Cisco TelePresence ISDN GW 3241 & MSE 8321 Version 2.1(1.49) P

Software release notes

D14776.12

September 2011

Contents

Introduction

Software version 2.1(1.49) P (referred to as version 2.1 in this document) is a maintenance release for the Cisco TelePresence ISDN GW 3241 unit and the Cisco TelePresence ISDN GW MSE 8321 blade. The release fixes some specific issues as described in the Resolved caveats section and also implements some general improvements to the overall stability and security of the software.

This document describes the features that are supported by version 2.1 and the maintenance issues that it resolves.

For clarity, in this document the Cisco TelePresence ISDN GW 3241 unit and the Cisco TelePresence ISDN GW MSE 8321 blade are each generically referred to as the ISDN gateway.

CAUTION: ISDN GW MSE 8321 - Supervisor blade software version

In the case of the ISDN GW MSE 8321 blade, full functionality is supported for the Cisco TelePresence Supervisor MSE 8050 (Supervisor) blade if the Supervisor is running 2.2 or later. If the Supervisor is running version 2.1(1.18), you can use it to configure an IPv4 address for Port A but we advise you not to use it for other configuration options as results may be unpredictable. If the Supervisor is running a version earlier than 2.1(1.18), we advise you not to use it for *any* gateway configuration purposes.

CAUTION: Back up your configuration and CDR data before upgrading

You must back up your configuration before you upgrade the software.

If you use Call Detail Records (CDR) for billing, auditing or any other purpose, you must also download and save your current CDR data before you upgrade.

Features and functionality

- IPv6 support
- National/International Type of Number
- API enhancements
- Enhanced handling for incoming H.221 aggregation calls
- Enhanced handling for leased line group allocation

IPv6 support

Release 2.1 introduces IPv6 functionality for the ISDN gateway. IPv6 is enabled by assigning an IPv6 address to a physical interface on the system (restart is not needed). There is no feature key or global configuration requirement.

The key elements of IPv6 functionality in 2.1 are described here:

- Address assignment
- Routes
- DNS
- Services
- Link-local addresses

IPSec support is not available for IPv6.

Address assignment

IPv6 address assignment supports manual or automatic configuration modes.

In manual configuration mode you specify a single global IPv6 address with the prefix length. Optionally you can define a default gateway, either a link-local or global address.

In automatic configuration mode the gateway obtains an IPv6 address automatically with one of the following protocols:

- SLAAC (stateless address auto-configuration)
- Stateful DHCPv6 (address assignment by DHCPv6)
- Stateless DHCPv6 (address assignment by SLAAC; other configuration information by DHCPv6)

The protocol used depends on the ICMPv6 Router Advertisement (RA) messages. When the system multicasts an ICMPv6 Router solicitation, if no RA is received within 5 seconds, the system attempts stateful DHCPv6 to obtain an address. If an RA is received, the system proceeds with address assignment as indicated by the RA. Preference is given to stateful DHCPv6. For details, see the Automatic IPv6 address preferences table below.

Multiple global IPv6 addresses are not supported. If multiple IPv6 prefixes are advertised by the Router Advertisement (RA) messages then the gateway will select one valid IPv6 address prefix.

To configure IPv6 address assignment, go to **Network > Port A** or **Network > Port B** as appropriate.

Automatic IPv6 address preferences table

*RA flags			Preferred address
a	**o**	**m**	
0	0	0	Stateful DHCPv6
1	0	0	SLAAC
0	1	0	Stateful DHCPv6
1	1	0	Stateless DHCPv6
0	0	1	Stateful DHCPv6
1	0	1	Stateful DHCPv6
0	1	1	Stateful DHCPv6
1	1	1	Stateful DHCPv6

*a: ICMPv6 prefix information, auto flag

*o: ICMPv6, other flag

*m: ICMPv6, managed flag

Routes

The default gateway of a physical interface can be selected as the IPv6 gateway preference. All outgoing traffic is routed using the default gateway preference unless specified otherwise using explicit routes. You can add explicit routes to the routing table by specifying the IPv6 address in standard CIDR notation (address/prefix length) and selecting a physical interface or specifying a gateway IP address.

To configure IPv6 routing settings, go to **Network > Routes**.

DNS

DNS preference settings now include IPv6 options for Port A and Port B. If these are specified the DNS information can be obtained using DHCPv6, provided that the network interface is configured to use DHCP addressing and (in order to have meaningful DNS settings applied) that the DHCPv6 server provides DNS information along with network interface configuration information.

To configure DNS settings, go to **Network > DNS**.

Services

All network services available in the ISDN gateway support IPv6. Services can be enabled, disabled and configured to use a custom port.

To configure services settings, go to **Network > Services**.

Link-local addresses

Link-local IPv6 addresses are generated using the MAC address of each physical interface, and are thus unique per physical interface. No restrictions are imposed on link-local IPv6 addresses and all services enabled on their corresponding global IPv6 address are available on the link-local address. They support basic configuration and administration services (such as the web interface) but may not support full functionality such as making and receiving calls. Full functionality is only guaranteed for the main global IPv6 address on each interface.

IPv6 address fields

Note that when entering an IPv6 address in any address field in the web user interface, the address must be enclosed in square brackets [ ].

National/International Type of Number

Release 2.1 allows the ISDN Type of Number to be explicitly set to National or International, as required by some ISDN configurations including certain 4ESS switches.

This feature introduces two new fields on the **Settings > ISDN** page:

- Specify national/international type of number
- International prefix

If the *Specify national/international type of number* option is selected, then the Type of Number for an outgoing ISDN call will be National or International depending on whether the beginning of the dialed number matches the value (if any) specified in the *International prefix* field. If there is a match the call is International; otherwise the call is National.

If the *Specify national/international type of number* option is selected and no value is specified for the *International prefix* field then all calls will be National. Note that if the called number contains the International prefix, the ISDN gateway strips the prefix from both the called number that is sent to the ISDN switch and the number that is displayed in the UI pages (the prefix remains present in CDR logs).

If *Specify national/international type of number* is not selected then the situation remains unchanged and outgoing ISDN calls are made with Type of Number: Unknown.

API enhancements

Release 2.1 includes API enhancements which introduce feedback receivers and improved call history retrieval for configurations that use the Cisco TelePresence Management Suite (Cisco TMS).

Enhanced handling for incoming H.221 aggregation calls

Release 2.1 introduces improved call setup handling by the ISDN gateway for incoming, simultaneous H.221 aggregation calls.

Enhanced handling for leased line group allocation

This change applies only if the ISDN gateway is configured in leased line mode. In previous releases the gateway would respond by framing to an incoming ISDN leased line call on a configured leased line group. This occurred even if the ISDN to IP dial plan would subsequently cause the call to be rejected. In release 2.1 a framing response is triggered only if the dial plan is such that it would accept the incoming call on that leased line group.

Resolved caveats

The following issues that were found in previous releases of the ISDN gateway are now resolved.

Resolved since version 2.1(1.43)

Identifier	Internal reference	Summary
CSCts02706	110385	When the ISDN gateway auto attendant was under heavy load, it was possible that small amounts of memory might leak on each call. This could eventually lead to a crash due to running out of memory. This is now fixed.
CSCtr51248	117180	The ISDN gateway would send *syslog* entries with only the component and no log messages. This is now fixed.
CSCtr61439	117383	When receiving incoming calls, if the network side did not indicate a specific channel number in the setup message, the ISDN gateway would incorrectly try to place the call on channel 0, which is a reserved channel. As a result, the call would be rejected by the network as an invalid channel number is used. This is now fixed.

Resolved since version 2.1(1.22)

Identifier	Internal reference	Summary
CSCts03908	113188	When configured to use Non-Facility Associated Signaling (NFAS), the ISDN gateway sent a superfluous zeroed byte in Channel Identification Information Element messages. The message content length was indicated as 5 bytes rather than 4 bytes. This is now fixed.
CSCts03885	113244	Previously it was not possible to set the Ethernet port association for the H.323 gatekeeper (**Settings > H.323**) according to IP version. This has been resolved through the addition of two new check boxes.
CSCts03890	113424	To improve clarity, one field name on the DNS page of the ISDN gateway web interface has been changed from "*Name server (DNS) preference*" to "*DNS configuration*" and the associated DHCP-related settings have been renamed. The online help topic has also been reworded.
CSCtq41647	113738	If you defined an H.323 gatekeeper address through the ISDN gateway web interface as a hostname with more than 31 characters, the name would be truncated to 31 characters. The maximum length for H.323 gatekeeper addresses has now been extended to 255 characters.
CSCts03895	114529	Calls from a Polycom® RMX® over ISDN using a TCS-4 extension would connect as one-way audio only. This was due to an issue with asymmetric audio codecs that has now been resolved.

Known limitations

Raw IPv6 addresses in Firefox 4.0

It is not possible to access an ISDN gateway HTTPS web interface in Mozilla Firefox Version 4.0 using a raw IPv6 address. It is possible with IPv4 addresses and in earlier versions of Firefox, or if a hostname is used instead of the raw IPv6 address. This is being tracked by Mozilla as bug *633001*.

Open caveats

The following issues currently apply to this release of the ISDN gateway.

Identifier	Internal reference	Summary
CSCts03875	102867	This caveat applies to calls from one IP endpoint, through an MGC gateway and then a Cisco TelePresence ISDN Gateway, to a second IP endpoint. In this situation the second IP endpoint does not receive any video. The workaround is to use the MGC as an MCU instead of as a gateway. To do this: 1. The *Transcoding* option on the MGC conference must be enabled. 2. Make a direct ISDN call from an MGC conference to the second IP endpoint through the Cisco TelePresence ISDN Gateway. The call will be fully connected. 3. From the same conference, call the first IP endpoint over H.323. As there are only two endpoints in the conference, the call will appear to the callers in the same way as a point-to-point call over an MGC gateway.
CSCts03878	105356	When ISDN-side encryption is enabled on a point-to-point call using a TCS-4 dial plan between two MXP-based endpoints, the ISDN endpoint shows diminished resolution (H.263/CIF) compared to a call in which no ISDN-side encryption is used (H.264/400p). This usually happens when the MXP doesn't successfully switch the video codec when the call goes through the TCS-4 dial plan rule with encryption. This problem was only observed on NTSC models using TCS-4 and happens intermittently. Apart from a lower resolution, no other issues were observed in this call.
CSCts03881	105779	ISDN call fails to a Polycom VSX when the VSX is configured in Basic mode.
CSCts03904	106188	In the case of a call from an IP MXP endpoint through a Cisco TelePresence ISDN Gateway and then a TANDBERG Gateway to another IP MXP endpoint, the MXP endpoint on the TANDBERG Gateway may not receive any video. The workaround is to disable the H.264 video codec on the Cisco TelePresence ISDN Gateway. You can disable the codec either on a box-wide basis through the **Settings > ISDN** page or for the particular dial plan.
CSCts03871	108595	It is not possible to send H.239 from an Aethra ISDN endpoint to an IP participant through the ISDN gateway if H.243 floor and chair control is enabled. The workaround is to disable H.243 floor and chair control on the **Settings > ISDN** page of the gateway.

Updating the software

Software dependencies

In the case of the ISDN GW MSE 8321 blade, for full functionality the Cisco TelePresence Supervisor MSE 8050 (Supervisor) blade must be running software version 2.2 or later before you install this release on the ISDN GW MSE 8321 blade. If the Supervisor is running version 2.1(1.18), you can use it to configure an IPv4 address for Port A on the ISDN GW MSE 8321 blade but we advise you not to use it for other configuration options as results may be unpredictable.

If the Supervisor is running a version earlier than 2.1(1.18), we advise you not to use it for *any* gateway configuration purposes.

Prerequisites

CAUTION: You **must** back up your configuration **before** you upgrade the software. Certain features of this release change the format of the configuration file in a way that is not compatible with previous software versions.

In advanced security mode, if you do not keep an appropriate configuration file and you attempt to downgrade to a previous software version without using this configuration file, you will no longer be able to log in to the ISDN gateway.

CAUTION: If you use Call Detail Records (CDR) for billing, auditing or any other purpose, you **must** download and **save** your current CDR data. If you subsequently need to downgrade from version 2.1 back to any older version, the ISDN gateway will delete all existing CDRs.

Make sure that the ISDN gateway is not in use. The software upgrade process requires a hardware restart. Anyone using the gateway at the time of the upgrade may experience poor performance and loss of connectivity.

Have the following items available before you start:

- The new software image file.
- The current software image file (in case you need to reverse the upgrade).
- Your configuration backup XML file.
- The administrator user name and password for the backup file (you will need these if you have to use the backup).
- If applicable, make sure that the CDR data has been downloaded and saved.

Backup instructions

If the ISDN gateway is currently running software version 2.0 or later then you can back up the configuration via the web interface or via FTP. If the ISDN gateway is running an earlier version then you must back up via FTP.

To back up the configuration through the web interface, follow the instructions in the online help accessible from the interface.

To back up the gateway through FTP, follow the steps below:

1. Ensure that the FTP service is enabled on the **Network > Services** page.
2. Connect to the ISDN gateway using an FTP client. Log in as an administrator. You will see a file called configuration.xml. This contains the complete configuration of your unit.
3. Copy this file and store it somewhere safe.

CAUTION: You must remember the administrator user name and password for the backup configuration. You will need these if you ever need to use the backup file.

Upgrade instructions

Note: The upgrade may take up to 25 minutes to complete (you can monitor progress through the serial port).

Process using the web interface

1. Unzip the image file to a local folder.
2. In a web browser, navigate to the web interface of the ISDN gateway.
3. Sign in as administrator. On a new device the default user name is *admin* with no password.
4. Go to **Settings > Upgrade**.
5. In the **Main software image** area, specify the location of the software image file.
6. Click **Upload software image**.

   A progress bar displays while the web browser uploads the file to the gateway. This takes some time depending on your network connection. Do not navigate away from the upgrade page or refresh the page during the upload.

   The browser refreshes automatically after the upload completes and displays an upload completed message.
7. Close the success message.
8. In the changed Upgrade page, click **Shutdown N-port ISDN-IP gateway**.
9. When prompted, confirm the shutdown.
10. When the shutdown completes, click **Restart N-port ISDN-IP gateway and upgrade**.

    The device reboots and upgrades as it restarts. This may take some time to complete.

Note: If you are logged out due to inactivity, sign in again as admin and click **Restart N-port ISDN-IP gateway and upgrade**.

Process using FTP

1. Connect to the ISDN gateway via FTP.
   For example, from a command prompt type **`ftp <gateway IP address>`**.
2. Sign in as administrator. On a new device, the default user name is *admin* with no password.
3. Upload the upgrade file.
   For example, from the FTP prompt type **`put <image filename>.`**
4. When the upload completes, reboot the device. You can reboot from the upgrade page on the web interface. The device upgrades as it restarts. This may take some time to complete.

Note: If you are logged out due to inactivity, sign in again as admin and click **Restart N-port ISDN-IP gateway and upgrade**.

Downgrade instructions

If you need to reverse the upgrade, you can re-install a former version of the software. The downgrade procedure is the same as for the upgrade except that it uses an earlier software image.

CAUTION: If you use CDR data for any purpose you must download and save the CDR data before you downgrade the software. The ISDN gateway will delete all existing CDRs during the downgrade.

Process

1. Go to Settings > Upgrade.
2. In the **Restore configuration** area, navigate to and select the appropriate *configuration.xml* backup file.
3. Check the *User settings* check box.
4. If required, check the *Network settings* check box.
5. Click **Restore backup file**.
6. When the configuration restore is complete, follow the upgrade instructions in Updating the software.

Checking for updates and getting help

If you experience any problems when configuring or using the product, consult the online help available from the user interface. The online help explains how the individual features and settings work.

If you cannot find the answer you need, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that the ISDN gateway is running the most up-to-date software.
- Find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions.
- Get help from the Cisco Technical Support team. Make sure you have the following information ready before raising a case:
  - The serial number and product model number of the unit (if applicable).
  - The software build number which can be found on the product user interface (if applicable).
  - Your contact email address or telephone number.
  - A full description of the problem.

References and related documents

All documentation for the latest version of the ISDN gateway can be found at http://www.cisco.com/en/US/products/ps11448/tsd_products_support_series_home.html.