Cisco TelePresence ISDN GW 3200 Series & MSE 8310 Version 2.1(1.22) N

Software release notes

D14777.05

March 2011

Contents

Introduction

Software version 2.1(1.22) N (referred to as version 2.1 in this document) is a new feature release for the Cisco TelePresence ISDN GW 3200 Series and the Cisco TelePresence ISDN GW MSE 8310 blade (each generically referred to as the ISDN gateway in this document) and *only* for these products. This document describes the new features supported in version 2.1.

CAUTION: ISDN GW MSE 8310 - Supervisor blade software version

In the case of the ISDN GW MSE 8310 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 the configuration before upgrading

You **must** back up your configuration **before** upgrading to software version 2.1. Certain features of this release change the format of the configuration file in a way that is not compatible with previous software versions. 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 your ISDN gateway. See Downgrading software later in this document for more information.

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

If the ISDN gateway is currently running software version 2.0 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: Save Call Detail Records before upgrading

If you are using Call Detail Records (CDR) for billing, auditing or any other purpose, before you upgrade to this release, you **must** download and **save** your current CDR data.

If you downgrade from version 2.1 to any older version, the ISDN gateway will delete **all** existing CDRs.

New 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	NA
1	0	0	SLAAC
0	1	0	NA
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 issue in previous releases is resolved in this release.

Resolved since version 2.0(1.51)

Reference ID	Summary
9340	In previous releases, the ISDN gateway did not support Request in Progress (RIP) messages from gatekeepers. This has now been implemented.

Open caveats

The following issues currently apply to version 2.1.

Reference ID	Summary
664	Console port LED does not work.
2867	This caveat applies to calls from an IP endpoint (1) -> an MGC gateway -> Cisco TelePresence ISDN Gateway -> an IP endpoint (2). It causes IP endpoint (2) to not receive any video. There is a workaround for this situation: use the MGC as an MCU instead of as a gateway. That is, make a direct ISDN call from an MGC conference to IP endpoint (2) through the Cisco TelePresence ISDN Gateway and the call will be fully connected. Then from the same conference, call the IP endpoint (1) over H.323. For this workaround to work, the 'Transcoding' option on the MGC conference must be enabled. 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.
5356	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.
5779	ISDN call fails to Polycom VSX when VSX is configured in Basic mode.
6188	When placing a call from an IP MXP endpoint -> Cisco TelePresence ISDN Gateway -> TANDBERG Gateway -> IP MXP endpoint, the MXP endpoint, which connects to the TANDBERG Gateway, sometimes does not receive any video. The suggested workaround for this problem is to disable H.264 on the Cisco TelePresence ISDN Gateway. This can be done by disabling H.264 video codec under custom-codec selection from either Settings > ISDN page (box-wide) or on the particular dial plan.
8595	It is not possible to send H.239 from an Aethra ISDN endpoint to an IP participant through the Cisco TelePresence ISDN Gateway if H.243 floor and chair control is enabled. The work-around is to disable H.243 floor and chair control on the Cisco TelePresence ISDN Gateway's **Settings > ISDN** page.
12659	For multipoint calls to certain third-party ISDN MCUs, there is an issue with opening a content channel from the ISDN side. The content channel request will fail and the video channel may freeze. This is because the ISDN gateway does not currently handle incoming MCS (Multipoint Command Symmetrical data-transmission) messages in accordance with ITU-T H.239/H.243 recommendations. Specifically, it does not maintain messaging symmetry. This issue will be resolved in a subsequent maintenance release.

Upgrading software

Prerequisites

Before upgrading the software, you **must** back up your configuration and save your CDR data as described in the Introduction.

Make sure that the ISDN gateway is not in use. Anyone using the ISDN gateway at the time of the upgrade may experience poor performance and loss of connectivity.

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

Upgrading using a web browser

1. Unzip the image file.
2. In a web browser, browse to the IP address of the ISDN gateway.
3. Log in as administrator.
4. Go to the **Settings > Upgrade** page.
5. In the Main software image section, 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 ISDN GW or ISDN GW MSE blade. This takes some time depending on your network connection. Do not move your web browser away from the Upgrade software page or refresh the page during the upload process; if you do the upload will abort.

   When the upload completes the web browser refreshes automatically and displays “Main image upload completed successfully”.
7. Click **Close Status window**.
8. In the changed Upgrade page, click **Shut down N-port ISDN-IP gateway**.
9. Click **Confirm N-port ISDN-IP gateway shutdown**.
10. When shutdown has completed, click **Restart N-port ISDN-IP gateway and upgrade**.
11. When prompted, confirm the restart. The unit will reboot and upgrade itself – this may take up to 25 minutes to complete.

Note: If you are logged out due to inactivity, log in again as admin and on the Shutdown page click **Restart N-port ISDN gateway and upgrade**.

Upgrading using FTP

1. From the command prompt, use an FTP client to connect to the ISDN gateway. For example:
   `ftp <ISDN GW IP Address>`
2. Log in as administrator.
3. Upload the upgrade file from the command prompt. For example:

   put codian_isdn_gw_2.1_1.22(N)
4. When the upload has completed, go to the Upgrade page within the web interface.
5. Click **Shut down N-port ISDN-IP gateway**.
6. Click **Confirm N-port ISDN-IP gateway shutdown**.
7. When shutdown has completed, click **Restart N-port ISDN-IP gateway and upgrade**.
8. When prompted, confirm the restart. The unit will reboot and upgrade itself – this may take up to 25 minutes.

Note: If you are logged out due to inactivity, log in again as admin and on the Shutdown page click **Restart N-port ISDN gateway and upgrade**.

Downgrading software

Prerequisites

Before downgrading to an older software version, you **must** save your CDR data as described in the Introduction. If you downgrade from version 2.1 to any older version, the ISDN gateway will delete all existing CDRs.

Procedure

1. Go to **Settings > Upgrade**.
2. In the **Restore configuration** area, navigate to and select an appropriate *configuration.xml* backup file that is compatible with the release to which you want to downgrade.
3. Select *User settings*. If required, select *Network settings*.
4. Click **Restore backup file**.

When the configuration has been restored, follow the instructions in Upgrading software.

Checking for updates and getting help

We recommend that you register your product at http://www.tandberg.com/services/video-conferencing-product-registration.jsp in order to receive notifications about the latest software and security updates. New feature and maintenance releases are published regularly, and we recommend that your ISDN gateway software is always kept up to date.

If you experience any problems when configuring or using the ISDN gateway, consult the documentation at http://www.tandberg.com/support/video-conferencing-documentation.jsp for an explanation of how its individual features and settings work. You can also check the support site at http://www.tandberg.com/support/ to make sure you are running the latest software version.

You or your reseller can get help from our support team by raising a case at http://www.tandberg.com/support/video-conferencing-online-support.jsp. Make sure you have the following information ready:

- The serial number and product model number of the unit
- The software build number which can be found on the product user interface
- Your contact email address or telephone number

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.