

Software version IL1.1

FEBRUARY 2013

CISCO TELEPRESENCE ISDN LINK

ADMINISTRATOR GUIDE



What's in this guide?

The top menu bar and the entries in the Table of Contents are all hyperlinks, just click on them to go to the topic.

We recommend you visit our web site regularly for updated versions of the user documentation.

Go to: <http://www.cisco.com/go/isdnlink-docs>

Table of Contents

Introduction.....	4	Configuring the TelePresence endpoint for ISDN.....	18
About this guide.....	5	Setting the default call protocol to H320.....	18
User documentation	5	Setting the call protocol to H320 by each call	18
Technical specification	5	Making a call using the Touch controller.....	19
Support and software download	5	Making a call using the remote control.....	20
What's new in this version	6	Making a call using the web interface of the endpoint	21
Automatic pairing mode	6	Making a call using the command line interface on the endpoint.....	22
Support for H.320 side encryption.....	6	Software upgrade.....	23
Support for AAC-LD audio protocol.....	6	The software upgrade menu	24
Support for CDP.....	6	Upgrading the software	25
Serial port access	6	Installing the software from a file	25
New settings.....	6	Installing the software from an URL	25
Settings that are removed.....	7	Status information.....	26
About ISDN Link.....	8	Monitoring ISDN Link status.....	27
Supported software versions	8	The status information descriptions.....	28
Automatic pairing mode	8	System settings	48
Manual pairing mode.....	8	The ISDN Link Configuration menu.....	49
Changing the password	8	The system setting descriptions.....	50
Getting started.....	9	Appendices.....	72
User scenarios	10	Password protection.....	73
Two user scenarios with IP network.....	10	Password management.....	73
User scenario with no IP infrastructure	10	Changing the system password	73
Installing and pairing the ISDN Link.....	11	Setting a root password.....	73
Installing the ISDN Link.....	11	Connecting to the ISDN Link.....	74
Prerequisites for pairing	11	Connect to the ISDN Link through the serial port	74
Pairing the ISDN Link.....	11	Connect to the ISDN Link through SSH	74
Automatic pairing mode	11	Connect to the ISDN Link through the endpoint's web interface	74
Manual pairing mode.....	11	Finding the IP address	75
Configuring the ISDN Link.....	12	Finding the IP address by connecting to the ISDN Link serial port	75
ISDN Link web interface overview	13	Finding the IP address from the endpoint's web interface	75
Configuration examples	14		
Example with support for PRI E1 mode.....	14		
Example with support for PRI T1 mode.....	15		
Example with support for BRI Euro type.....	16		
Example with support for External Network.....	17		



- Unpairing the ISDN Link 76
 - Persistent pairing..... 76
 - Unpairing from the TelePresence endpoint's web interface 76
 - Forced unpairing..... 76
- Factory resetting the ISDN Link 77
 - Factory resetting the ISDN Link..... 77
 - Factory resetting the ISDN Link during boot through the serial port 77
- Software upgrade from the command line interface..... 78
 - Software upgrade from IL1.0 to IL1.1 78
 - Checking the software version..... 78
 - Installing the software from an URL 78
 - The SCP upgrade method..... 78
- About audio and video encryption..... 79
 - Encryption indicators 79
- Configuring parallel dialing for ADTRAN switch and PRI 80
- The physical interface 81
 - Front panel 81
 - Rear panel 82
- Connecting the cables..... 83
- Mounting the unit..... 84
 - Wall mounting 84
 - Table stand 84
- Pin-out schemes..... 85
- Cables 87
- Supported RFCs 88



INTRODUCTION

About this guide

The main objective with this guide is to describe how to manage the Cisco TelePresence ISDN Link in automatic pairing mode.

When using the ISDN Link in [automatic pairing mode](#) the recommended way to manage the ISDN Link is from the TelePresence endpoint's web interface. The ISDN Link must be running software version IL1.1 or later, and the TelePresence endpoint must be running TC6.0 or later. It is also possible to connect to the unit through the serial port, or over the network through SSH. For details see: [ISDN Link API Reference Guide](#).

When using the ISDN Link in [manual pairing mode](#) you will connect through the serial port or, if you know the IP address, over the network through SSH. For details see: [ISDN Link API Reference Guide](#).

User documentation

User documentation for Cisco TelePresence ISDN Link can be found on <http://www.cisco.com/go/isdnlink-docs>.

Document categories

For each product you will find the documents under the following categories:

Installation guide:

Install and Upgrade | Install and Upgrade Guides

Administrator guide:

Maintain and Operate | Maintain and Operate Guides

API reference guide:

Reference Guides | Command references

Regulatory compliance and safety information:

Install and Upgrade | Install and Upgrade Guides

Software release notes:

Software Downloads, Release and General Information | Release Notes

Licensing information:

Software Downloads, Release and General Information | Licensing Information

Technical specification

Information about the technical specification is found on our web site: [Cisco TelePresence ISDN Link Data Sheet](#)

Support and software download

You can download the software for the ISDN Link from our web site: <http://www.cisco.com/cisco/web/support>

1. Click the *Download* tab.
2. Type "ISDN Link" in the search field.
3. Click the *Download* button. To download the software, you must log in with your Cisco.com user ID.

What's new in this version

This section provides an overview of the new and changed settings and new features in the IL1.1 software version.

Automatic pairing mode

Automatic pairing mechanism with the endpoint, for enhanced user interaction and management.

Support for H.320 side encryption

Support for H.320 side encryption (AES-128).

H.320 side encryption is only supported when:

- automatic pairing mode is used.
- and, the endpoint supports media (SIP) encryption.

Support for AAC-LD audio protocol

Support for AAC-LD audio protocol.

Support for CDP

Support for obtaining VLAN configuration from CDP (Cisco Discovery Protocol) provisioner.

Serial port access

Configurable disabling of serial port access during boot.

New settings

xConfiguration Gateway PairingMode

xConfiguration Network [1..1] VLAN Voice Mode

xConfiguration Network [1..1] VLAN Voice VlanId

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Encryption Type

xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Encryption Type

xStatus Network [1..1] CDP Address

xStatus Network [1..1] CDP Capabilities

xStatus Network [1..1] CDP DeviceId

xStatus Network [1..1] CDP Duplex

xStatus Network [1..1] CDP Platform

xStatus Network [1..1] CDP PortId

xStatus Network [1..1] CDP PrimaryMgmtAddress

xStatus Network [1..1] CDP SysName

xStatus Network [1..1] CDP SysObjectID

xStatus Network [1..1] CDP Version

xStatus Network [1..1] CDP VoIPApplianceVlanID

xStatus Network [1..1] CDP VTPMgmtDomain

xStatus Network [1..1] VLAN Native VlanId

xStatus Network [1..1] VLAN Voice VlanId



Settings that have been modified

xConfiguration Network [1..1] IPv6 Assignment

OLD: Value space: Static/Autoconf

NEW: Value space: Static/DHCPv6/Autoconf

xConfiguration H320 Encryption

RENAMED: From SIP Encryption to H320 Encryption

Settings that are removed

xConfiguration SIP Profile [1..1] TlsVerify

COMMENT: Was never used.

About ISDN Link

The Cisco TelePresence® ISDN Link is a compact appliance for in-room ISDN and external network connectivity.

The ISDN Link provides direct connectivity for IP-to-ISDN or IP-to-V.35 networks (MX-, SX-, EX-, and C-series). It can be used as main connection or a back up connection. Support for up to 4 Basic Rate Interface (BRI) or 1 Primary Rate Interface (PRI) ISDN ports and external networks (cable standards V.35, RS530, RS449, and RS366).

Supported software versions

Software version IL1.1:

- Software version IL1.1.x is supported for Cisco TelePresence EX-, MX-, SX-, and C-Series running TC6.0.x.
- Software version IL1.1.x is supported for TelePresence EX-, MX-, SX-, and C-Series running TC5.1.x.

Software version IL1.0:

- Software version IL1.0.x is supported for TelePresence EX-Series running TE6.0.x.
- Software version IL1.0.x is supported for TelePresence EX-, MX-, SX-, and C-Series running TC5.1.x.
- Software version IL1.0.x is supported for TelePresence E-Series running TE4.2.x.

Automatic pairing mode

Automatic pairing mode is supported in software version IL1.1, and later, for Cisco TelePresence MX-, SX-, EX-, and C-Series running TC6.0, and later.

Manual pairing mode

Manual pairing mode is supported from software version IL1.0, and later, for TelePresence EX-, MX-, SX-, and C-Series running TC5.

NOTE: If you have TC6/IL1.1 it is recommended to use the ISDN Link in automatic pairing mode.

Changing the password

The ISDN Link is delivered with a default user account with no password set. This user has full access rights to configuration of the system.

NOTE: We strongly recommend that you set a password to restrict access to system configuration.

For details see [“Password protection”](#) on page 73

GETTING STARTED

User scenarios

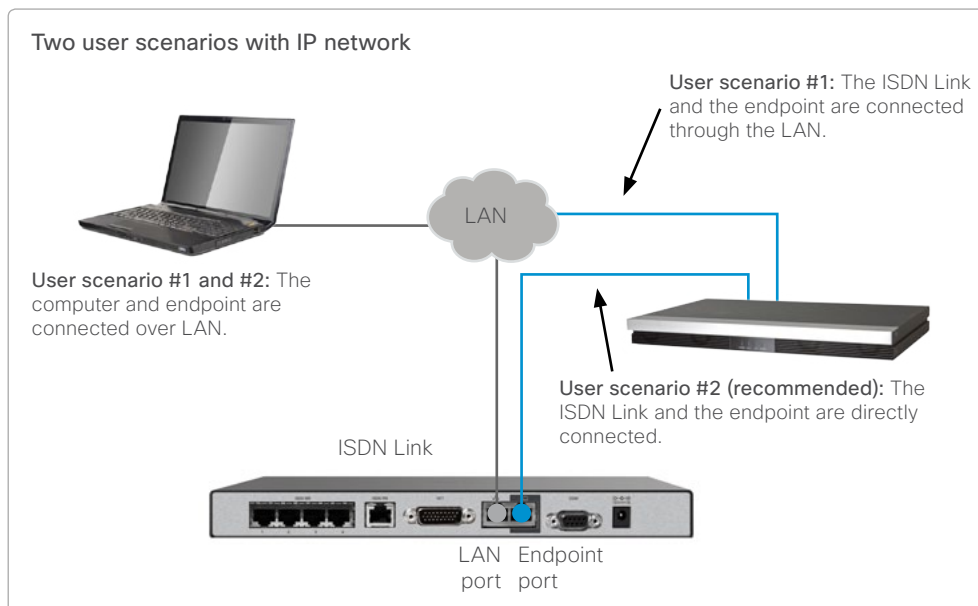
The ISDN Link can be used with or without IP infrastructure. The TelePresence endpoint in the illustrations for the three user scenarios is shown as a single codec without monitor, microphone and loudspeakers. You will need a computer for configuration and maintenance of the ISDN Link.

NOTE: The endpoint and ISDN Link must be on the same subnet. If the endpoint and/or ISDN Link are assigned new IP addresses they will remain paired as long as they are kept in the same subnet.

Two user scenarios with IP network

The user scenarios with IP network allows for automatic pairing mode via the TelePresence endpoint's web interface.

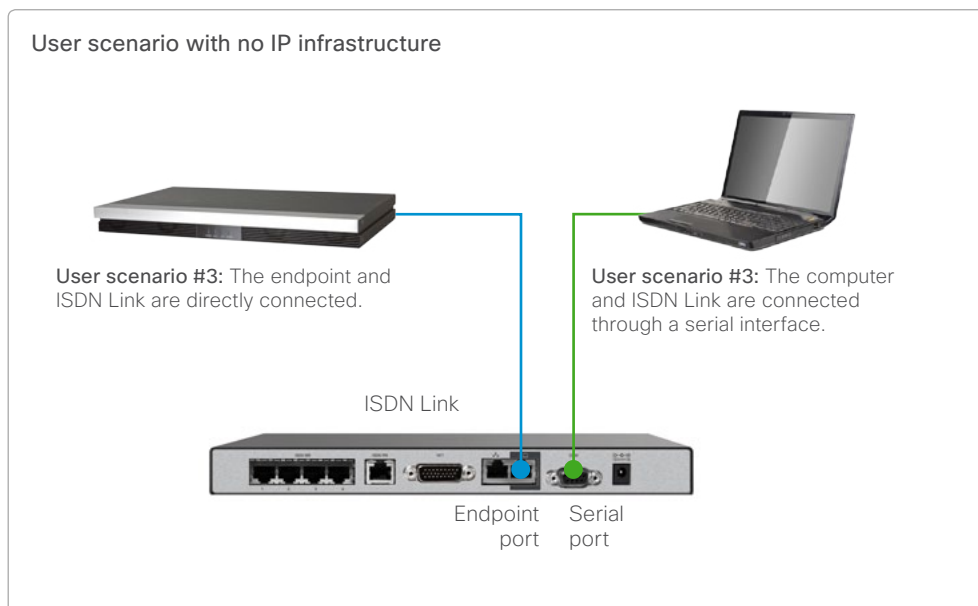
- **User scenario #1:** The ISDN Link and endpoint are connected through the LAN. The endpoint and computer are connected through the LAN.
- **User scenario #2 (recommended):** The ISDN Link and endpoint are connected through a direct connection. The endpoint and computer are connected through the LAN.



User scenario with no IP infrastructure

In the user scenario with no IP infrastructure, you must manually pair the ISDN Link via the command line interface. See the [ISDN Link API Guide](#) for details.

- **User scenario #3:** The ISDN Link and endpoint are connected through a direct connection. The ISDN Link and computer are connected through the serial interface.



Installing and pairing the ISDN Link

Installing the ISDN Link

Follow the instructions as described in the **ISDN Link Installation Guide** supplied with the unit, or download the **ISDN Link Installation Guide** from our web page.

Go to: http://www.cisco.com/en/US/products/ps12504/prod_installation_guides_list.html

Prerequisites for pairing

- The TelePresence endpoint and ISDN Link must run the correct software. For details see “Supported software versions” on page 8.
- The endpoint and ISDN Link must be on the same subnet.
- For optimum use, the Ethernet cable should be directly connected between the Endpoint port on the ISDN Link, and the Ethernet port on the endpoint.
- If the ISDN Link has been previously paired to a TelePresence endpoint, make sure both devices are properly unpaired before starting the pairing process.
- Make sure the *NetworkServices SSH Mode* is set to On (default) to enable access from the web interface.

Pairing the ISDN Link

Pairing is a process in which the ISDN Link and endpoint communicate with each other in order to establish a connection. The ISDN Link is shipped with pairing mode set to Auto, which enables the ISDN Link to be discovered by a TelePresence endpoint. In both pairing modes there is a one-to-one relationship between the endpoint and ISDN link:

- An endpoint can only use one ISDN Link.
- An ISDN Link can only be used by one endpoint.

Automatic pairing mode

In automatic pairing mode the ISDN Link can be managed from the TelePresence endpoint’s web interface.

1. Open a web browser on your computer, enter the address (IP address or host name) of the TelePresence endpoint in the address bar, and login.
2. From the top menu, go to *Configuration > Peripherals*.
3. Click the Manage ISDN Link button. This will open the ISDN Link page.
4. Click the Search for devices button.
5. Choose your ISDN Link from the list and Click the Pair! button.
During the pairing process a message will display: *Pairing with device: <MAC address>*. The ISDN Link is identified by the MAC Address, which is found on a label underneath the unit.
6. When successfully paired the following text will appear on the ISDN Link page:
This TelePresence device is paired with an ISDN Link.

Manual pairing mode

In manual pairing mode the ISDN Link is managed from a command line interface through the serial port or, if you know the IP address, over Ethernet using SSH.

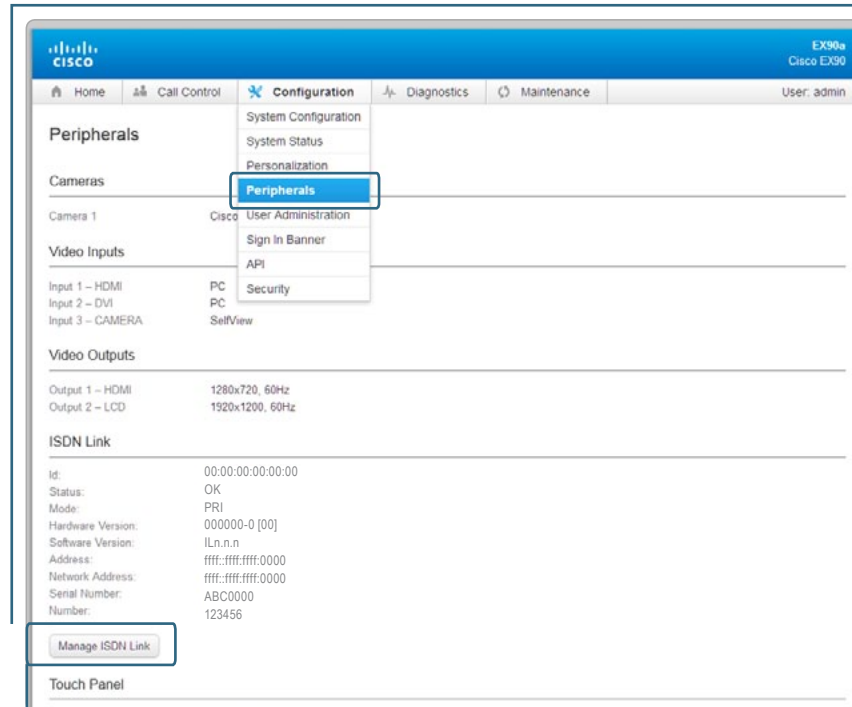
Manual pairing is described in the Appendices section.

Configuring the ISDN Link

The web interface provides full configuration access to the endpoint and ISDN Link. You can connect from a computer and administer the systems remotely.

1. **Connect to the TelePresence endpoint's web interface**
2. Open a web browser on your computer and enter the address (IP address or host name) of the TelePresence endpoint in the address bar.
3. **Sign in**
Enter the username and password for the endpoint and click Sign In.
4. **Manage ISDN Link**
 - From the top menu, go to *Configuration > Peripherals*.
 - Click the Manage ISDN Link button to access the ISDN Link pages.

In the following pages you will find information how to use the web interface for system configuration and maintenance.



The ISDN Link can be managed from the TelePresence endpoint's web interface.

Manage the ISDN Link

Navigate to the *Peripherals* page and click the Manage ISDN Link button to access the ISDN Link pages.

ISDN Link web interface overview

ISDN Link status

Shows the ISDN Link status.

Unpairing the ISDN Link

Click the Unpair this device button to unpair the ISDN Link from the endpoint. See more details in the section: “Unpairing the ISDN Link” on page 76.

The Software Upgrade menu

The software upgrade page is described in the section: “Software upgrade” on page 23.

The ISDN Link Status menu

The status that can be read from the ISDN Link is described in the section: “Status information” on page 26.

The ISDN Link Configuration menu

The system settings that can be set for the ISDN Link is described in the section: “System settings” on page 48.

The screenshot displays the Cisco TelePresence web interface for an ISDN Link. At the top, there is a navigation bar with tabs for Home, Call Control, Configuration, Diagnostics, and Maintenance. The main content area is titled 'ISDN Link' and shows the status as 'OK'. Below this, there are three tabs: 'Software Upgrade', 'ISDN Link Status', and 'ISDN Link Configuration'. A 'SystemUnit' configuration menu is visible on the left, with options for General Settings, Hardware, Software, and State. A callout box points to the 'Unpair this device' button, and another callout box points to the 'ISDN Link Status' tab, listing its sub-items: Software upgrade, ISDN Link Status, and ISDN Link Configuration.

Unpair this device

Click the Unpair this device button to unpair the ISDN Link from the endpoint.

Configuration examples

Use the search option on the page to find the parameters, or choose from the list of menus to the left and then navigate to the parameters in the right pane.

Example with support for PRI E1 mode

Set the H320 net type to PRI:

H320 > General Settings > NetType: PRI

Set the PRI switch type to E1 (Euro):

ISDN > PRI > SwitchType: Euro

Set the number of the high channel for PRI E1 mode:

ISDN > PRI Interface 1 > HighChannel: 31

Set the number of PRI channels:

ISDN > PRI Interface 1 > MaxChannels: 30

Enter the PRI number(s), replace xxx with your number(s):

ISDN > PRI Interface 1 > NumberRangeStart: xxx

ISDN > PRI Interface 1 > NumberRangeStop: xxx

Check the status after configuration

Go to *Configuration > Peripherals* and check the ISDN status information to confirm there are no errors before proceeding. If any errors, or if the power LED is red, please check your configuration.

The first screenshot shows the 'ISDN Link Configuration' page for H320. The 'General Settings' section has 'NetType' set to 'PRI'. The second screenshot shows the 'PRI' configuration page with 'SwitchType' set to 'Euro'. The third screenshot shows the 'Interface 1' configuration page with 'HighChannel' set to 31, 'MaxChannels' set to 30, 'NumberRangeStart' set to 8000, and 'NumberRangeStop' set to 8000.

Navigate to H320 > General Settings > NetType.

Set the H320 Net Type:

- PRI

Click the *Save* button.

Navigate to ISDN > PRI > SwitchType.

Set the ISDN PRI Switch Type:

- Euro

Click the *Save* button.

Navigate to ISDN > PRI > Interface 1.

Enter the number of high and maximum channels for the PRI Euro switch:

- HighChannel: 31
- MaxChannels: 30

Enter your ISDN PRI number:

- NumberRangeStart: xxx
- NumberRangeStop: xxx

Click the *Save* buttons.

Configuration examples

Use the search option on the page to find the parameters, or choose from the list of menus to the left and then navigate to the parameters in the right pane.

Example with support for PRI T1 mode

Set the H320 net type to PRI:

H320 > General Settings > NetType: PRI

Set the PRI switch type to T1. Choose the National ISDN, or the switch type provided by the ISDN Carrier:

ISDN > PRI > SwitchType: NI

Set the number of the high channel for PRI T1 mode:

ISDN > PRI Interface 1 > HighChannel: 23

Set the number of PRI channels:

ISDN > PRI Interface 1 > MaxChannels: 23

Enter the PRI number(s), replace xxx with your number(s):

ISDN > PRI Interface 1 > NumberRangeStart: xxx

ISDN > PRI Interface 1 > NumberRangeStop: xxx

Check the status after configuration

Go to *Configuration > Peripherals* and check the ISDN status information to confirm there are no errors before proceeding. If any errors, or if the power LED is red, please check your configuration.

The first screenshot shows the 'ISDN Link Configuration' page for H320. The 'NetType' dropdown menu is open, showing options: PRI, BRI, External, and G703. 'PRI' is selected.

The second screenshot shows the 'PRI' configuration page. The 'SwitchType' dropdown menu is open, showing options: NI, ATT, Euro, and Japan. 'NI' is selected.

The third screenshot shows the 'PRI Interface 1' configuration page. The following fields are highlighted with blue boxes: HighChannel (23), MaxChannels (23), NumberRangeStart (8000), and NumberRangeStop (8000).

Navigate to H320 > General Settings > NetType.

Set the H320 Net Type:

- PRI

Click the *Save* button.

Navigate to ISDN > PRI > SwitchType.

Set the ISDN PRI Switch Type:

- NI

Click the *Save* button.

Navigate to ISDN > PRI > Interface 1.

Enter the number of high and maximum channels for the PRI NI switch:

- HighChannel: 23
- MaxChannels: 23

Enter your ISDN PRI number:

- NumberRangeStart: xxx
- NumberRangeStop: xxx

Click the *Save* buttons.

Configuration examples

Use the search option on the page to find the parameters, or choose from the list of menus to the left and then navigate to the parameters in the right pane.

Example with support for BRI Euro type

Set the net type:

H320 > General Settings > NetType: BRI

Set the BRI switch type. The switch type setting must match the switch type for the BRI network the ISDN Link is connected to.

ISDN > BRI > SwitchType: Euro

Enter the BRI numbers according to the assigned numbers for each interface, replace xxx with your numbers::

- ISDN > BRI Interface 1 > DirectoryNumber 1 Number: xxx
- ISDN > BRI Interface 1 > DirectoryNumber 2 Number: xxx
- ISDN > BRI Interface 2 > DirectoryNumber 1 Number: xxx
- ISDN > BRI Interface 2 > DirectoryNumber 2 Number: xxx
- ISDN > BRI Interface 3 > DirectoryNumber 1 Number: xxx
- ISDN > BRI Interface 3 > DirectoryNumber 2 Number: xxx
- ISDN > BRI Interface 4 > DirectoryNumber 1 Number: xxx
- ISDN > BRI Interface 4 > DirectoryNumber 2 Number: xxx

Enable the BRI interfaces in use:

- ISDN > BRI Interface 1 > Mode: On
- ISDN > BRI Interface 2 > Mode: On
- ISDN > BRI Interface 3 > Mode: On
- ISDN > BRI Interface 4 > Mode: On

Check the status after configuration

Go to *Configuration > Peripherals* and check the ISDN status information to confirm there are no errors before proceeding. If any errors, or if the power LED is red, please check your configuration.

The first screenshot shows the 'H320' configuration page. The 'NetType' dropdown menu is open, showing options: BRI, PRI, External, and G703. 'BRI' is selected.

The second screenshot shows the 'ISDN > BRI' configuration page. The 'SwitchType' dropdown menu is open, showing options: Ni, ATT, Euro, Japan, TTRG, Australia, and FETEX. 'Euro' is selected.

The third screenshot shows the 'ISDN > BRI > Interface [1..4]' configuration page. The 'Interface 1' section has 'DirectoryNumber 1 Number' set to 8001, 'DirectoryNumber 2 Number' set to 8002, and 'Mode' set to 'On'. The 'Interface 2' section has 'DirectoryNumber 1 Number' set to 8003 and 'DirectoryNumber 2 Number' set to 8004.

Navigate to H320 > General Settings > NetType.

Set the H320 Net Type:

- BRI

Click the *Save* button.

Navigate to ISDN > BRI > SwitchType.

Set the ISDN BRI Switch Type:

- Euro

Click the *Save* button.

Navigate to ISDN > BRI > Interface [1..4].

Enter the BRI numbers according to the assigned numbers for each interface, replace xxx with your numbers::

- ISDN > BRI Interface [1..4] > DirectoryNumber [1..2] Number: xxx

Enable the BRI interfaces in use:

- ISDN > BRI Interface [1..4] > Mode: On

Click the *Save* buttons.

Configuration examples

Use the search option on the page to find the parameters, or choose from the list of menus to the left and then navigate to the parameters in the right pane.

Example with support for External Network

Set the net type:

H320 > General Settings > NetType: External

Set the call control protocol:

ExternalNetwork > Interface 1 > CallControl: RS366

Set the clocking mode:

ExternalNetwork > Interface 1 > Clocking: Dual

If using RS530, set the DTRPulse to On; else set to Off:

ExternalNetwork > Interface 1 > DtrPulse: On

Check the status after configuration

Go to *Configuration > Peripherals* and check the ISDN status information to confirm there are no errors before proceeding. If any errors, or if the power LED is red, please check your configuration.

The figure consists of three screenshots of the Cisco TelePresence configuration interface, arranged vertically. Each screenshot shows a different configuration step for the H320 and ExternalNetwork components.

- Top Screenshot:** Shows the 'H320' configuration page. The 'NetType' dropdown menu is open, with 'External' selected. Other settings include 'DefaultCall Restrict' (Off), 'Encryption' (BestEffort), 'Bonding' (On), and 'Timer' (Normal).
- Middle Screenshot:** Shows the 'ExternalNetwork Interface 1' configuration page. The 'CallControl' dropdown menu is open, with 'RS366' selected. Other settings include 'Clocking' (Dual) and 'DtrPulse' (On).
- Bottom Screenshot:** Shows the 'ExternalNetwork Interface 1' configuration page. The 'DtrPulse' dropdown menu is open, with 'On' selected. Other settings include 'CallControl' (RS366) and 'Clocking' (Dual).

Navigation instructions for each step:

- Navigate to H320 > General Settings > NetType.
- Set the H320 Net Type:
 - External
 Click the *Save* button.
- Navigate to ExternalNetwork > Interface 1.
- Set the call control protocol:
 - CallControl: RS366
- Set the clocking:
 - Clocking: Dual
- Set the DTR pulse:
 - DTRPulse: On/Off
 Click the *Save* buttons.

Configuring the TelePresence endpoint for ISDN

When paired to ISDN Link, the default call settings for the TelePresence endpoint can be configured for ISDN (H320), or you can set the call protocol and call rate each time you make a call.

Setting the default call protocol to H320

Configuring the default call settings to ISDN (H320):

1. Open a web browser on your computer, enter the address (IP address or host name) of the TelePresence endpoint in the address bar, and login.
 - Navigate to *Configuration > System configuration > Conference 1 > DefaultCall* and set the *Protocol* to **H320**.
 - Click the *Save* button.

Setting the call protocol to H320 by each call

- If using a TelePresence Touch device, see: “[Making a call using the Touch controller](#)” on page 19.
- If using a TelePresence Remote Control, see: “[Making a call using the remote control](#)” on page 20.
- If calling from the TelePresence endpoint’s web interface, see: “[Making a call using the web interface of the endpoint](#)” on page 21.

Making a call using the Touch controller

If your TelePresence endpoint has a Touch controller see the dialing example on this page.

About the ISDN number

- The *ISDN number* is the number to the far end endpoint (for example an MXP codec).

Replace the number used in the example (8000) with the number you want to call.

About restricted calls

If using the *ISDN Restrict* option, choose the *Restrict* in the Call settings menu.

The image shows a sequence of six screenshots illustrating the steps to make an ISDN call on a Cisco TelePresence endpoint. Each screenshot is annotated with a circled number and an arrow pointing to the specific UI element being interacted with.

- Step 1:** The user enters the ISDN number '8000' into the dial pad.
- Step 2:** The user taps the right arrow button to open the call dialog.
- Step 3:** The user taps the 'Call settings' button to open the ISDN call settings menu.
- Step 4:** The user moves the call protocol slider and chooses 'ISDN'.
- Step 5:** The user moves the bandwidth slider to set the appropriate call rate, choosing '64 kbps'.
- Step 6:** The user taps the green 'CALL' button to make the call.

How to make the call

Touch the panel gently to wake up the system.

1. Tap *DialPad* or *Contacts* and enter the *ISDN number* you want to call.

If the default call protocol is set to ISDN (H320), proceed to *Step 6*, else proceed to *Step 2*.

2. Tap the *right arrow* button to open the call dialog.
3. Tap *Call settings* button to open the ISDN call settings menu.
4. Move the call protocol slider and choose *ISDN*.
5. Move the bandwidth slider to set the appropriate *call rate*, or if dialing a telephone number, use the slider to choose *Audio Only*.
6. Tap the green *Call* button to make the call.

Connecting the call may take up to 30 seconds.

Making a call using the remote control

If your TelePresence endpoint has a remote control see the dialing example on this page.

About the ISDN number

- The *ISDN number* is the number to the far end endpoint (for example an MXP codec).

Replace the number used in the example (8000) with the number you want to call.

About restricted calls

If using the *Restrict* option, choose the *ISDN Restrict* in the Call settings menu.

How to make the call

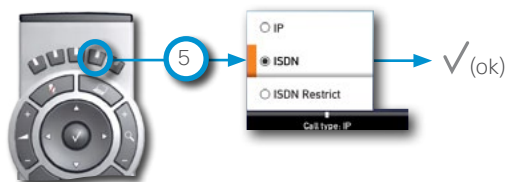
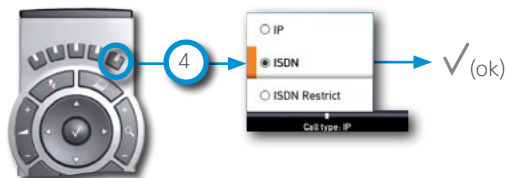
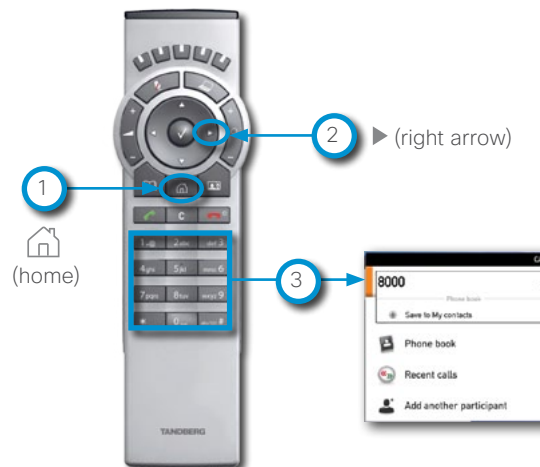
Press any button on the remote control to wake up the system.

1. Press  (home) button to open the *Home* menu.


2. Press  (right arrow) to open the *Call* menu.

3. Use the numeric pad and enter the *ISDN number* you want to call.

If the default call protocol is set to ISDN (H320), proceed to *Step 6*, else proceed to *Step 4*.




4. Press the fifth soft button to display the *Call Type* menu. Use the arrow keys to navigate and choose *ISDN*.

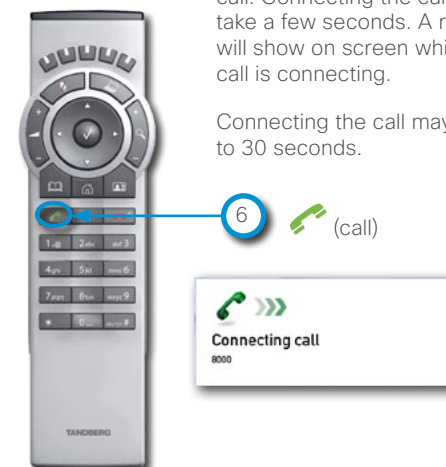
Press  (ok) to confirm your selection.

5. Press the fourth soft button to display the *Call Rate* menu. Use the arrow keys to navigate and choose the *call rate*. If dialing a telephone number, choose *Audio Only*.

Press  (ok) to confirm your selection.

6. Press  (call) to connect the call. Connecting the call may take a few seconds. A message will show on screen while the call is connecting.

Connecting the call may take up to 30 seconds.



Making a call using the web interface of the endpoint

When the ISDN Link is used in automatic pairing mode you can make a call from the TelePresence system's web interface.

About ISDN number

- The *ISDN number* is the number to the far end endpoint (for example an MXP codec).

Replace the number used in the example (8000) with the number you want to call.

About restricted calls

If using the *ISDN Restrict* option, choose the *ISDN Restrict* in the Call settings menu.

How to make the call

Open a web browser on your computer, enter the address (IP address or host name) of the TelePresence endpoint in the address bar, and login.

- Navigate to *Call Control > Call Control > Contacts*
- Enter the *ISDN number* you want to call.
If the default call protocol is set to ISDN (H320), proceed to *Step 5*, else proceed to *Step 3*.
- Click *Show call settings* and set the appropriate *call rate*.
If dialing a telephone number choose *Audio Only* from the drop down menu.
- Set the call protocol to H320.
- Click the green *Call* button to make the call.
Connecting the call may take up to 30 seconds.

Making a call using the command line interface on the endpoint

In order to make a call from the command line interface on the TelePresence endpoint, see the dialing examples on this page.

About <number>

The <number> is the number to the far end endpoint (for example an MXP codec).

Please notice that when dialing an ISDN network destination which requires sub-addressing, the sub-address number is provided in the following format:

`<number>*<subaddress>`

Replace the number used in the example (8000) with the number you want to call.

About 2xh221

If using 2xh221 the isdn number must be extended with a second number "`<1st-number>**<2nd-number>`".

Dialing on the NET interface

When using the NET (External) interface providing a number may not be required.

Furthermore, when using the NET interface, the <number> may consist of digits, * and #. In the rare situation that a # is required in the number, the # character must be encoded as %23. So to dial 1234#* on the NET interface, <number> must be set to 1234%23*.

Making a call when in automatic pairing mode

NOTE: It is not required to specify the parameter `Protocol:H320` if the default protocol for the endpoint is set to H320.

Simple dialing

`xCommand Dial Protocol:H320 Number:<number>`

Example: `xCommand Dial Protocol:H320 Number:8000`

Dialing with a non-default callrate

`xCommand Dial Protocol:H320 Number:<number> CallRate:1920`

Example: `xCommand Dial Protocol:H320 Number:8000 CallRate:1920`

Dialing in restricted networks

`xCommand Dial Protocol:H320 Number:<number>;x-h320restrict=true`

Example: `xCommand Dial Protocol:H320 Number:8000;x-h320restrict=true`

NOTE: The ISDN Link can be configured whether to use restricted calltype as default or not. If set to use restricted by default, then unrestricted calls can be made by using "`x-h320restrict=false`" (ie "`x-h320restrict=true`" is not required to make restricted calls).

Dialing a phone call (an audio only call)

`xCommand Dial Protocol:H320 Number:<number> CallType:Audio`

Example: `xCommand Dial Protocol:H320 Number:8000 CallType:Audio`

Making a call when in manual pairing mode

See the [ISDN Link API Reference Guide](#) for information about manual pairing mode.

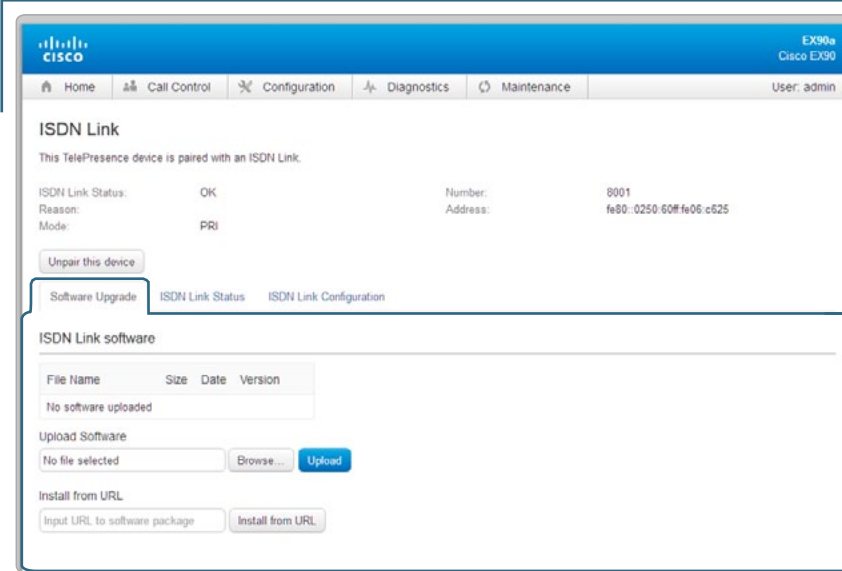
SOFTWARE UPGRADE

The software upgrade menu

When the ISDN Link is used in automatic pairing mode you can upgrade the ISDN Link software from the TelePresence system's web interface.

To access the page:

1. Open a web browser on your computer and enter the address (IP address or host name) of the TelePresence endpoint in the address bar.
2. From the top menu, go to *Configuration > Peripherals*, and on the Peripherals page click the Manage ISDN Link button.



The ISDN Link can be managed from the TelePresence endpoint's web interface.

Software Upgrade

- Software upload overview
- Install software from file
- Install software from URL

Upgrading the software

Contact your system administrator if you have questions about which software version to use.

For a complete overview of the news and changes, we recommend reading the Software Release Notes.

Go to: ► http://www.cisco.com/en/US/products/ps12504/prod_release_notes_list.html

NOTE: If upgrading from software version IL1.0 to IL1.1, see the section: “Software upgrade from IL1.0 to IL1.1” on page 78.

Installing the software from a file

1. Download the software from the Cisco web site to your computer.
2. Upload the software to the ISDN Link through the TelePresence endpoint’s web interface.
3. Install the new software.

For software download, go to ► <http://www.cisco.com/cisco/web/support/index.html>.

Installing the software from an URL

If you have an URL for the software installation, go to the Software upgrade page, paste the URL into the text field and click the Install from URL button.

The screenshot shows the Cisco TelePresence ISDN Link web interface. The top navigation bar includes Home, Call Control, Configuration, Diagnostics, and Maintenance. The main content area is titled "ISDN Link" and shows the status of the ISDN Link (OK) and its configuration (Number: 8001, Address: fe80:0250:60ff:fe06:c625). Below this, there are tabs for Software Upgrade, ISDN Link Status, and ISDN Link Configuration. The "ISDN Link software" section contains a table for uploaded software (currently empty), an "Upload Software" section with a "Browse" button and an "Upload" button, and an "Install from URL" section with an input field and an "Install from URL" button. Callout boxes on the right provide instructions for installing software from a file and from a URL.

ISDN Link software

When new software has been uploaded to the ISDN Link the file name, size, date and version is listed in the *Uploaded ISDN Link software* table.

Installing the software from a file

First download the software to your computer, then go to the Software upgrade page:

1. Click the Select file button and browse to locate the file.
2. Click the Upload button to upload the software file.
3. Click the Install button to install the software package, or click the Delete button to delete the file.

Installing the software from an URL

If you have an URL for the software installation:

1. Copy and paste the URL into the text field
2. Click the Install from URL button.

STATUS INFORMATION

Monitoring ISDN Link status

When the ISDN Link is used in automatic pairing mode you can check the ISDN Link status information from the TelePresence system's web interface.

To access the page:

1. Open a web browser on your computer and enter the address (IP address or host name) of the TelePresence endpoint in the address bar.
2. From the top menu, go to *Configuration > Peripherals*.
3. Click the Manage ISDN Link button.

ISDN Link Status

In the following pages you will find a description of each item found in the *ISDN Link Status* menu.

ISDN Link status
Shows the ISDN Link status.

ISDN Link status menu
Each entry in the menu is described in the following pages.

Collapse or expand the menus

Collapse all menus: Click the Collapse all button to collapse all sub menus.

Expand all menus: Click the Expand all button to expand all sub menus.

Collapse or expand a sub menu: Click the arrow to the right on the sub menu to hide or unhide the sub entries.

Descriptions of the ISDN Link status

In the following pages you will find a description of each item found in the ISDN Link Status menu.

Call status

ISDN Link operates as a gateway between a Caller and a Callee. Thus xStatus referring to "Caller" is about the calling party or the connection between the calling party and the ISDN Link. Similarly xStatus referring to "Callee" is about the called party or the connection between the ISDN Link and the called party.

xStatus Call [1..n] Status

Shows the status of a call.

- Idle:** The system is in idle status.
- Initializing:** The call is initializing.
- Accepted:** The call has been accepted.
- Active:** The call is active.
- Disconnecting:** The call is disconnecting.

xStatus Call [1..n] CallType

Shows the call type of the incoming or outgoing call.

- Video:** The call type is video.
- Audio:** The call type is audio.

xStatus Call [1..n] Duration

Shows the duration of a call (in seconds).

- Format:** Integer.

xStatus Call [1..n] Caller Status

xStatus Call [1..n] Callee Status

Shows the call status between the calling party and the ISDN Link (Caller Status) or between the ISDN Link and the called party (Callee Status).

- Idle:** The system is in idle status.
- Dialling:** The system is dialling.
- Ringing:** The system is ringing.
- Connecting:** The system is connecting.
- Connected:** The system is connected.
- Disconnecting:** The system is disconnecting.
- Unknown:** The call status is unknown.

xStatus Call [1..n] Caller Protocol

xStatus Call [1..n] Callee Protocol

Shows the call protocol being used between the calling party and the ISDN Link (Caller Protocol) or between the ISDN Link and the called party (Callee Protocol). In a command line interface, you can find the call identity by running the xStatus Call command.

- Format:** String.

xStatus Call [1..n] Caller RemoteNumber

xStatus Call [1..n] Callee RemoteNumber

Shows the number or URI of the calling party (Caller RemoteNumber) or called party (Callee RemoteNumber).

- Format:** String.

xStatus Call [1..n] Caller CallbackNumber

xStatus Call [1..n] Callee CallbackNumber

Shows the number or URI that ISDN Link shall use when calling back to the calling party (Caller CallbackNumber) or called party (Callee CallbackNumber).

- Format:** String.

xStatus Call [1..n] Caller LocalNumber

Shows the number called to reach the ISDN Link. For SIP callers this would be the number and parameters needed to reach the callee.

Format: String.

xStatus Call [1..n] Callee LocalNumber

Shows the number from which the ISDN Link is calling. This number is the callback number for the called party. For SIP callee's this would include the number and parameters to perform callback to the caller side.

Format: String.

xStatus Call [1..n] Caller TransmitCallRate

xStatus Call [1..n] Callee TransmitCallRate

Shows the transmit bandwidth used between the calling party and the ISDN Link (Caller TransmitCallRate) or between the ISDN Link and the called party (Callee TransmitCallRate). The bandwidth is in kilobits per second (kbps).

Format: Integer.

xStatus Call [1..n] Caller ReceiveCallRate

xStatus Call [1..n] Callee ReceiveCallRate

Shows the receive bandwidth used between the calling party and the ISDN Link (Caller ReceiveCallRate) or between the ISDN Link and the called party (Callee ReceiveCallRate). The bandwidth is in kilobits per second (kbps).

Format: Integer.

xStatus Call [1..n] Caller Encryption Type

xStatus Call [1..n] Callee Encryption Type

Shows the encryption type used between the calling party and the ISDN Link (Caller Encryption Type) or between the ISDN Link and the called party (Callee Encryption Type).

"None": The call is not encrypted.

"Aes-128": The encryption type for the call is AES-128.

ExternalNetwork status

xStatus ExternalNetwork Interface [1..1] Status

Shows the status of the External Network interface.

Ready: The external network is ready to relay calls.

NotReady: The external network is not ready for use, e.g. when clock is missing or the line is broken.

Off: The external network is not enabled (i.e. xConfiguration H320 NetType is not set to External).

xStatus ExternalNetwork Interface [1..1] ClockRate

Shows the clock rate (in kbps) used for synchronous communication on the external network. This clock is provided by the attached equipment.

Format: Integer.

xStatus ExternalNetwork Interface [1..1] Channel [1..n] Status

Gives information about the call progress in a channel on the external interface. The information indicates the various stages each channel goes through whilst establishing a connection. The channel status is available for the current call (when active) or the last call.

Idle: The channel is idle. This state is normally only seen if the channel has never been used.

Calling: The network has acknowledged an incoming call, but the connection is not yet established.

Answering: The network has acknowledged an outgoing call, but the connection is not yet established.

Connect: The connection is established.

Disconnecting: Waiting for the network to confirm the termination of the incoming or outgoing call.

Disconnected: The network has acknowledged the termination of the call. The channel is available for a new call.

xStatus ExternalNetwork Interface [1..1] Channel [1..n] Call [1..n] CallingNumber

Shows the number of the system initiating a call on the external network. The channel status is available for the current call (when active) or the last call.

Format: String.

xStatus ExternalNetwork Interface [1..1] Channel [1..n] Call [1..n] CauseLocation

Shows where the disconnection of a call on the external network is originated. The location codes are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element). The channel status is available for the current call (when active) or the last call.

Format: Integer.

xStatus ExternalNetwork Interface [1..1] Channel [1..n] Call [1..n] ChannelCause

Shows the reason why a call on the external network is disconnected. The cause values are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element). The channel status is available for the current call (when active) or the last call.

Some common cause values are listed below; ITU-T Q.850 contains the complete list.

- 1:** Unallocated (unassigned) number
- 2:** No route to specified transit network
- 16:** Normal call clearing
- 17:** User busy
- 18:** No user responding
- 21:** Call rejected
- 28:** Invalid number format (address incomplete)
- 29:** Facility rejected
- 31:** Normal, unspecified
- 34:** No circuit/channel available
- 41:** Temporary failure
- 58:** Bearer capability not presently available
- 65:** Bearer capability not implemented
- 69:** Requested facility not implemented
- 81:** Invalid call reference value
- 88:** Incompatible destination
- 100:** Invalid information element contents
- 102:** Recovery on timer expiry
- 127:** Interworking, unspecified
- 128-255:** Cisco specific codes

xStatus ExternalNetwork Interface [1..1] Channel [1..n] Call [1..n] Duration

Shows the duration (in seconds) of a call on the external network for the current call (when active) or the last call.

Format: Integer.

H320 status

xStatus H320 NetType

Shows which communication interface that is enabled on the ISDN Link.

BRI: The ISDN BRI interface is enabled.

PRI: The ISDN PRI interface is enabled.

External: The external network (NET) interface is enabled.

G703: For testing only.

ISDN status

xStatus ISDN PRI Interface [1..1] Status

Shows the status of the PRI interface.

Ready: The PRI interface is ready to relay calls.

NotReady: The PRI interface is not ready for use, e.g. when synchronization is missing or the line is broken.

Off: The PRI interface is not enabled (i.e. xConfiguration H320 NetType is not set to PRI).

xStatus ISDN PRI Interface [1..1] BChansFree

Shows the number of B channels (bearer channels, 64 kbps) currently available on the PRI interface.

Format: Integer between 0 and 30.

xStatus ISDN PRI Interface [1..1] BChansTotal

Shows how many B channels (bearer channels, 64 kbps) the PRI interface offers in total.

Format: Integer between 1 and 30.

xStatus ISDN PRI Interface [1..1] Layer1Status

Shows whether there are issues relating to framing information (physical layer).

Sync: The system is receiving framing information and the channels are synchronized.

Yellow: The system is receiving framing information, but the remote system is not receiving the transmitted framing information. This may be caused by a broken connector in the TX part of your PRI cable. It could also indicate a weak or noisy signal in the TX part of the PRI cable.

Red: There is no signal and thus the system receives no framing information from the remote site (this has the same effect as pulling out the PRI cable).

Blue: The network on the far side of the CSU (Channel Services Unit) is unavailable. For example, assume that a system is connected via a CSU (Channel Services Unit) as follows: System-CableA-CSU-CableB-Network. If the CSU loses framing/synchronisation from the network, e.g. due to a bad CableB, it will no longer send valid framing out on CableA towards the system. Instead it transmits "Blue Alarm". Seen from the system receiving the blue alarm, this means that the network on the far side of the CSU is unavailable.

Unknown: The system is not able to determine the layer 1 status.

xStatus ISDN PRI Interface [1..1] Channel [1..n] Type

Shows the channel type for a channel on the PRI interface. The PRI interface comprises a number of channels, each dedicated to either the primary communication or to control and signalling information.

DChannel: The channel is a data channel (D channel), which carries the control and signalling information in ISDN. The bit rate of the D channel on a PRI interface is 64 kbps.

BChannel: The channel is a bearer channel (B channel), which carries the primary video conference or speech call communication in ISDN. The bit rate of a B channel on a PRI interface is 64 kbps.

xStatus ISDN PRI Interface [1..1] Channel [1..n] Status

Gives information about the call progress in a channel on the PRI interface. The information indicates the various stages each channel goes through whilst establishing a connection.

Idle: The channel is idle. This state is normally only seen if the channel has never been used.

Calling: The network has acknowledged an incoming call, but the connection is not yet established.

Answering: The network has acknowledged an outgoing call, but the connection is not yet established.

Connect: The connection is established.

Disconnecting: Waiting for the network to confirm the termination of the incoming or outgoing call.

Disconnected: The network has acknowledged the termination of the call. The channel is available for a new call.

xStatus ISDN PRI Interface [1..1] Channel [1..n] Call [1..n] CallingNumber

Shows the number calling into the ISDN PRI interface (for an incoming call), and the number that ISDN Link is making a call to on the ISDN PRI interface (for an outgoing call).

Format: String.

xStatus ISDN PRI Interface [1..1] Channel [1..n] Call [1..n] CauseLocation

Shows where the disconnection of a call on the PRI interface is originated. . The location codes are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element).

Format: Integer.

xStatus ISDN PRI Interface [1..1] Channel [1..n] Call [1..n] ChannelCause

Shows the reason why a call on the PRI interface is disconnected. The cause values are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element).

Some common cause values are listed below; ITU-T Q.850 contains the complete list.

- 1:** Unallocated (unassigned) number
- 2:** No route to specified transit network
- 16:** Normal call clearing
- 17:** User busy
- 18:** No user responding
- 21:** Call rejected
- 28:** Invalid number format (address incomplete)
- 29:** Facility rejected
- 31:** Normal, unspecified
- 34:** No circuit/channel available
- 41:** Temporary failure
- 58:** Bearer capability not presently available
- 65:** Bearer capability not implemented
- 69:** Requested facility not implemented
- 81:** Invalid call reference value
- 88:** Incompatible destination
- 100:** Invalid information element contents
- 102:** Recovery on timer expiry
- 127:** Interworking, unspecified
- 128-255:** Cisco specific codes

xStatus ISDN PRI Interface [1..1] Channel [1..n] Call [1..n] Duration

Shows the duration (in seconds) of a call on the PRI interface.

Format: Integer.

xStatus ISDN BRI Interface [1..4] Status

Shows the status of the BRI interface.

Ready: The BRI interface is ready to relay calls.

NotReady: The BRI interface is not ready for use, e.g. when synchronization is missing or the line is broken.

Off: The BRI interface is not enabled (i.e. xConfiguration H320 NetType is not set to BRI).

xStatus ISDN BRI Interface [1..4] Layer1Alarm

Shows whether or not there are any alarms related to the physical layer, e.g. cable not properly connected to switch.

On: Layer 1 alarm.

Off: No alarm.

xStatus ISDN BRI Interface [1..4] Layer2Alarm

Shows whether there are any alarms related to the data-link layer.

On: Layer 2 alarm.

Off: No alarm.

xStatus ISDN BRI Interface [1..4] Channel [1..3] Type

Shows the channel type for a channel on a BRI interface. A BRI interface comprises two channels for the primary communication and one channel for control and signalling information.

DChannel: The channel is a data channel (D channel), which carries the control and signalling information in ISDN. The bit rate of the D channel of a BRI interface is 16 kbps.

BChannel: The channel is a bearer channel (B channel), which carries the primary video conference or speech call communication in ISDN. The bit rate of a B channel on a BRI interface is 64 kbps.

xStatus ISDN BRI Interface [1..4] Channel [1..3] Status

Gives information about the call progress in a channel on a BRI interface. The information indicates the various stages each channel goes through whilst establishing a connection.

Idle: The channel is idle. This state is normally only seen if the channel has never been used.

Calling: The network has acknowledged an incoming call, but the connection is not yet established.

Answering: The network has acknowledged an outgoing call, but the connection is not yet established.

Connect: The connection is established.

Disconnecting: Waiting for the network to confirm the termination of the incoming or outgoing call.

Disconnected: The network has acknowledged the termination of the call. The channel is available for a new call.

xStatus ISDN BRI Interface [1..4] Channel [1..3] Call [1..n] CallingNumber

Shows the number calling into the ISDN BRI interface (for an incoming call), and the number that ISDN Link is making a call to on the ISDN BRI interface (for an outgoing call).

Format: String.

xStatus ISDN BRI Interface [1..4] Channel [1..3] Call [1..n] CauseLocation

Shows where the disconnection of a call on the BRI interface is originated. . The location codes are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element).

Format: Integer.

xStatus ISDN BRI Interface [1..4] Channel [1..3] Call [1..n] ChannelCause

Shows the reason why a call on the BRI interface is disconnected. The cause values are specified in ITU-T Recommendation Q.850 (the Q.931 Cause information element).

Some common cause values are listed below; ITU-T Q.850 contains the complete list.

- 1: Unallocated (unassigned) number
- 2: No route to specified transit network
- 16: Normal clearing
- 17: User busy
- 18: No user responding
- 21: Call rejected
- 28: Invalid number format (address incomplete)
- 29: Facility rejected
- 31: Normal, unspecified
- 34: No circuit/channel available
- 41: Temporary failure
- 58: Bearer capability not presently available
- 65: Bearer capability not implemented
- 69: Requested facility not implemented
- 81: Invalid call reference value
- 88: Incompatible destination
- 100: Invalid information element contents
- 102: Recovery on timer expiry
- 127: Interworking, unspecified
- 128-255: Cisco specific codes

xStatus ISDN BRI Interface [1..4] Channel [1..3] Call [1..n] Duration

Shows the duration (in seconds) of a call. Applies to calls on a BRI interface channel only.

Format: Integer.

MediaChannels status

ISDN Link operates as a gateway between a Caller and a Callee. Thus xStatus referring to "Caller" is about the calling party or the connection between the calling party and the ISDN Link. Similarly xStatus referring to "Callee" is about the called party or the connection between the ISDN Link and the called party.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Encryption Status

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Encryption Status

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Encryption Status

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Encryption Status

Shows the encryption status on the incoming or outgoing audio channel, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

On: Encryption on the audio channel is enabled.

Off: Encryption on the audio channel is disabled.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Audio Protocol

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Audio Protocol

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Audio Protocol

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Audio Protocol

Shows the audio algorithm for the incoming or outgoing audio channel, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

G722: The G.722 algorithm is an ITU-T standard.

G7221: The G.722.1 algorithm is a licensed royalty-free ITU-T standard.

G711Mu: The G.711 Mu-law compression algorithm is used in North America and Japan.

G711A: The G.711 A-law compression algorithm is used in Europe and the rest of the world.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Audio Mute

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Audio Mute

Audio mute status of incoming audio on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

True: Audio is muted.

False: Audio is not muted.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Audio Channels

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Audio Channels

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Audio Channels

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Audio Channels

Shows the number of incoming or outgoing audio channels, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTP Local IpAddress

Shows the local IP address of the Real-time Transport Protocol (RTP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTP Local Port

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTP Local Port

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTP Local Port

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTP Local Port

Shows the local UDP port number of the Real-time Transport Protocol (RTP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTP Remote IpAddress

xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTP Remote IpAddress

xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTP Remote IpAddress

xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTP Remote IpAddress

Shows the remote IP address of the Real-time Transport Protocol (RTP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTP Remote Port

Shows the remote UDP port number of the Real-time Transport Protocol (RTP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTCP Local IpAddress

Shows the local IP address of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTCP Local Port

Shows the local UDP port number of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTCP Remote IpAddress

Shows the remote IP address of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingAudioChannel [1..n] Transport RCTP Remote Port
xStatus MediaChannels Call [1..n] Caller OutgoingAudioChannel [1..n] Transport RTCP Remote Port
xStatus MediaChannels Call [1..n] Callee IncomingAudioChannel [1..n] Transport RTCP Remote Port
xStatus MediaChannels Call [1..n] Callee OutgoingAudioChannel [1..n] Transport RTCP Remote Port

Shows the remote UDP port number of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing audio, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Encryption Status
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Encryption Status
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Encryption Status
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Encryption Status

Shows the encryption status on the incoming or outgoing video channel, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

On: Encryption on the video channel is enabled.

Off: Encryption on the video channel is disabled.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Encryption Type
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Encryption Type

Shows the encryption type used between the calling party and the ISDN Link (Caller Encryption Type) or between the ISDN Link and the called party (Callee Encryption Type).

"None": The call is not encrypted.

"Aes-128": The encryption type for the call is AES-128.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] ChannelRole

xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] ChannelRole

xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] ChannelRole

xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] ChannelRole

Shows whether the incoming or outgoing channel is the main video channel, presentation channel or legacy (Y/Composite and C connectors). The status is for the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee)

Main: Main video on video channel.

Presentation: Presentation on the video channel.

Legacy: Legacy (Composite) on the video channel.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Video Protocol

xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Video Protocol

xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Video Protocol

xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Video Protocol

Shows the video algorithm for the incoming or outgoing video channel, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

H264: The H.264 algorithm is an ITU-T standard for video compression.

H263pp: The H.263pp algorithm is an ITU-T standard for video compression.

H263: The H.263 algorithm is an ITU-T standard for video compression.

H261: The H.261 algorithm is an ITU-T standard for video compression.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTP Local IpAddress

xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTP Local IpAddress

Shows the local IP address of the Real-time Transport Protocol (RTP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTP Local Port
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTP Local Port
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTP Local Port
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTP Local Port

Shows the local UDP port number of the Real-time Transport Protocol (RTP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTP Remote IpAddress
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTP Remote IpAddress

Shows the remote IP address of the Real-time Transport Protocol (RTP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTP Remote Port
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTP Remote Port

Shows the remote UDP port number of the Real-time Transport Protocol (RTP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTCP Local IpAddress
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTCP Local IpAddress

Shows the local IP address of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTCP Local Port
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTCP Local Port

Shows the local UDP port number of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTCP Remote IpAddress
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTCP Remote IpAddress

Shows the remote IP address of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: String.

xStatus MediaChannels Call [1..n] Caller IncomingVideoChannel [1..n] Transport RCTP Remote Port
xStatus MediaChannels Call [1..n] Caller OutgoingVideoChannel [1..n] Transport RTCP Remote Port
xStatus MediaChannels Call [1..n] Callee IncomingVideoChannel [1..n] Transport RTCP Remote Port
xStatus MediaChannels Call [1..n] Callee OutgoingVideoChannel [1..n] Transport RTCP Remote Port

Shows the remote UDP port number of the Real-time Transport Control Protocol (RTCP) port for the incoming or outgoing video, on the connection between the ISDN Link and the calling party (Caller) or between the ISDN Link and the called party (Callee).

Format: Integer.

Network status

xStatus Network [1..1] Ethernet MacAddress

Shows the MAC (Media Access Control) address for the ISDN Link.

Format: String.

xStatus Network [1..1] Ethernet Link Network

Shows the Ethernet link status for the LAN port on ISDN Link. This port is used for connecting the ISDN Link to the network (LAN).

"No LAN": There is no connection.

"10half": The Ethernet speed is 10 Mbps half-duplex.

"10full": The Ethernet speed is 10 Mbps full-duplex.

"100half": The Ethernet speed is 100 Mbps half-duplex.

"100full": The Ethernet speed is 100 Mbps full-duplex.

"1000full": The Ethernet speed is 1 Gbps full-duplex.

xStatus Network [1..1] Ethernet Link Endpoint

Shows the Ethernet link status for the Endpoint port on ISDN Link. This port is used for connecting the ISDN Link to a TelePresence endpoint.

"No LAN": There is no connection.

"10half": The Ethernet speed is 10 Mbps half-duplex.

"10full": The Ethernet speed is 10 Mbps full-duplex.

"100half": The Ethernet speed is 100 Mbps half-duplex.

"100full": The Ethernet speed is 100 Mbps full-duplex.

"1000full": The Ethernet speed is 1 Gbps full-duplex.

xStatus Network [1..1] IPv4 Address

Shows the IPv4 address that uniquely identifies this system.

Format: String.

xStatus Network [1..1] IPv4 SubnetMask

Shows the subnet mask which determines which subnet an IPv4 address belongs to.

Format: String.

xStatus Network [1..1] IPv4 Gateway

Shows the address of the IPv4 gateway.

Format: String.

xStatus Network [1..1] IPv4 DNS Domain Name

Shows the domain name.

Format: String.

xStatus Network [1..1] IPv4 DNS Server [1..3] Address

Shows the IP address of the DNS server.

Format: String.

xStatus Network [1..1] IPv6 Address

Shows the IPv6 address that uniquely identifies this system.

Format: String.

xStatus Network [1..1] IPv6 Gateway

Shows the address of the IPv6 gateway.

Format: String.

xStatus Network [1..1] MTU

Shows the MTU (Maximum Transmission Unit) size for the network.

Format: Integer.

xStatus Network [1..1] VLAN Voice VlanId

The feedback will show the VLAN Voice ID, or Off if the VLAN Voice Mode is not enabled.

"Off": VLAN Voice mode is not enabled.

"1".."4094": Displays the VLAN Voice ID when VLAN is enabled.

xStatus Network [1..1] VLAN Native VlanId

Identifies the VLAN associated with any untagged traffic between the switch and the endpoint. For more information see documentation for the IEEE 802.1Q protocol.

xStatus Network [1..1] CDP Platform

Returns the hardware platform name of the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP Version

Returns information about the software release version running on the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP Capabilities

Describes the functional capability for the switch that ISDN Link is connected to (if the network switch supports CDP) in form of a device type. See documentation for CDP (Cisco Discovery Protocol) protocol on our web site for more information.

Format: String.

xStatus Network [1..1] CDP DeviceId

Identifies the name of the switch that ISDN Link is connected to (if the network switch supports CDP) in the form of a character string.

Format: String.

xStatus Network [1..1] CDP PortID

Identification that the switch uses for the port the ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP Duplex

Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP VTPMgmtDomain

Returns information about the VTP management domain name-string as configured in the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP Address

Returns the first network address of both the receiving and the sending devices (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP PrimaryMgmtAddress

Returns the management address used to configure and monitor the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP SysName

Returns the SysName as configured in the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP SysObjectID

Returns the SysObjectID as configured in the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

xStatus Network [1..1] CDP VoIPApplianceVlanID

Returns the VoIPApplianceVlanID as configured in the switch that ISDN Link is connected to (if the network switch supports CDP).

Format: String.

SIP status

xStatus SIP Profile [1..1] Proxy [1..1] Status

Shows the status of the communication between the endpoint and the SIP Proxy server.

Active: The communication between the endpoint and the SIP Proxy is active.

DNSFailed: The attempt to establish communication to the DNS server failed.

Off: There is no communication between the endpoint and the SIP Proxy.

Timeout: The attempt to establish communication to the SIP Proxy timed out.

UnableTCP: The system is unable to use TCP as the transport method.

UnableTLS: The system is unable to use TLS as the transport method.

Unknown: The status of the communication is not known.

xStatus SIP Profile [1..1] Proxy [1..1] Address

Shows the address of the SIP Proxy that the system communicates with.

Format: String.

xStatus SIP Profile [1..1] Secure

Shows the encryption status of the signalling with the SIP Proxy server.

True: Encryption is enabled.

False: Encryption is disabled.

xStatus SIP Profile [1..1] Verified

The result returned for this command will always be False.

xStatus SIP Profile [1..1] Authentication

Shows which authentication mechanism is used when registering to the SIP Proxy Server.

Digest: Uses the Digest access authentication method, as specified by RFC 2069.

NTLM: Uses the NTLM authentication method, which is a Microsoft authentication protocol.

Off: No authentication mechanism is used.

xStatus SIP Profile [1..1] Registration [1..n] Status

Shows the status of the registration to the SIP Proxy Server.

Deregister: The system is in the process of de-registering to the SIP Proxy.

Failed: The system failed to register to the SIP Proxy.

Inactive: The system is not registered to any SIP Proxy.

Registered: The system is registered to the SIP Proxy.

Registering: The system is in the process of registering to the SIP Proxy.

xStatus SIP Profile [1..1] Registration [1..n] Reason

Shows a message to explain the reason why the SIP registration failed.

Format: String.

xStatus SIP Profile [1..1] Registration [1..n] URI

Shows the URI used for registration to the SIP Proxy server.

Format: String.

SystemUnit status

xStatus SystemUnit ProductType

Shows the product type.

Format: String.

xStatus SystemUnit Uptime

Shows the number of seconds since the last restart of the system.

Format: Integer.

xStatus SystemUnit Software Version

Shows the software version installed on the system.

Format: String.

xStatus SystemUnit Software Name

Shows the name of the software that is installed on the system.

Format: String.

xStatus SystemUnit Software ReleaseDate

Shows the release date of the software installed on the system.

Format: String.

xStatus SystemUnit Software BootStage1

Shows the version of boot stage 1 loader.

Format: String.

xStatus SystemUnit Software BootStage2

Shows the version of the boot stage 2 loader.

Format: String.

xStatus SystemUnit Software MaxVideoCalls

Shows the maximum number of simultaneous video calls that is supported by the software installed. May vary depending of the selected network interface type and other configuration.

Format: Integer.

xStatus SystemUnit Software MaxAudioCalls

Shows the maximum number of simultaneous audio calls that is supported by the software installed.

Format: Integer.

xStatus SystemUnit Hardware Module SerialNumber

Shows the serial number of the system.

Format: String.

xStatus SystemUnit Hardware Module Identifier

Shows the revision of the system.

Format: String.

xStatus SystemUnit Hardware MainBoard SerialNumber

Shows the serial number of the main board in the system.

Format: String.

xStatus SystemUnit Hardware MainBoard Identifier

Shows the revision of the main board in the system.

Format: String.

xStatus SystemUnit Hardware MainBoard CPLDFirmware

Shows the version of installed CPLD firmware.

Format: String.

xStatus SystemUnit Hardware MainBoard Temperature

Shows the temperature (in degrees Celsius) of the system's main board.

Format: String.

xStatus SystemUnit State Status

Shows the system state, i.e. whether there are any errors or warnings issued.

Initializing: The system is initializing and not yet ready for use.

OK: The system is ready for use.

OKWithWarning: The system can be used for making calls, but there are warnings issued that might influence its behavior.

Error: The system is in an erroneous state and cannot be used for making calls.

xStatus SystemUnit State StatusCode

Shows the type of error or warning that is issued for the system (if any).

OK: The system is ready for use.

EthLinkDown: There is no Ethernet connection, and thus the ISDN Link cannot be used.

BRIWarning: A warning is issued for the BRI interface.

BRIError: There is an error on the BRI interface.

PRIError: There is an error on the PRI interface.

ExtNetError: There is an error on the external network interface (NET).

Initializing: The system is initializing and not yet ready for use.

xStatus SystemUnit State StatusText

Textual description of the system state, e.g. type of alarm if in an erroneous state.

Format: String.

xStatus SystemUnit State H320Number

Shows the number that can be used to dial in on the ISDN BRI/PRI interface in order to reach this ISDN Link and subsequently the endpoint associated with the ISDN Link. This requires that numbers have been assigned to the BRI or PRI interfaces respectively.

Not applicable when using the external network (NET) interface.

Format: String.

xStatus SystemUnit State MaxNumberOfCalls

Shows the maximum number of simultaneous calls supported, with the current configuration. The normal value is 3, with the following exceptions:

- 1) When using the External (V.35) interface, only one call is possible.
- 2) When H.320 side encryption is enabled, maximum 2 calls are supported on the PRI interface.

Format: Integer between 1 and 3.

xStatus SystemUnit State NumberOfActiveCalls

Shows the number of active calls.

Format: Integer between 0 and 3.

xStatus SystemUnit State NumberOfSuspendedCalls

Shows the number of suspended calls.

Format: Integer between 0 and 3.

xStatus SystemUnit State NumberOfInProgressCalls

Shows the number of calls in progress.

Format: Integer between 0 and 3.

SYSTEM SETTINGS

The ISDN Link Configuration menu

When the ISDN Link is used in automatic pairing mode you can configure the ISDN Link system settings from the TelePresence system's web interface.

To access the page:

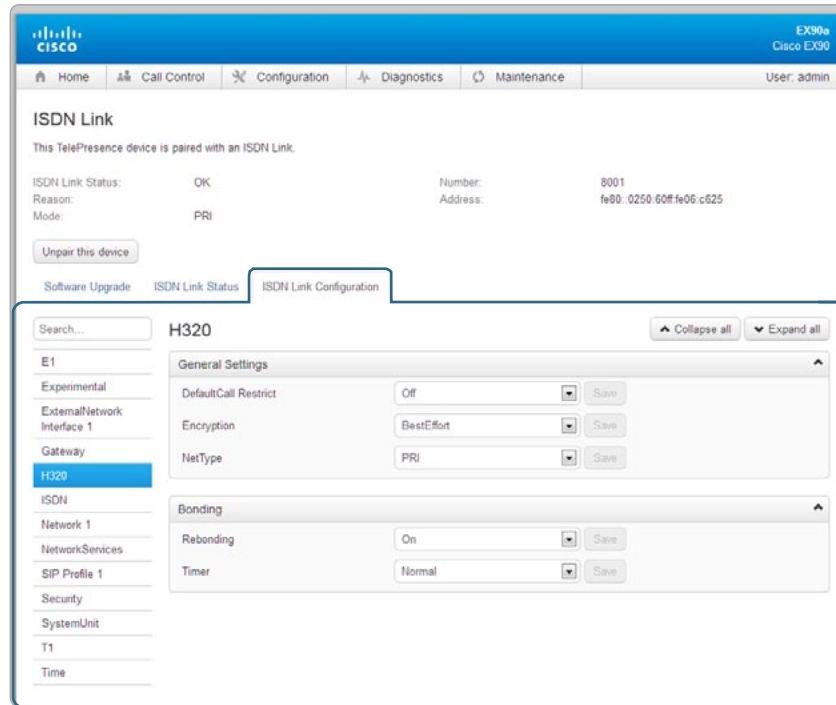
1. Open a web browser on your computer and enter the address (IP address or host name) of the TelePresence endpoint in the address bar.
2. From the top menu, go to *Configuration > Peripherals*, and on the Peripherals page click the Manage ISDN Link button.

Description of the system settings

In the following pages you will find a description of each item found in the ISDN Link Configuration menu.

About user roles

A user can have different levels of access rights (ADMIN, USER, AUDIT). To change settings for the ISDN Link the user must have ADMIN rights. Read more about user roles in the Administrator Guide for your video system.



ISDN Link Configuration

Each entry in the menu is described in the following pages.

Collapse or expand the menus

Collapse menus: Click the Collapse all button to collapse all sub menus.

Expand menus: Click the Expand all button to expand all sub menus.

Collapse or expand a sub menu: Click the arrow to the right on the sub menu to hide or unhide the sub entries.

Changing system settings

The value space for a setting is specified either as a drop down list or with explanatory text following a text input field.

Drop down list: Click the down arrow to open the drop down list. Then select the preferred value.

Text input field: Enter a new value in the field and press ok to save the new value.

Descriptions of the ISDN Link configurations

In the following pages you will find a description of each item found in the ISDN Link Configuration menu.

E1 configuration

E1 Interface [1..1] CRC4

E1 CRC-4 (Cyclic Redundancy Check 4-bit) is used for most E1-PRI configurations.

Value space: <Off/On>

Off: Some manufactures do not support this feature. By setting E1 CRC4 to Off this functionality will be disabled.

On: When set to On, the Cyclic Redundancy Check is enabled. The default value is On.

ExternalNetwork configuration

ExternalNetwork Interface [1..1] CallControl

Configure the dialling sheme which is compatible with the external equipment.

Value space: <Manual/RS366/RS366AdtranIMUX/RS366CustomIMUX/LeasedLine>

Manual: Select Manual used when no handshake signals are available and the external equipment requires a constantly connected line.

RS366: This is the only dialling protocol supported and would normally be used together with Dual network clocking when the external equipment uses RS366 ports.

RS366AdtranIMUX: This setting offers extra usability when dialling RS366 via an ADTRAN IMUX. This dialling scheme will map the call type and bandwidth selection to ADTRAN IMUX specific suffixes to the dialled number. Should only be used when connected to an ADTRAN IMUX. The Adtran IMUX uses the following suffixes: <Number>#C#R.

#C = Call Type

#2 = audio (telephony)

#3 = 56kbps (restricted)

#4 = 64kbps (unrestricted)

#R = Channel Rate

#0 = 2x221 (2x56/64kbps)

#n, where n is one of [1, 2, 3, 4, 5, 6, 8, 12, 18, 23, 30]; ie n*64kbps

RS366CustomIMUX: Uses a custom prefix/suffix table which describes the available bandwidths. The system administrator shall be able to specify the IMUX prefix/suffix table for the following bandwidths (kbps): 64, 64 Restrict, 128, 128 Restrict, 192, 192 Restrict, 256, 256 Restrict, 320, 320 Restrict, 384, 384 Restrict, 512, 512 Restrict, 768, 768 Restrict, 1152, 1152 Restrict, 1472, 1472 Restrict, 1920.

LeasedLine: Leased Line is a non-dialling protocol and should be used when two codecs are connected in a point-to-point connection. Use Leased Line when the handshaking signals DTR and CD are available. DTR and CD correspond to the X.21 network's C and I signals.

ExternalNetwork Interface [1..1] Clocking

Configure the clocking signal which is compatible with the external equipment.

Value space: <Dual/Single>

Dual: (RS449/V35 Compatible) Use this setting when the external equipment provides two clock signals, one for transmit and one for receive. The difference between RS449 and V35 lies solely in the cable.

Single: (X21 Compatible) Use this setting when the external equipment provides a common clock signal for both transmit and receive.

ExternalNetwork Interface [1..1] DtrPulse

Configures the DTR signal on the External Network port (Net).

Value space: <Off/On>

Off: The DTR pulse will stay low.

On: The DTR signal will give a low pulse lasting for 5 seconds.

ExternalNetwork Interface [1..1] CustomIMUX bw64 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw64 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw64R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw64R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw128 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw128 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw128R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw128R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw192 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw192 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw192R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw192R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw256 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw256 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw256R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw256R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw320 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw320 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw320R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw320R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw384 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw384 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw384R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw384R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw512 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw512 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw512R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw512R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw768 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw768 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw768R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw768R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1152 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1152 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1152R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1152R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1472 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth..

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1472 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1472R Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1472R Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this restricted bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1920 Prefix

Defines the prefix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

ExternalNetwork Interface [1..1] CustomIMUX bw1920 Suffix

Defines the suffix to be used with the RS366 Custom IMUX at this bandwidth.

Value space: <S: 0, 12>

Format: String with a maximum of 12 characters.

Gateway configuration

Gateway PairingMode

Configure the ISDN Link to operate in automatic or manual pairing mode. Pairing is a process in which the ISDN Link and endpoint communicate with each other in order to establish a connection. When pairing is completed the ISDN Link is dedicated to the endpoint it has been paired with. The automatic pairing mode provides an improved user experience, but requires that the endpoint supports this feature.

Value space: <Auto/Manual>

Auto: Set to Auto (default) to enable the ISDN Link to be discovered by a TelePresence endpoint. In automatic pairing mode the ISDN Link can be managed from the TelePresence endpoint's web interface.

Manual: In manual pairing mode the ISDN Link is managed from a command line interface through the serial interface, or over the network through SSH.

Gateway SIP PeerHost

NOTE: Only applicable when in manual pairing mode.

Set the IP address of the peer SIP codec using the ISDN link. Only one SIP codec can use the ISDN link, and it must be on the same subnet as the ISDN link. This IP address must correspond to the IP address type (IPv4 or IPv6) that the codec is configured to use for SIP calls.

The address is used for:

- 1) Verification of the SIP remote media transport addresses (if there is a mismatch, the call will be rejected/disconnected).
- 2) System status monitoring, indicating alarm etc if specified codec is not reachable.
- 3) If not SIP (VCS = Video Communication Server) registered, this address is used to call the SIP codec for incoming H.320 side calls.

Value space: <S: 0, 64>

Format: Compact string with a maximum of 64 characters.

Gateway SIP PeerUri

NOTE: Only applicable when in manual pairing mode.

Set the address be used to reach the peer codec for incoming H.320 side calls when SIP (VCS = Video Communication Server) registered mode is used. It should hold the same setting as the peer codec uses to register itself on the VCS server. If SIP registered mode is not used, this setting is not used.

Value space: <S: 0, 256>

Format: Compact string with a maximum of 256 characters.

H320 configuration

H320 DefaultCall Restrict

A restricted call uses 56 kbps channels rather than the default unrestricted 64 kbps channels. Some older networks (primarily in the USA) do not support 64 kbps channels and require the use of restricted 56 kbps calls. By default, the system will dial an unrestricted call and downspeed to 56 kbps if necessary. Restricted mode can be selected when making a call.

Value space: <Off/On>

Off: Set to Off to disable restricted calls by default.

On: Set to On to force restricted (56 kbps) calls by default.

H320 Encryption

Set the encryption mode for the communication between the endpoint and the H.320 side interface (PRI/BRI/NET). The endpoint encryption status does ONLY reflect the encryption status for the SIP transport leg between the endpoint and the ISDN Link. For more details on encryption, see the "About audio and video encryption" section in the Appendices.

Value space: <Off/On/BestEffort>

Off: The system will never use encryption on H.320 side.

On: The system will always use encryption H.320 side. No audio/video media is conveyed until encryption with peer H.320 device is established.

BestEffort: The system will use encryption on H.320 side whenever possible. A call will start without encryption, and if an encryption session with peer H.320 device is established, it will switch automatically to encrypting media traffic.

H320 NetType

Defines the network type to use for H.320 calls.

Value space: <BRI/PRI/External/G703>

BRI: Select BRI for the BRI network.

PRI: Select PRI for the PRI network.

External: Select External for the external network (Net/V.35).

G703: For test purpose only.

H320 Bonding Rebonding

Rebonding is used to re-establish H.320 calls if corrupted data is received for a longer period (10 - 15 sec).

Value space: <Off/On>

Off: Some manufactures do not support this feature. By setting Rebonding to Off this functionality will be disabled.

On: Set to On to enable rebonding. The default value is On.

H320 Bonding Timer

Relaxed bonding timer is used when B channels requires additional time before they can become transparent.

Value space: <Normal/Relaxed>

Normal: The default value is Normal.

Relaxed: Relaxed bonding timing should be used with applications where the B channels use some additional time before they become transparent, like external encryption devices etc.

ISDN configuration

ISDN CliNumbPlan

Value to be used for calling party number field Plan in the ISDN setup message. If the value is set to 1, the numbering plan in the setup message will signal ISDN. This is required in the UAE (United Arab Emirates).

Value space: <0..14>

Range: Select a value between 0 and 14.

ISDN CliNumbSpec

Select if calling party numbers should be enabled. Explicitely specify Calling Party Number fields Type/Plan to be used in outgoing calls in the ISDN setup message.

Value space: <Off/On>

Off: When set to Off, default values are used.

On: When set to on, the system will use the values set by "ISDN CliNumPlan" and "ISDN CliNumbType".

ISDN CliNumbType

Value to be used for calling party number field Type. If the value is set to 2, the number type in the setup message will be set to National. This is required in the UAE (United Arab Emirates).

Value space: <0..6>

Range: Select a value between 0 and 6.

ISDN HLC

Select if HLC (Higher Level Capability) information should be included in the setup message (video calls only).

Value space: <Off/On>

Off: When set to Off, no HLC information will be sent.

On: When set to On, the system will signal the type of call i.e. video call, telephony or data. HLC must be enabled to work with some PRI networks in Italy.

ISDN MSN

The use of MSN (Multiple Subscriber Number) enables the system to attach different ISDN terminals, with different numbers, to the same physical ISDN telephone line. This service can be ordered from your telephone company.

Value space: <Off/On>

Off: When set to Off, only calls to numbers specified for the specific ISDN interfaces will be answered.

On: Set to On to enable MSN on the video system when you have subscribed to a MSN service from your telephone company.

ISDN ParallelDial

Select if the channels in bonding calls should be connected in parallel or one by one.

Value space: <Off/On>

Off: When set to Off, channels will be dialled one by one, which may increase the dialling time.

On: When set to On, channels will be dialled and connected in parallel when setting up a bonding call.

ISDN SendComplete

Select if the ISDN message should contain sending complete information.

Value space: <Off/On>

Off: If set to Off The system will not send Sending Complete.

On: If set to On the system will send the ISDN message information element Sending Complete.

ISDN SendNumber

Select if the system should send its own number to the far end.

Value space: <Off/On>

Off: When set to Off, the system will not send its own numbers to the far end. Note that the network may still send your numbers to the far end.

On: When set to On, the system will send its own numbers to the far end.

ISDN SpeechTimers

Select if speech timers should be active for ISDN Layer 3, telephony calls.

Value space: <Off/On>

Off: When set to Off, there will be no speech timers.

On: Set to On to enable speech timers (T310, T304, T301).

ISDN SubAddress

Using a sub address enables you to connect up to eight ISDN terminals to the same ISDN telephone number and line. The terminals are addressed by using different sub addresses. To call a terminal with a sub address, separate the ISDN telephone number and the sub address with a * (asterisk). Note that this service has limited access on some ISDN networks.

Value space: <S: 0, 20>

Format: String with a maximum of 20 characters.

ISDN SubAddressSend

Using a sub address enables you to connect up to eight ISDN terminals to the same ISDN telephone number and line. The terminals are addressed by using different sub addresses. To call a terminal with a sub address, separate the ISDN telephone number and the sub address with a * (asterisk). Note that this service has limited access on some ISDN networks.

Value space: <Off/On>

Off: Set to Off to disable use of sub addresses.

On: When set to on, the system will use the values set by "ISDN SubAddress".

ISDN BRI Alert

Select if the system should respond with an alert message to all incoming setup messages, or to the first incoming channel only.

Value space: <Off/On>

Off: When set to Off (default) the system will respond with an alert message only to the incoming setup message related to the initial channel. Note that if the PBX requires this signalling you will only get connected on the first incoming channel.

On: When set to On, the system will respond with an alert message to all incoming setup messages.

ISDN BRI AutoActivation

Set the auto activation mode of the BRI interface (ISDN Layer 1).

Value space: <Off/Selected/All>

Off: When set to Off, no interfaces will be activated.

Selected: When set to Selected, the system will activate the interfaces which are already on.

All: When set to All, the system will activate all interfaces regardless of status.

ISDN BRI ChanId

Select if BRI Channel ID information should be sent to the PxB.

Value space: <Off/On>

Off: When set to Off, Channel ID information is not sent. Default setting is Off.

On: When set to On, the system will signal to the PBX which BRI channels is used for the call. NOTE: This setting must be set to On, to work with an Ericsson MD110 PBX.

ISDN BRI InterfaceSearch

Selects whether to start searching for available B-channels from the highest numbered interface or from the lowest numbered interface.

Value space: <High/Low>

High: When set to High, the system will start searching for available B-channels from the highest numbered interface.

Low: When set to Low, the system will start searching for available B-channels from the lowest numbered interface.

ISDN BRI MaxDeactiveTime

Set the maximum duration for Layer 1 in de-active state before auto activation (re)starts.

Value space: <1..60>

Range: Select a value between 1 and 60 seconds.

ISDN BRI SwitchType

Select the type of BRI switch the system is connected to.

Value space: <NI/ATT/Euro/Japan/1TR6/Australia/FETEX>

NI: Select NI if the switch is a National ISDN switch type.

ATT: Select ATT if the switch is an AT&T (for the U.S.) ISDN switch type.

Euro: Select Euro if the switch is an Euro (UK and others) ISDN switch type.

Japan: Select Japan if the switch is a Japanese ISDN switch type.

1TR6: Select 1TR6 if the switch is an 1TR6 switch type.

Australia: Select Australia if the switch is an Australian ISDN switch type.

FETEX: Select FETEX if the switch is a FETEX ISDN switch type.

ISDN BRI Interface [1..4] DirectoryNumber [1..2] Number

Configure the Directory Numbers for the various BRI interfaces.

Value space: <S: 0, 24>

Format: String with a maximum of 24 characters.

ISDN BRI Interface [1..4] Mode

Select BRI interface 1 to 4, and set the BRI interface mode.

Value space: <Off/On>

Off: Set to Off to disable the selected BRI interface.

On: Set to On to enable the selected BRI interface.

ISDN BRI Interface [1..4] SPID [1..2] Number

Configure the SPID Numbers for the various BRI interfaces.

Value space: <S: 0, 20>

Format: String with a maximum of 20 characters.

ISDN PRI Alert

Select if the system should respond with an alert message to all incoming setup messages, or to the first incoming channel only.

Value space: <Off/On>

Off: When set to Off (default) the system will respond with an alert message only to the incoming setup message related to the initial channel. Note that if the PBX requires this signalling you will only get connected on the first incoming channel.

On: When set to On, the system will respond with an alert message to all incoming setup messages.

ISDN PRI ChanId

Select if PRI Channel ID information should be sent to the PBX.

Value space: <Off/On>

Off: When set to Off, Channel ID information is not sent. Default setting is Off.

On: When set to On, the system will signal to the PBX which PRI channels is used for the call. NOTE: This setting must be set to On, to work with an Ericsson MD110 PBX.

ISDN PRI InitialRestart

Select if the system should re-initialize the PRI interfaces after the system has been restarted.

Value space: <Off/On>

Off: When set to Off, the PRI interface will not be re-initialized after restart.

On: When set to On, the PRI interfaces will be re-initialized after restart of the system.

ISDN PRI L2WindowSize

Set Layer 2 window size (ISDN Layer 2).

Value space: <1..7>

Range: Select a value between 1 and 7.

ISDN PRI SwitchType

Selects the type of PRI switch the system is connected to.

Value space: <NI/ATT/Euro/Japan>

NI: Select NI if the switch is a National ISDN switch type.

ATT: Select ATT if the switch is an AT&T (for the U.S.) ISDN switch type.

Euro: Select Euro if the switch is an Euro (UK and others) ISDN switch type.

Japan: Select Japan if the switch is a Japanese ISDN switch type.

ISDN PRI Interface [1..1] HighChannel

Set the highest numbered B-channel that may be used by the system when selecting channels for outgoing calls.

Value space: <1..31>

Range: Select a value between 1 and 31.

ISDN PRI Interface [1..1] LowChannel

Set the lowest numbered B-channel that may be used by the system when selecting channels for outgoing calls.

Value space: <1..31>

Range: Select a value between 1 and 31.

ISDN PRI Interface [1..1] MaxChannels

Set the maximum number of channels the system may use at any given time.

Value space: <1..30>

Range: Select a value between 1 and 30.

ISDN PRI Interface [1..1] NumberRangeStart

If the PRI line has a range of numbers, the first number in the range should be entered in the Number Range Start field.

Value space: <S: 0, 24>

Format: String with a maximum of 24 characters.

ISDN PRI Interface [1..1] NumberRangeStop

If the PRI line has a range of numbers, the last number in the range is entered in the Number Range Stop field.

Value space: <S: 0, 24>

Format: String with a maximum of 24 characters.

ISDN PRI Interface [1..1] Search

Selects whether to start searching for available B-channels from the highest numbered channel or from the lowest numbered channel.

Value space: <High/Low>

High: When set to High, the system will start searching for available B-channels from the highest numbered channel.

Low: When set to Low, the system will start searching for available B-channels from the lowest numbered channel.

ISDN PRI NSFTelephony Mode

Configure the NSF (Network Service Facility) mode for telephony.

Value space: <Off/On>

Off: Set to Off to disable Network Service Facility for telephony.

On: Set to On, to enable Network Service Facility for telephony.

ISDN PRI NSFTelephony Number

Defines what Service Facility to use for telephony. Requires the NSFTelephony Mode set to On.

Service profiles for AT&T (ref. 1):

- NSF Service
- 0 Disable
- 1 SDN (including GSDN)
- 2 Toll Free Megacom (800)
- 3 Megacom
- 6 ACCUNET Switched Digital Service (including Switched Digital International)
- 7 Long Distance Service (including AT&T World Connect)
- 8 International Toll Free Service (I800)
- 16 AT&T MultiQuest
- 23 Call Redirection Service

Service profiles for Sprint (ref. 2):

- NSF Service
- 0 Reserved
- 1 Private
- 2 Inwatts
- 3 Outwatts
- 4 FX
- 5 TieTrunk

Service profiles for MCI (ref. 3):

- NSF Service
- 1 VNET/Vision
- 2 800
- 3 PRISM1, PRISMII, WATS
- 4 900
- 5 DAL

Value space: <0..31>

Range: Select a value between 0 and 31.

ISDN PRI NSFVideoTelephony Mode

Configure the NSF (Network Service Facility) mode for video telephony.

Value space: <0ff/0n>

Off: Set to Off, to disable Network Service Facility for video telephony.

On: Set to On, to enable Network Service Facility for video telephony.

ISDN PRI NSFVideoTelephony Number

Defines what Service Facility to use for video telephony. Requires NSFVideoTelephony Mode set to On.

Value space: <0..31>

Range: Select a value between 0 and 31.

Network configuration

Network [1..1] Assignment

Define how the system will obtain its IPv4 address and the default gateway address. This setting only applies to systems on IPv4.

Value space: <Static/DHCP>

Static: Set the network assignment to Static and configure the static IPv4 settings (IP Address, Gateway, SubnetMask).

DHCP: The systems addresses are automatically assigned by the DHCP server.

Network [1..1] IPStack

Select which internet protocols the system will support.

Value space: <IPv4/IPv6>

IPv4: IP version 4 is supported.

IPv6: IP version 6 is supported, and the IPv4 settings (IP Address, IP Subnet Mask and Gateway) will be disabled.

Network [1..1] MTU

Set the Ethernet MTU (Maximum Transmission Unit).

Value space: <576..1500>

Range: Select a value from 576 to 1500 bytes.

Network [1..1] RemoteAccess Allow

Filter IP addresses for access to ssh/HTTP/HTTPS.

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters, comma separated IP addresses or IP range.

Network [1..1] DNS Domain Name

DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is "domain.com" and the name to lookup is "MyVideoSystem", this will result in the DNS lookup "MyVideoSystem.domain.com".

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Network [1..1] DNS Server [1..3] Address

Define the network addresses for DNS servers. Up to 3 addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Network [1..1] IPv4 Address

Enter the static IPv4 network address for the system. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Only the valid IP address format is accepted. Any IP address that contains letters (192.a.2.0) or invalid IP addresses (192.0.1234.0) will be rejected.

Network [1..1] IPv4 Gateway

Define the IPv4 network gateway. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Compact string with a maximum of 64 characters.

Network [1..1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Compact string with a maximum of 64 characters.

Network [1..1] IPv6 Address

Enter the static IPv6 network address for the system. Only applicable if the Network IPv6 Assignment is set to Static.

Value space: <S: 0, 64>

Format: The IPv6 address of host name.

Network [1..1] IPv6 Assignment

Define how the system will obtain its IPv6 address and the default gateway address. This setting only applies to systems on IPv6.

Value space: <Static/DHCPv6/Autoconf>

Static: The codec and gateway IP-addresses must be configured manually using the Network IPv6 Address and Network IPv6 Gateway settings. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

DHCPv6: All IPv6 addresses, including options, will be obtained from a DHCPv6 server. See RFC3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC4862 for a detailed description. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

Network [1..1] IPv6 Dhcoptions

Retrieves a set of DHCP options from a DHCPv6 server.

Value space: <Off/On>

Off: Set to Off when the IPv6 Assignment setting is set to Static.

On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

Network [1..1] IPv6 Gateway

Define the IPv6 network gateway address. Only applicable if the Network IPv6 Assignment is set to Static.

Value space: <S: 0, 64>

Format: The IPv6 address of host name.

Network [1..1] Link Endpoint

Set the Ethernet link speed for the Endpoint PHY port on ISDN Link.

Value space: <Auto/10half/10full/100half/100full/1000full>

Auto: Autonegotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

1000full: Force link to 1 Gbps full-duplex.

Network [1..1] Link Network

Set the Ethernet link speed for the LAN PHY port on ISDN Link.

Value space: <Auto/10half/10full/100half/100full/1000full>

Auto: Autonegotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

1000full: Force link to 1 Gbps full-duplex.

Network [1..1] QoS Mode

The QoS (Quality of Service) is a method which handles the priority of audio, video, data, etc. in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Value space: <Off/Diffserv>

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to Diffserv you must configure the Diffserv sub menu settings (Audio, Data, Signalling, Video, ICMPv6 and NTP).

Network [1..1] QoS Diffserv Audio

The Diffserv Audio defines which priority Audio packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for Audio packets is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.

Network [1..1] QoS Diffserv Data

The Diffserv Data defines which priority Data packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for Data packets is Diffserv Code Point (DSCP) AF23, which equals the value 22. If in doubt, contact your network administrator.

Network [1..1] QoS Diffserv ICMPv6

The Diffserv ICMPv6 defines which priority ICMPv6 packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for ICMPv6 packets is Diffserv Code Point (DSCP) CS7, which equals the value 56. If in doubt, contact your network administrator.

Network [1..1] QoS Diffserv NTP

The Diffserv NTP defines which priority NTP packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for NTP packets is Diffserv Code Point (DSCP) CS7, which equals the value 56. If in doubt, contact your network administrator.

Network [1..1] QoS Diffserv Signalling

The Diffserv Signalling defines which priority Signalling packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for Signalling packets is Diffserv Code Point (DSCP) AF31, which equals the value 26. If in doubt, contact your network administrator.

Network [1..1] QoS Diffserv Video

The Diffserv Video defines which priority Video packets should have in an IP network. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator.

Value space: <0..63>

Range: Select a value from 0 to 63. A recommended value for Video packets is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.

Network [1..1] VLAN Voice Mode

Set the VLAN voice mode.

NOTE: The ISDN Link and the TelePresence endpoint must be configured for the same VLAN. First configure the ISDN Link, then configure the endpoint. If done opposite, or if configured to different VLANs, the two devices will lose contact and you will need to connect to the ISDN Link through the serial interface to complete the VLAN configuration. When set to Auto on both devices, the CDP provisioner on the

, if present, will take care of the VLAN configuration.

NOTE: If configuring the TelePresence endpoint for provisioning to CUCM, note that the VLAN Voice Mode is automatically set to Auto on the endpoint when the Provisioning Mode is set to CUCM. In cases like this: First set the VLAN Voice Mode to Auto on ISDN Link, then configure the TelePresence endpoint for provisioning to CUCM.

Value space: <Auto/Manual/Off>

Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled.

Manual: If the ISDN Link is paired with a TelePresence endpoint; first set the VLAN Voice VlanId, then set the VLAN Voice Mode to Manual. The VLAN Voice ID is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.

Off: VLAN is not enabled.

Network [1..1] VLAN Voice VlanId

Set the VLAN voice ID. This setting will only take effect if VLAN Voice Mode is set to Manual.

Value space: <1..4094>

Range: Select a value from 1 to 4094.

NetworkServices configuration

NetworkServices SSH Mode

SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.

Value space: <Off/On>

Off: If disabling SSH Mode and operating in automatic pairing mode, it will no longer be possible to manage the ISDN Link via the TelePresence endpoint's web interface.

On: The SSH mode is enabled.

NetworkServices NTP Address

Enter the NTP Address to define the network time protocol server address. This address will be used if NTP Mode is set to Manual, or if set to Auto and no address is supplied by a DHCP server.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the time of the system to a reference time server.

Value space: <Off/Auto/Manual>

Off: The system will not use an NTP server.

Auto: The system will use the NTP server, by which address is supplied from the DHCP server in the network. If no DHCP server is used, or the DHCP server does not provide the system with a NTP server address, the system will use the static defined NTP server address specified by the user.

Manual: The system will always use the static defined NTP server address specified by the user.

Security configuration

Security Session InactivityTimeout

NOTE: Changing this parameter does not take effect for users that are already logged in.

Determines how long the system will accept inactivity from the user before the user is automatically logged out.

Value space: <0..10000>

Range: Select a value from 0 to 10000 minutes. 0 means that inactivity will not enforce automatically logout.

SIP configuration

SIP Profile [1..1] DefaultTransport

NOTE: Only applicable when used in manual pairing mode.

Select the transport protocol to be used over the LAN.

Value space: <UDP/TCP/Tls/Auto>

UDP: The system will always use UDP as the default transport method.

TCP: The system will always use TCP as the default transport method.

Tls: The system will always use TLS as the default transport method.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

SIP Profile [1..1] Outbound

NOTE: Only applicable when used in manual pairing mode.

The client initiated connections mechanism for firewall traversal, connection reuse and redundancy. The current version supports <http://tools.ietf.org/html/draft-ietf-sip-outbound-20>.

Value space: <Off/On>

Off: Connect to the single proxy configured first in Proxy Address list.

On: Set up multiple outbound connections to servers in the Proxy Address list.

SIP Profile [1..1] Type

NOTE: Only applicable when used in manual pairing mode.

Enables SIP extensions and special behaviour for a vendor or provider.

Value space: <Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel/Broadsoft>

Standard: To be used when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)

Alcatel: To be used when registering to Alcatel-Lucent OmniPCX Enterprise. NOTE: This mode is not fully supported.

Avaya: To be used when registering to Avaya Communication Manager. NOTE: This mode is not fully supported.

Cisco: To be used when registering to Cisco Unified Communication Manager.

Microsoft: To be used when registering to Microsoft LCS or OCS. NOTE: This mode is not fully supported.

Nortel: To be used when registering to Nortel MCS 5100 or MCS 5200 PBX. NOTE: This mode is not fully supported.

Broadsoft: To be used when registering to Broadsoft.

SIP Profile [1..1] URI 1

NOTE: Only applicable when used in manual pairing mode.

The SIP URI or number is used to address the system. This is the URI that is registered and used by the SIP services to route inbound calls to the system. A Uniform Resource Identifier (URI) is a compact string of characters used to identify or name a resource.

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters.

SIP Profile [1..1] Authentication [1..1] LoginName

NOTE: Only applicable when used in manual pairing mode.

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

SIP Profile [1..1] Authentication [1..1] Password

NOTE: Only applicable when used in manual pairing mode.

This is the password part of the credentials used to authenticate towards the SIP proxy.

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

SIP Profile [1..1] Proxy [1..4] Address

NOTE: Only applicable when used in manual pairing mode.

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided. If Outbound is enabled, multiple proxies can be addressed.

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters. An IP address that contains letters (192.a.2.0) or invalid IP addresses (192.0.1234.0) will be rejected.

SIP Profile [1..1] Proxy [1..4] Discovery

NOTE: Only applicable when used in manual pairing mode.

Select if the SIP Proxy address is to be obtained manually or by using Dynamic Host Configuration Protocol (DHCP).

Value space: <Auto/Manual>

Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).

Manual: When Manual is selected, the manually configured SIP Proxy address will be used.

SystemUnit configuration

SystemUnit Name

Enter the name of the unit. Is used to identify the unit in various scenarios.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

T1 configuration

T1 Interface [1..1] CableLength

Specifies the length of the cable connected to the T1 interface.

Value space: <Range1/Range2/Range3/Range4/Range5>

Range1: 0-133 ft (0-40 m)

Range2: 133-266 ft (40-81 m)

Range3: 266-399 ft (81-122 m)

Range4: 399-533 ft (122-162 m)

Range5: 533-655 ft (162-200 m)

Time configuration

Time Zone

Set the time zone where the system is located, using Windows time zone description format.

Value space: See the following list:

GMT-12:00 (International Date Line West)
 GMT-11:00 (Midway Island, Samoa)
 GMT-10:00 (Hawaii)
 GMT-09:00 (Alaska)
 GMT-08:00 (Pacific Time (US & Canada); Tijuana)
 GMT-07:00 (Arizona)
 GMT-07:00 (Mountain Time (US & Canada))
 GMT-07:00 (Chihuahua, La Paz, Mazatlan)
 GMT-06:00 (Central America)
 GMT-06:00 (Saskatchewan)
 GMT-06:00 (Guadalajara, Mexico City, Monterrey)
 GMT-06:00 (Central Time (US & Canada))
 GMT-05:00 (Indiana (East))
 GMT-05:00 (Bogota, Lima, Quito)
 GMT-05:00 (Eastern Time (US & Canada))
 GMT-04:30 (Caracas)
 GMT-04:00 (La Paz)
 GMT-04:00 (Santiago)
 GMT-04:00 (Atlantic Time (Canada))
 GMT-03:30 (Newfoundland)
 GMT-03:00 (Buenos Aires, Georgetown)
 GMT-03:00 (Greenland)
 GMT-03:00 (Brasilia)
 GMT-02:00 (Mid-Atlantic)
 GMT-01:00 (Cape Verde Is.)
 GMT-01:00 (Azores)
 GMT (Casablanca, Monrovia)
 GMT (Coordinated Universal Time)
 GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)
 GMT+01:00 (West Central Africa)
 GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna)
 GMT+01:00 (Brussels, Copenhagen, Madrid, Paris)
 GMT+01:00 (Sarajevo, Skopje, Warsaw, Zagreb)
 GMT+01:00 (Belgrade, Bratislava, Budapest, Ljubljana, Prague)
 GMT+02:00 (Harare, Pretoria)
 GMT+02:00 (Jerusalem)
 GMT+02:00 (Athens, Istanbul, Minsk)
 GMT+02:00 (Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)
 GMT+02:00 (Cairo)
 GMT+02:00 (Bucharest)
 GMT+03:00 (Nairobi)
 GMT+03:00 (Kuwait, Riyadh)
 GMT+03:00 (Moscow, St. Petersburg, Volgograd)
 GMT+03:00 (Baghdad)
 GMT+03:30 (Tehran)
 GMT+04:00 (Abu Dhabi, Muscat)
 GMT+04:00 (Baku, Tbilisi, Yerevan)
 GMT+04:30 (Kabul)
 GMT+05:00 (Islamabad, Karachi, Tashkent)
 GMT+05:00 (Ekaterinburg)
 GMT+05:30 (Chennai, Kolkata, Mumbai, New Delhi)
 GMT+05:45 (Kathmandu)
 GMT+06:00 (Sri Jayawardenepura)

GMT+06:00 (Astana, Dhaka)
GMT+06:00 (Almaty, Novosibirsk)
GMT+06:30 (Rangoon)
GMT+07:00 (Bangkok, Hanoi, Jakarta)
GMT+07:00 (Krasnoyarsk)
GMT+08:00 (Perth)
GMT+08:00 (Taipei)
GMT+08:00 (Kuala Lumpur, Singapore)
GMT+08:00 (Beijing, Chongqing, Hong Kong, Urumqi)
GMT+08:00 (Irkutsk, Ulaan Bataar)
GMT+09:00 (Osaka, Sapporo, Tokyo)
GMT+09:00 (Seoul)
GMT+09:00 (Yakutsk)
GMT+09:30 (Darwin)
GMT+09:30 (Adelaide)
GMT+10:00 (Guam, Port Moresby)
GMT+10:00 (Brisbane)
GMT+10:00 (Vladivostok)
GMT+10:00 (Hobart)
GMT+10:00 (Canberra, Melbourne, Sydney)
GMT+11:00 (Magadan, Solomon Is., New Caledonia)
GMT+12:00 (Fiji, Kamchatka, Marshall Is.)
GMT+12:00 (Auckland, Wellington)
GMT+13:00 (Nuku alofa)

Range: Select a time zone from the listed time zones. If using a command line interface watch up for typos.



Experimental configuration

The Experimental commands are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

APPENDICES

Password protection

NOTE: Although password is optional we strongly recommend that a password is set.

The ISDN Link is protected in the following ways:

- You always need to enter a username to sign in to the command line interface. If a password is set, you need to enter the password.
- You can protect the file system of the ISDN Link by setting a password for the root user. The root user is disabled by default.
- In addition, the following is applicable if using automatic pairing mode: When logging in to the ISDN Link, through the TelePresence endpoint's web interface, the access to the ISDN Link is handled by the protection mechanisms of the endpoint itself. In addition, the above mentioned protection mechanisms for accessing the ISDN Link directly still apply.

Password management

Make sure to keep a record of the password in a secure place. If you have forgotten the password and cannot access the system, you need to do a factory reset via the boot monitor. For details see [“Factory resetting the ISDN Link during boot through the serial port”](#) on page 77.

Changing the system password

The ISDN Link is delivered with a default user account with username `admin` and no password set. This user has full access rights to configuration of the system.

NOTE: We strongly recommend that you set a password for the `admin` user to restrict access to system configuration.

Please notice that the password on the ISDN Link cannot be set via the web interface. It must be set from a command line interface. Connect to the ISDN Link from the serial port, or over the network by SSH.

Perform the following steps to change the password:

- Connect to the ISDN Link over the network (SSH) or serial port. See [“Connecting to the ISDN Link”](#) on page 74.
- Run the following command:

```
systemtools passwd
```
- Follow the instructions on screen.

When prompted enter the current password and the new password, and confirm the new password. If no password has been set, the current password is blank.

The password format is a string with 0–64 characters.

Setting a root password

If you sign in to the ISDN Link as `root`, you can access the file system on the unit.

The root user is disabled by default. You can check if root is enabled or disabled by entering the following command:

```
systemtools rootsettings get
```

The command will respond with `On` if already enabled.

Setting a root password and activating the root user

Perform the following steps to activate the root user and set a password:

- Connect to the ISDN Link through the network over SSH or through the serial port.
- Sign in to the system with the username (`admin`) and password.
- Run the command:

```
systemtools rootsettings on [password]
```

Where `[password]` is the password you want to set.

NOTE: Although password is optional we **strongly** recommend that a password is set and a record made of this password. Having no root password, if root user is enabled, poses a serious security risk.

Connecting to the ISDN Link

When using the ISDN Link in *automatic pairing mode* you can connect to the ISDN Link from the TelePresence endpoint's web interface. In addition you can connect to the ISDN Link through the serial port or over the network through SSH.

Connect to the ISDN Link through the endpoint's web interface

When the ISDN Link is used in *automatic pairing mode* you can connect to the ISDN Link from the TelePresence endpoint's web interface. This requires that the ISDN Link and endpoint have been successfully paired.

1. Open a web browser and enter the address (IP address or URI) of the Telepresence endpoint.
2. Sign in with your username and, if a password is set, enter the password.

Connect to the ISDN Link through the serial port

3. Use a standard serial cable and connect the cable between ISDN Link serial (COM) port and a computer.
4. Use a terminal program to connect to the ISDN Link (115200, 8, 1, none)
5. Login as `admin` and, if a password is set, enter the password.

Connect to the ISDN Link through SSH

When you know the IP address of your ISDN Link an SSH over IP connection can be established.

1. Connect the network cable between ISDN Link Ethernet (LAN) port and the network.
2. Use a computer and open a command line interface, e.g. PuTTY. Enter the URI or IP address of the ISDN Link and select Connection Type SSH.
3. Login as `admin` and, if a password is set, enter the password.

Finding the IP address

When the ISDN Link is used in *automatic pairing mode* you can find the IP address of the ISDN Link on the TelePresence endpoint's web interface, else you must connect through the serial port of the ISDN Link.

Finding the IP address from the endpoint's web interface

When the ISDN Link is used in *automatic pairing mode* you can find the IP address of the ISDN Link on the TelePresence endpoint's web interface.

1. Connect to the ISDN Link through the TelePresence endpoint's web interface.
2. Navigate to: *Configuration > Peripherals* and press the **Manage ISDN Link** button.
3. Navigate to: *ISDN Link Status > Network > IPv4 > Address*.

Finding the IP address by connecting to the ISDN Link serial port

Finding the IP address by connecting through the serial port.

1. Connect to the ISDN Link through the serial port.
2. Run the following command:

```
xStatus Network
```

Unpairing the ISDN Link

When the ISDN Link is used in automatic pairing mode, unpairing of the ISDN Link and TelePresence endpoint can be done from the endpoint's web interface. This requires both the ISDN Link and the endpoint to be operational in order to reset pairing information on both units.

NOTE: Unpairing should always be done before replacing either the endpoint or the ISDN Link.

Persistent pairing

Pairing between the ISDN Link and the endpoint is persistent, which means that the two devices will remain paired until they are unpaired.

If the power is unplugged the ISDN Link will remain paired when the power is reconnected.

The endpoint and ISDN Link must be on the same subnet. If the endpoint and/or ISDN Link are assigned new IP addresses they will remain paired as long as they are kept in the same subnet.

NOTE: The pairing information is unique to the endpoint / ISDN Link entity. As a consequence, once paired, only those two units can interwork. Unpairing is required in order to change to another endpoint.

Unpairing from the TelePresence endpoint's web interface

When the ISDN Link is used in automatic pairing mode, unpairing of the ISDN Link and TelePresence endpoint can be done from the endpoint's web interface.

1. Open a web browser on your computer, enter the address (IP address or host name) of the TelePresence endpoint in the address bar, and login.
2. From the top menu, go to *Configuration > Peripherals*, and on the Peripherals page click the Manage ISDN Link button.
3. Click the Unpair this device button. This will clear the pairing information on both the endpoint and the ISDN Link.

Forced unpairing

When the ISDN Link is used in manual pairing mode, unpairing the ISDN Link is done from a command line interface.

There are some situations where the ISDN Link may not have been unpaired. In these situations you must force unpairing by manually unpair the ISDN Link in order to be able to restart pairing.

- The TelePresence endpoint was replaced without being unpaired.
- The ISDN Link was moved to another endpoint without unpairing prior to moving.

Follow the steps:

1. Connect to the ISDN Link over the network (SSH) or serial port.
See "[Connecting to the ISDN Link](#)" on page 74.
2. Run the command: `xCommand PairRestart Confirm: Yes`

Factory resetting the ISDN Link

NOTE: When running the factory reset command the codec will be reset to factory defaults. The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted.

The ISDN Link will automatically restart after the factory reset.

Factory resetting the ISDN Link

The ISDN Link can be reset to factory defaults using a command line interface.

1. Connect to the ISDN Link over the network (SSH) or serial port.
See [“Connecting to the ISDN Link”](#) on page 74.
2. Run the command: `xCommand SystemUnit FactoryReset Confirm: Yes`

Factory resetting the ISDN Link during boot through the serial port

The ISDN Link can be reset to factory defaults through the serial interface during boot:

3. Connect to the ISDN Link through the serial port.
See [“Connecting to the ISDN Link”](#) on page 74.
4. While power cycling the unit, press the ‘b’ key (use lower case) to halt the boot process.
5. When the boot process is halted you should see the following text:

```
Press 'b' to enter u-boot prompt  
Press 'c' to stop autoboot: 5
```
6. Press ‘c’ (use lower case) within 5 seconds.
7. When boot prompt is shown, run the factory reset command:

```
xCommand SystemUnit FactoryReset Confirm: Yes
```

Software upgrade from the command line interface

When the ISDN Link is used in automatic pairing mode you can upgrade the ISDN Link software from the TelePresence endpoint's web interface. For details see: "Software upgrade" on page 23.

Software upgrade from IL1.0 to IL1.1

If upgrading the software from IL1.0 to IL1.1 you must connect to the ISDN Link through the serial port, or if you know the IP address you can connect over the network through SSH.

Checking the software version

To see which software version is installed on the ISDN Link, run the command:

```
xStatus SystemUnit Software Version
```

Installing the software from an URL

If you have Internet access; you can initiate a software upgrade by fetching the software on a given URL. If the FTP site requires username and password, these parameters must be included.

- Software is available from the following URL:
<http://ftp.tandberg.com/pub/software/endpoints>

```
xCommand SystemUnit SoftwareUpgrade URL: "http://ftp.tandberg.com/pub/
software/endpoints/isdnlink/<filename>" UserName: "" Password: ""
```

```
*r SoftwareUpgradeResult (Status=OK)
```

- When finished loading and installing the software, the unit will reboot.

The SCP upgrade method

If you do not have Internet access, follow the SCP upgrade method.

1. Download the software to your computer. Software is available from the following URL:
▶ <http://ftp.tandberg.com/pub/software/endpoints>
2. If logging in as `root`, then root access needs to be enabled on ISDN Link.
For details see "Setting a root password and activating the root user" on page 73.
3. Copy the file to the ISDN Link using SCP, ensuring that the file is placed in folder `/appl` and is named `installsw`:
 - If using SCP from the command line of your computer enter:
 - `scp filetoupload.pkg root@ip.of.isdn.link:/appl/installsw`
 - If using WinSCP then connect to the ISDN Link as `root` and copy the file into `/appl` folder.
 - **IMPORTANT:** When you see the copy dialogue box showing `/appl/*.*` change this to `/appl/installsw` so that the filename is changed to `installsw`. When file is copied using WinSCP you may get some errors - these can be ignored.
4. Once the file has been uploaded to ISDN Link the unit needs to be restarted in order to use the new software.
 - If logged in as `root` enter `reboot`.
 - If logged in as `admin` enter `xCommand Boot`.
5. The software version is displayed when logging on to the unit; or you can run the command `xStatus SystemUnit` and check for the Software Version.

About audio and video encryption

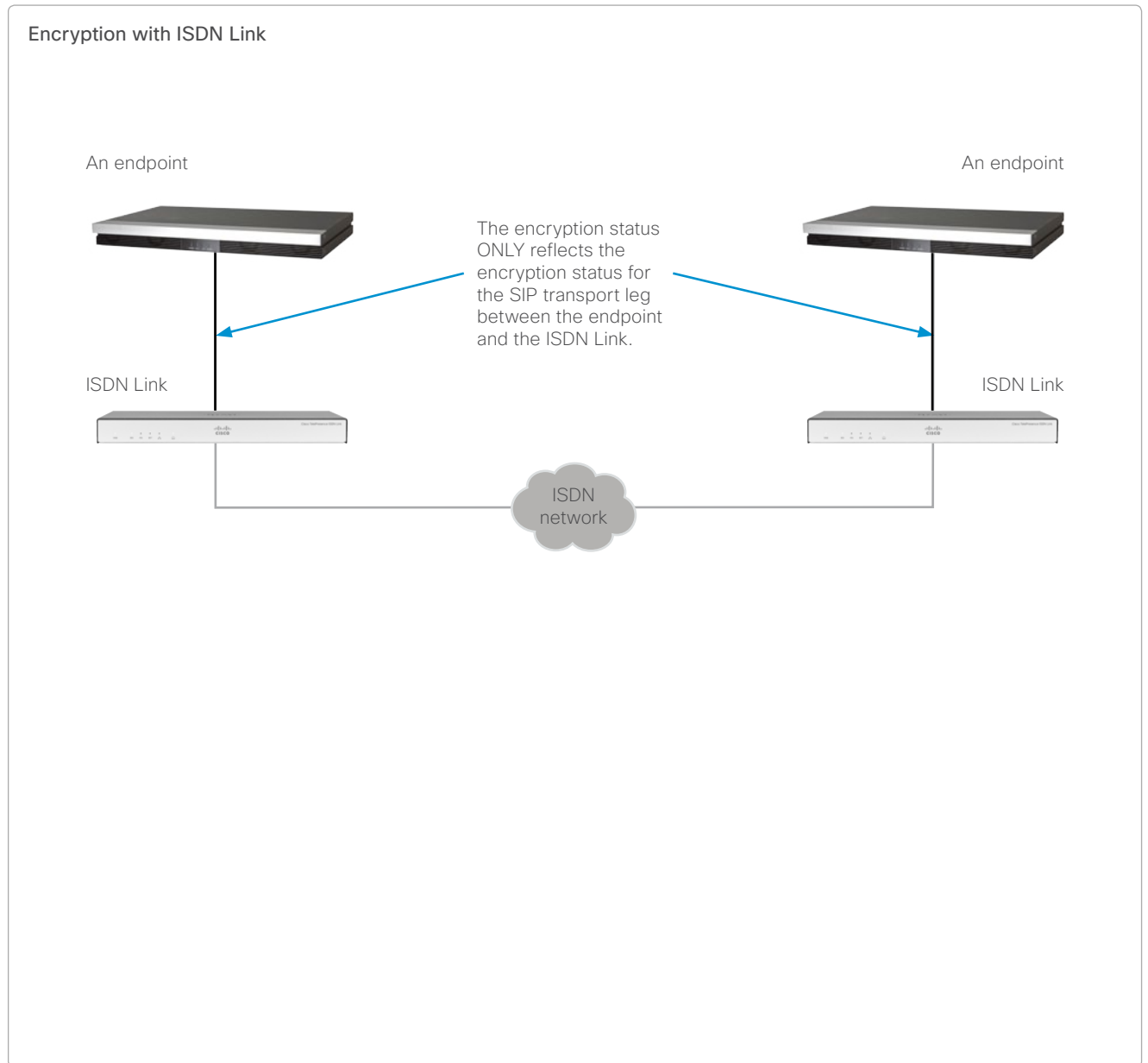
When the ISDN Link is used with TelePresence endpoints that support encryption the ISDN Link supports encryption (AES-128) on the media flow towards the endpoint and the ISDN/External network side. Plain telephony calls cannot be encrypted on the ISDN side.

NOTE: The encryption status shown on the endpoint side ONLY reflects the encryption status for the SIP transport leg between the endpoint and the ISDN Link.

Encryption indicators

Closed padlock: The call is encrypted between the paired endpoint and the H.323 side interface (PRI/BRI/NET).

Open padlock: No encryption.



Configuring parallel dialing for ADTRAN switch and PRI

When connecting PRI to an ADTRAN switch, you SHOULD disable parallel dialing used in bonding calls, due to internal ADTRAN capacity problems. Otherwise, outgoing calls (especially higher rates) may take a long time, or even fail. For other PBXs, you should be able to allow parallel dialing.

Configuring parallel dialing using the web interface

1. Open a browser, enter the address of the TelePresence endpoint and login with your username and password.
2. From the top menu, go to *Configuration > Peripherals*, and on the Peripherals page click the *Manage ISDN Link* button.
3. On the ISDN Link page go to the *ISDN Link Configuration* menu, and go to *ISDN > General Settings-*
4. Set *ParallelDial* to **Off** (or **On**)

Configuring parallel dialing using the command line interface

Connect to the ISDN Link over the network (SSH) or serial port.

See [“Connecting to the ISDN Link”](#) on page 74.

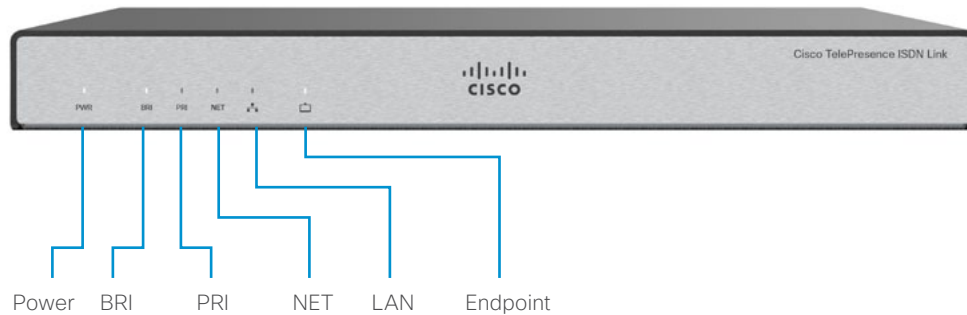
Run the command:

```
xConfiguration ISDN ParallelDial: Off (or On)
```


The physical interface

Front panel

The LED indicators are located on the front panel of the unit.

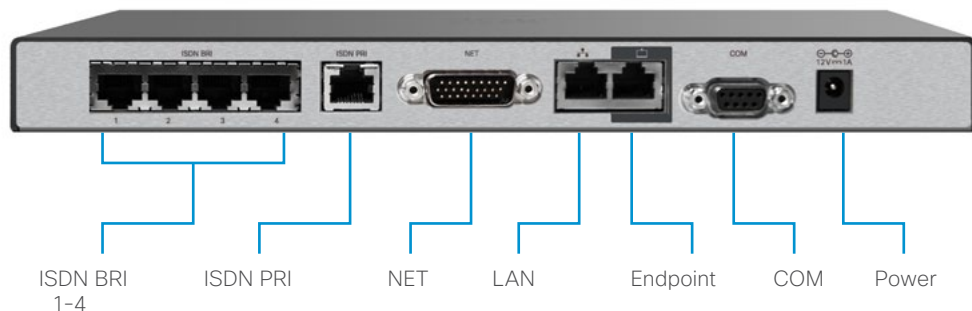


- | | |
|-------------|---|
| Power | <p>The LED lights up and remains lit when the ISDN Link is powered up.</p> <p>When the ISDN Link is not configured correctly this LED will be red. This will typically happen when you power up the unit for the first time.</p> <p>The LED typically turns red when there is an error with the selected interface (BRI/PRI/NET), or possibly other system errors that require attendance. Check the ISDN Link status information for errors:</p> <ul style="list-style-type: none"> • When used in automatic pairing mode, and after being paired with a TelePresence endpoint, the ISDN Link status information is available from the endpoint's web interface. • When used in manual pairing mode, see the user documentation for further details. |
| BRI/PRI/NET | <p>The BRI/PRI/NET LED indicates the activated network interface type. The LED blinks while there is call activity on the selected interface type.</p> |
| LAN | <p>The LED flickers when there is activity on the LAN network.</p> |
| Endpoint | <p>The LED flickers when there is activity between the ISDN Link and the endpoint (codec / video system).</p> |

The physical interface

Rear panel

The connectors are located on the rear panel.



Select one of the three options

- ISDN BRI S/T (RJ45) 512 kbps (4 × 128 kbps)
- ISDN PRI (RJ45) 1920 kbps (E1) / 1472 kbps (T1)
- NET (External Network, V.35/RS449/RS366/RS530) 1920 kbps

LAN (Ethernet 10/100/1000 Mbps, RJ45)

Connect to the IP network.

Endpoint (Ethernet 10/100/1000 Mbps, RJ45)

Connect to the endpoint (codec / video system).

COM/Serial port (RS-232)

Connect to a computer for configuration. Use: 115200 bps, 8 data bits, 1 stop bit, no parity.

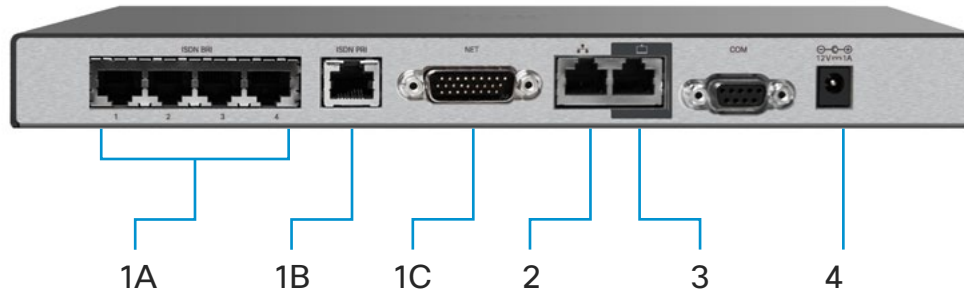
Power

External power adapter with 12 V/1.25 A DC output supports 100/240 VAC and 50/60 Hz inputs.

Connecting the cables

Connect the cables as described in steps A to D.

CAUTION: Always use the AC-DC adapter shipped with the product.



1. Select **one** of the three options for the ISDN line connection:
 - A. Connect the ISDN cable(s) between the ISDN BRI port(s) and the ISDN line(s),
 - B. or, connect the ISDN cable between the ISDN PRI port and the ISDN line,
 - C. or, connect the V.35 cable between the NET port and the external network line.

2. For system configuration, connect a Category 5e Ethernet cable between the Ethernet port on the ISDN Link and the LAN network.
3. Connect a Category 5e Ethernet cable between the Endpoint port on the ISDN Link and the Ethernet port on the endpoint.
4. Connect the supplied power adapter between the power connector and an electrical outlet.

CAUTION: Always use the AC-DC adapter shipped with the product.

Mounting the unit

Wall mounting

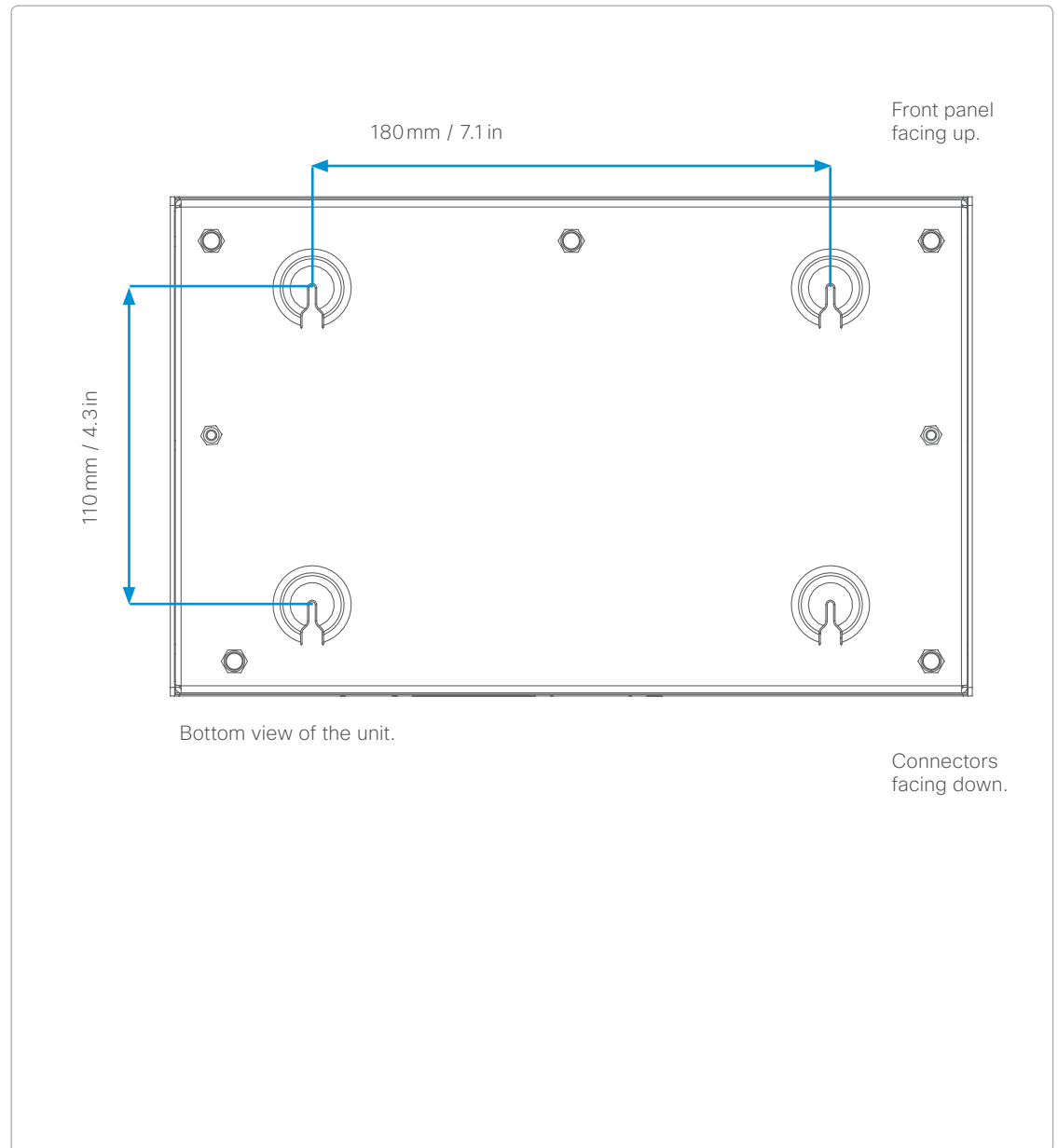
If you want to mount the ISDN Link on a wall, follow the instructions below. Mount the unit with the front panel facing up.

It is of great importance that the wall mount unit is safely installed, that the wall is able to support the product and that the screws or mounting means used are suitable for the wall and the weight of the product.

This type of equipment is to be installed by the submitter's/dealer's qualified installer. Installer is responsible for obtaining safety inspection of the structural integrity of the installation by the local authority/inspection department.

Table stand

Mount the four foot bumpers on its feet if you would like to place the ISDN Link on a table.



Pin-out schemes

This page gives an overview of the pin-out schemes for the connectors on the ISDN Link.

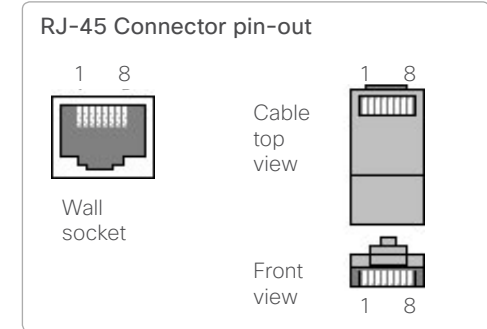
Pin-out RS-232 COM Port ¹		
Pin	Signal name	Direction ²
1	Carrier detect, CD	From DCE
2	Receive data, RXD	From DCE
3	Transmit data, TXD	To DCE
4	Data terminal ready, DTR	From DCE
5	Signal GND	
6	Data set ready, DSR	From DCE
7	Ready to send, RTS	To DCE
8	Clear to send, CTS	From DCE
9	Ring indicator, RI	From DCE

1) Only RXD, TXD and signal GND are used, the other pins are reserved for possible future use.

2) The ISDN Link is the DCE (Data Circuit-terminating Equipment).

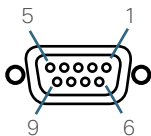
Gigabit Ethernet				
Pin	Name	Description	TIA/EIA 568A	TIA/EIA 568B
1	BI_DA+	Bi-directional pair A+ (tranceive)	white/green	white/orange
2	BI_DA-	Bi-directional pair A- (tranceive)	green	orange
3	BI_DB+	Bi-directional pair B+ (receive)	white/orange	white/green
4	BI_DC+	Bi-directional pair C+	blue	blue
5	BI_DC-	Bi-directional pair C-	white/blue	white/blue
6	BI_DB-	Bi-directional pair B- (receive)	orange	green
7	BI_DD+	Bi-directional pair D+	white/brown	white/brown
8	BI_DD-	Bi-directional pair D-	brown	brown

Ethernet interface: 2 × Gigabit ethernet (RJ-45). Gigabit Ethernet requires, at least Category 5 cable, but Category 5e or Category 6 cables may also be used and are often recommended. Gigabit Ethernet requires all four pairs to be present.



RS-232 9 pin D-SUB pin-out

External view of socket.



E1/T1 Interface		
PRI	Pin-Out	Crossover PRI cable
Pin 1	RX+	4
Pin 2	RX-	5
Pin 4	TX+	1
Pin 5	TX-	2

ISDN PRI (E1/T1) interface: 1 × PRI (RJ-45 Jack) Primary Rate Interface. Use any standard PRI cable to connect the ISDN Link to PRI.

S/T Interface	
BRI	Pin-Out
Pin 3	TX+
Pin 4	RX+
Pin 5	RX-
Pin 6	TX-

ISDN BRI (S/T) interface: 4 × ISDN I.420 (RJ-45 Jack) Basic Rate Interface (S/T). Use any standard ISDN BRI cable to connect the ISDN Link to BRI.

Pin-out schemes

This page gives an overview of the pin-out schemes for the connectors on the ISDN Link.

Pin-out V.35 DTE - DCE Port		
Pin	Signal Name	Description
1	FGND	Frame GND on equipment
11	SD(A)	Send Data / Transmit
12	SD(B)	Send Data / Transmit
13	RD(A)	Receive Data
14	RD(B)	Receive Data
15	SCR(A)	Signal Clock Receive
16	SCR(B)	Signal Clock Receive
17	SCT(A)	Signal Clock Transmit
18	SCT(B)	Signal Clock Transmit
19	GND ¹	Signal GND
22	RLSD(CD)	Received Line Signal Detector / Carrier Detect
23	RLSD(GND) ¹	Signal GND
24	RI	Ring Indicator
25	LOS	Loss of Signal (KG194)
26	DTR	Data Terminal Ready

1) These pins are connected to ground for correct operations

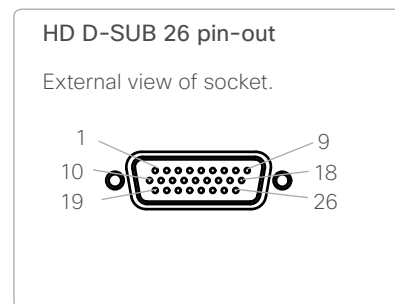
Pin-out RS449 DTE - DCE Port		
Pin	Signal Name	Description
1	FGND ¹	Frame GND
11	SD(A)	Send Data
12	SD(B)	Send Data
13	RD(A)	Receive Data
14	RD(B)	Receive Data
15	RT(A)	Receive Timing
16	RT(B)	Receive Timing
17	ST(A)	Send Timing
18	ST(B)	Send Timing
19	GND ²	GND
20	TR(A)	Terminal Ready
21	TR(B)	Terminal Ready
22	RR(A)	Carrier Detect / Receiver Ready
23	RR(B)	Carrier Detect / Receiver Ready
24	IC	Incoming Call
25	LOS	Loss of Signal (KG194)

1) Frame GND is connected to pin 1 on DTE

2) This pin is connected to ground for correct operations

Pin-out RS366 DTE - DCE Port		
Pin	Signal Name	Description
1	FGND	Frame GND
2	DPR	Digit Present
3	ACR	Abandon Call & Retry
4	CRQ	Call Request
5	PND	Present Next Digit
6	DLO	Data Line Occupied
7	NB1	Digit Bit 1
8	NB2	Digit Bit 2
9	NB4	Digit Bit 4
10	NB8	Digit Bit 8

Pin-out X.21 DTE - DCE Port		
Pin	Signal Name	Description
1	FGND	Frame GND
11	T(A)	Send Data / Transmit
12	T(B)	Send Data / Transmit
13	R(A)	Received Data / Receive
14	R(B)	Received Data / Receive
15	S(A)	Signal Element Timing
16	S(B)	Signal Element Timing
20	C(A)	Terminal Ready / Control
21	C(B)	Terminal Ready / Control
22	I(A)	Carrier Detect
23	I(B)	Carrier Detect



Cables

This page gives an overview of the cables available for ISDN Link.

Item Number	Description
CAB-DB26-530366	Cable Specification for Cisco TelePresence DB26 to RS-530 w/RS-366 Interface.
CAB-DB26-KIV7	Cable Specification for Cisco TelePresence DB26 to KIV-7 Interface.
CAB-DB26-530	Cable Specification for Cisco TelePresence DB26 to RS-530 Interface.
CAB-DB26-V35	Cable Specification for Cisco TelePresence DB26 to V.35 Interface.
CAB-DB26-V35366	Cable Specification for Cisco TelePresence DB26 to V.35 w/RS-366 Interface.
CAB-DB26-449366	Cable Specification for Cisco TelePresence DB26 to RS-449 w/RS-366 Interface.

Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

Current RFCs and drafts supported

- RFC 1889 RTP: A Transport Protocol for Real-time Applications
- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2429 RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)
- RFC 2460 Internet protocol, version 6 (IPv6) specification
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3047 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3960 Early Media
- RFC 4028 Session Timers in SIP
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol. draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4583 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams. draft-ietf-bfcpbis-rfc4583bis-00 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4587 RTP Payload Format for H.261 Video Streams
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5168 XML Schema for Media Control
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6184 RTP Payload Format for H.264 Video

Intellectual property rights

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ► <http://www.cisco.com/web/siteassets/contacts>

Corporate Headquarters

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134 USA