To set the amount of time that the digital signal processor (DSP) farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails, use the **switchback interval**command in SCCP Cisco Unified CallManager configuration mode. To reset the amount of time to the default value, use the **no** form of this command.

switchback interval *seconds*
no switchback interval

Syntax Description

seconds	Timer value, in seconds. Range is 1 to 3600. Default is 60.

Command Default

60 seconds

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback interval value to meet your needs.

Examples

The following example sets the length of time the DSP farm waits to before polling the primary Cisco Unified CallManager to 120 seconds (2 minutes):

```
Router(conf-sccp-ccm)# switchback interval 120
```

Related Commands

Command	Description
connect interval	Specifies how many times a given profile attempts to connect to the specific CiscoUnified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchback method

To set the Cisco Unified CallManager switchback method, use the **switchback method**command in Skinny SCCP Cisco Unified CallManager configuration mode. To reset to the default value, use the **no** form of this command.

switchback method {**graceful** | **guard** [*timeout-guard-value*] | **immediate** | **uptime** *uptime-timeout-value*}
no switchback method

Syntax Description

graceful	Selects the graceful switchback method.
guard	Selects the graceful with guard switchback method.
guard timeout value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.
immediate	Selects the immediate switchback method.
uptime	Selects the uptime-delay switchback method.
uptime timeout value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.

Command Default

Guard is the default switchback method, with a timeout value of 7200 seconds.

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to set the Cisco Unified CallManager switchback method. When a switch-over happens with the secondary Cisco Unified CallManager initiates the switchback process with that higher-order Cisco Unified CallManager. The available switchback methods follow:

- graceful--The Cisco Unified CallManager switchback happens only after all the active sessions are terminated gracefully.
- guard--The Cisco Unified CallManager switchback happens either when the active sessions are terminated gracefully or when the guard timer expires, whichever happens first.
- immediate--Performs the Cisco Unified CallManager switchback to the higher order CiscoUnified CallManager immediately as soon as the timer expires, whether there is an active connection or not.
- uptime--Once the higher-order Cisco Unified CallManager comes alive, the uptime timer in initiated.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback method to meet your needs.

Examples

The following example sets the Cisco Unified CallManager switchback method to happen only after all the active sessions are terminated gracefully.

```
Router(config-sccp-ccm)# switchback method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchover method

To set the switchover method that the Skinny Client Control Protocol (SCCP) client uses when the communication link between the active Cisco Unified CallManager and the SCCP client goes down, use the switchover methodcommand in SCCP Cisco Unified CallManager configuration mode. To reset the switchover method to the default, use the **no** form of this command.

switchover method {**graceful** | **immediate**}
no switchover method

Syntax Description

graceful	Switchover happens only after all the active sessions are terminated gracefully.
immediate	Switches over to any one of the secondary Cisco Unified CallManager immediately.

Command Default

Graceful

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When the communication link between the active Cisco Unified CallManager and the SCCP client goes down the SCCP client tries to connect to one of the secondary Cisco Unified CallManagers using one of the following switchover methods:

- graceful--The Cisco Unified CallManager switchover happens only after all the active sessions are terminated gracefully.
- immediate--Regardless of whether there is an active connection or not the SCCP client switches over to one of the secondary Cisco Unified CallManagers immediately. If the SCCP Client is not able to connect to a secondary Cisco CUnified allManager, it continues polling for a CiscoUnified CallManager connection.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchover method to meet your needs.

Examples

The following example sets the switchover method that the SCCP client uses to connect to a secondary Cisco Unified CallManager to happen only after all the active sessions are terminated gracefully:

```
Router (config-sccp-ccm)# switchover method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters the SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.