Release Notes for Cisco IOS Release 12.2(12)DA6 for Cisco DSLAMs with NI-2 Cards

These notes are Part Number OL-3177-01 Rev. C0, updated June 16, 2004

These release notes describe features and caveats in Cisco IOS Release 12.2(12)DA6 for the Cisco 6015, Cisco 6160, and Cisco 6260 digital subscriber line access multiplexers (DSLAMs).

Cisco IOS Release 12.2(12)DA6 is based on Cisco IOS Release12.2(12)DA5, and includes all of the new features and corrections made in 12.2(12)DA4, 12.2(12)DA3, 12.2(12)DA2, 12.2(12)DA1 and 12.2(12)DA.

To see the release notes for Cisco IOS Release 12.2(12)DA5, go to www.cisco.com and click Products & Solutions > Switches > All Switches > Cisco 6000 Series IP DSL Switches > Release Notes > Release Notes for Cisco IOS Release 12.2(12)DA5s.

Note When you upgrade from Cisco IOS Release 12.1(5)DA2 or earlier images on the NI-2 card to Release 12.2(12)DA6, you must format the bootflash on the NI-2 card before loading the Release 12.2(12)DA6 dboot image. See the "Limitations and Restrictions" section on page 11.

For pointers to more information about the Cisco 6015, Cisco 6160, and Cisco 6260 DSLAMs, and their software, refer to the "Related Documentation" section on page 22. To learn more about caveats, visit the Cisco web site—see the "Obtaining Documentation" section on page 22 for details. Information about electronic documentation can also be found in both the "Obtaining Documentation" section on page 22 and the "Documentation CD-ROM" section on page 23.

Contents

This document contains the following topics:

System Requirements

Cisco IOS Release 12.2(12)DA runs on these DSLAMs:

- Cisco 6015 DSLAM
- Cisco 6160 DSLAM
- Cisco 6260 DSLAM

New and Changed Information

The following sections provide new and changed information for Cisco IOS Release 12.2(12)DA6, 12.2(12)DA5, 12.2(12)DA4, 12.2(12)DA3, 12.2(12)DA2, 12.2(12)DA1, and 12.2(12)DA.

Cisco IOS Release 12.2(12)DA6

Cisco IOS Release 12.2(12)DA6 is based on Cisco IOS Release 12.2(12)DA5 and includes all of the new features and corrections in Release 12.2(12)DA5, 12.2(12)DA4, 12.2(12)DA3, 12.2(12)DA2, 12.2(12)DA1, and 12.2(12)DA. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA6" section on page 19.

Cisco IOS Release 12.2(12)DA5

Cisco IOS Release 12.2(12)DA5 is based on Cisco IOS Release 12.2(12)DA4 and includes all of the new features and corrections in Release 12.2(12)DA4, 12.2(12)DA3, 12.2(12)DA2, 12.2(12)DA1, and 12.2(12)DA. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA5" section on page 20.

Cisco IOS Release 12.2(12)DA4

Cisco IOS Release 12.2(12)DA4 is based on Cisco IOS Release 12.2(12)DA3 and includes all of the new features and corrections in Release 12.2(12)DA3, 12.2(12)DA2, 12.2(12)DA1, and 12.2(12)DA. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA4" section on page 20.

Cisco IOS Release 12.2(12)DA3

Cisco IOS Release 12.2(12)DA3 is based on Cisco IOS Release 12.2(12)DA2 and includes all of the new features and corrections in Release 12.2(12)DA2, 12.2(12)DA1, and 12.2(12)DA. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA3" section on page 20.

Cisco IOS Release 12.2(12)DA2

Cisco IOS Release 12.2(12)DA2 is based on Cisco IOS Release 12.2(12)DA1 and includes all of the new features and corrections in Release 12.2(12)DA1, and 12.2(12)DA. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA2" section on page 21.

Cisco IOS Release 12.2(12)DA1

Cisco IOS Release 12.2(12)DA1 is based on Cisco IOS Release 12.2(12)DA and includes all of the new features introduced in that release. In addition, this release fixes the bugs described in the "Resolved Caveats—Release 12.2(12)DA1" section on page 21.

New Hardware Features in Release 12.2(12)DA

Cisco IOS Release 12.2(12)DA introduces the following new hardware feature:

- The Cisco OC-3c/OC-3c NI-2 card has been enhanced to support quality of service (QoS) in a fully loaded chassis of G.SHDSL SHTU-C (8xG.SHDSL) line cards. This enhancement eliminates the random cell drops that previously occurred in a chassis loaded with more than 16 G.SHDSL line cards.

Use the enhanced NI-2 card if you plan to deploy more than 16 G.SHDSL line cards in a Cisco DSLAM.

Notes A Cisco DSLAM can support either legacy or enhanced NI-2 cards.

The new NI-2 cards (NI2-155SM-155SM2 and NI2-155MM-155MM2) support Cisco IOS Release 12.1(7)DA2 or later; however, the card's new features are only enabled in Release 12.2(12)DA or later.

Enhanced Cisco OC-3c/OC-3c NI-2 Card Overview

This section describes how the Cisco OC-3c/OC-3c NI-2 card was enhanced to support QoS in a fully loaded chassis of G.SHDSL SHTU-C (8xG.SHDSL) line cards.

To accommodate these enhancements, the following changes were made to the legacy NI-2 card:

- The upstream field programmable gate array (FPGA) was enhanced to support QoS tables for the upstream traffic manager (UPTM).

  The DSLAM automatically builds the upstream QoS tables using the QoS values defined by commands such as **atm connection-traffic-table-row** and **atm pvc**. (See the "New and Changed Software for New Cisco OC-3c/OC-3c NI-2 Cards" section on page 4 for a list of **atm** commands used to set upstream QoS table values.)

- The size of the bootflash memory and main dynamic RAM (DRAM) were increased (see Table 1).

Supported Cisco DSLAM Chassis

The enhanced NI-2 card can be installed in the following Cisco DSLAM chassis:

Cisco 6100 DSLAM
Cisco 6130 DSLAM
Cisco 6015 DSLAM
Cisco 6160 DSLAM
Cisco 6260 DSLAM

OC-3c/OC-3c NI-2 Card Memory Enhancements

Table 1 shows the memory enhancements made to the new Cisco OC-3c/OC-3c NI-2 card.

Table 1   NI-2 Memory Enhancements

Memory Type	New NI-2 Card	Legacy NI-2 Card
Main DRAM	128 MB	64 MB
Flash	16 MB	16 MB
Bootflash	8 MB	4 MB

New and Changed Software for New Cisco OC-3c/OC-3c NI-2 Cards

The following list describes the software changes made to accommodate the enhanced NI-2 card:

- The **show hardware** command output displays the new NI-2 card types:

  NI2-155MM-155MM2
  NI2-155SM-155SM2

- The following **atm** commands were enhanced to accommodate upstream QoS tables. In addition to configuring the QoS values for the ATM switch component of the DSLAM, these commands now also define the values for the upstream QoS tables.

  atm clp-drop
  atm connection-traffic-table-row
  atm input-queue
  atm input-threshold
  atm pvc
  atm soft-vc

- The **show ni2-switch registers** and **show ni2-switch memory** commands have been enhanced to show upstream field programmable gate array (FPGA) data. For more information, see the description of these commands in the *Command Reference for Cisco DSLAMs with NI-2*.

- Two new object identifiers (OIDs) were added to the CISCO-ENTITY-VENDORTYPE-OID-MIB for the enhanced Cisco OC-3c/OC-3c NI-2 cards:

    cevNi2WanOc3smSubOc3smRev2
    cevNi2WanOc3mmSubOc3mmRev2

- The policer function was modified to reduce congestion in the DSLAM. The policer was moved to the upstream FPGA, which is closer to the upstream source. Note that as a result of this change, the DSLAM experiences low data throughput when policing on peak cell rate (PCR) with a large packet size and a data rate that greatly exceeds the selected PCR.

Cisco OC-3c/OC-3c NI-2 Card Requirements

The following requirements apply to legacy and enhanced Cisco OC-3c/OC-3c NI-2 cards:

Enhanced NI-2 Card Requirements

- An enhanced NI-2 card (NI2-155SM-155SM2 or NI2-155MM-155MM2).

- Cisco IOS Release 12.2(12)DA or later. The enhanced NI-2 card supports Release 12.1(7)DA2 or later. However, the card's new features are only enabled in Release 12.2(12)DA or later.

- A new ni2-dboot2-mz image (which is shipped preinstalled in the NI-2 bootflash memory).

Note The old dboot image does not work on enhanced NI-2 cards. If you load a dboot image onto a new NI-2 card, the NI-2 card becomes inoperable. (See the "Correcting Bootup Problems" section on page 9 for instructions on how to recover if this happens.)

Legacy NI-2 Card Requirements

- A legacy NI-2 card.

- A Cisco IOS software release that supports the features you need.

- A corresponding ni2-dboot-mz image.

New Software Features in Release 12.2(12)DA

Cisco IOS Release 12.2(12)DA introduces the following new software feature:

- The Octal-Port DMT ATU-C over ISDN (8xDMT over ISDN) line card has been enhanced to operate with the following customer premises equipment (CPEs):

    - Cisco SOHO 76 and 826 CPEs

    - Alcatel-based CPEs

Note Alcatel-based CPEs and Cisco SOHO 76 and 826 CPEs require Cisco IOS Release 12.2(4)YA2 or later. We also recommend that you issue the **dsl operating-mode annexb-ur2** command at the CPE to enable DMT operating mode on these CPEs.

Installation Notes

The following sections provide useful information for Cisco IOS Release 12.2(12)DA6 installation and operation:

- Upgrading Bootflash on a Legacy NI-2 Card to the 12.2(12)DA6 dboot Image, page 6 (Legacy NI-2 Cards)
- Upgrade Bootflash on a Legacy NI-2 Card to the 12.1(5)DA1 dboot Image, page 7 (Legacy NI-2 Cards)
- Booting the Enhanced OC-3/OC-3 NI-2 Card, page 8 (Enhanced NI-2 Cards)

Upgrading Bootflash on a Legacy NI-2 Card to the 12.2(12)DA6 dboot Image

When you upgrade from Cisco IOS Release 12.1(5)DA1 or earlier images on a legacy NI-2 card to Release 12.2(12)DA6, you must reformat the bootflash on the NI-2 card.

If you are upgrading from Cisco IOS Release 12.1(7)DA3, 12.2(1b)DA1, 12.2(5)DA1, 12.2(7)DA, 12.2(10) DA, 12.2(12)DA, 12.2(12)DA1, 12.2(12)DA2, 12.2(12)DA3, 12.2(12)DA4, or 12.2(12)DA5 you do not need to reformat the bootflash. You can skip this section and follow the DSLAM upgrade procedure at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/rel122/config/04conf09.htm

✎ **Note** We recommend that you have console access to the NI-2 card during the upgrade procedure. You can use the console connection to troubleshoot any unexpected events that occur during the upgrade.

To upgrade the boot image on a legacy NI-2 card, perform the following steps in privileged EXEC mode:

	Command	Purpose
Step 1	DSLAM# **show hardware**	Verify the type of Cisco OC-3c/OC-3c NI-2 card installed in the chassis to determine whether to download a new dboot image: • NI2-155MM-155MM2 or NI2-155SM-SM2—Indicates a new Cisco OC-3c/OC-3c NI-2 card, which is shipped with the correct image (dboot2) preinstalled. Skip this procedure and the following procedure. • Any other value—Indicates a legacy NI-2 card, which may need to be updated with a new image. Continue with this procedure.
Step 2	DSLAM# **dir bootflash:**	Verify that the bootflash image is **ni2-dboot-mz.121-5.da1** or **ni2-dboot-mz.121-4.da**. If it is neither, go to the "Upgrade Bootflash on a Legacy NI-2 Card to the 12.1(5)DA1 dboot Image" section on page 7 and perform the instructions there, and then return to this step. This is required because of a problem (CSCdr89374) in old bootflash images.
Step 3	DSLAM# **dir flash:**	Determine the name of the flash file that begins with **ni2-** and use it as *filename* in Step 4.
Step 4	DSLAM# **delete flash:**_filename_	Delete the flash file name found in Step 3. Repeat Step 3 and Step 4 until all files in the flash file have been deleted.

	Command	Purpose
Step 5	DSLAM# **squeeze flash:**	Recover available space in flash memory.
Step 6	DSLAM# **copy tftp:**//*tftpserver*:**TFTPBOOT/ni2-dsl-mz.122-12.da6.bin flash:**	Copy the Cisco IOS software image from a TFTP server to flash.
Step 7	DSLAM# **configure terminal** DSLAM (config)# **no boot system** DSLAM (config)# **boot system flash:ni2-dsl-mz.122-12.da6.bin** DSLAM# **end**	Enter global configuration mode. Disable the boot from system. Specify the name of the system image to load at startup. Exit global configuration mode.
Step 8	DSLAM# **copy running-config startup-config**	Save your changes to the startup configuration.
Step 9	DSLAM# **reload**	Reload the system to upgrade the image.
Step 10	DSLAM# **show version**	Confirm that the running image is **ni2-dsl-mz.122-12.da6.bin**. If it is not, go to Step 6.
Step 11	DSLAM# **format bootflash:**	Erase all information in bootflash memory. Answer **y** to all confirm questions. When the DSLAM returns to the EXEC prompt, bootflash memory is successfully formatted and ready for use. Ensure that the bootflash is 3.8 MB total. If it is not, go to Step 5.
Step 12	DSLAM# **copy tftp:**//*tftpserver*:**TFTPBOOT/ni2-dboot-mz.122-12.da6.bin bootflash:**	Copy the boot image from a TFTP server to the bootflash.
Step 13	DSLAM# **reload**	Reload the system to upgrade the image.

Upgrade Bootflash on a Legacy NI-2 Card to the 12.1(5)DA1 dboot Image

When you upgrade from Release 12.1(3)DA or earlier images on a legacy NI-2 card to Release 12.1(5)DA1, we recommend that you upgrade the bootflash image on the NI-2 card to the 12.1(5)DA1 dboot image.

To upgrade the dboot image in bootflash on a legacy NI-2 card, perform the following steps:

	Command	Purpose
Step 1	DSLAM> **enable** Password: <password> DSLAM#	Enter enable mode. Enter the password. The enable mode prompt is DSLAM#.
Step 2	DSLAM# **delete bootflash:***filename*	Make room in the bootflash by deleting the name of the current boot image.
Step 3	DSLAM# **squeeze bootflash**	Recover available space in bootflash using the **squeeze bootflash** command.
Step 4	DSLAM# **copy** tftp://[server name] **/[directory]/ni2-dboot-mz.121-5.da1 bootflash:**	Copy the boot image to the bootflash.
Step 5	DSLAM# **show version**	Record the current value of the config-register that appears on the last line of the show version display.

	Command	Purpose
Step 6	`DSLAM# `**`configure terminal`**	Enter global configuration mode, which has a prompt of `DSLAM(config)#`.
Step 7	`DSLAM(config)# `**`config-register 0`**	Set the config register to 0x0000 so that the NI-2 card reboots in the ROM monitor.
Step 8	`DSLAM(config)# `**`exit`**	Exit global configuration mode.
Step 9	`DSLAM# `**`copy running-config startup-config`**	Save the running configuration.
Step 10	`DSLAM# `**`reload`**	Reset the system.
Step 11	`rommon> set`	If you see BOOTLDR after you enter this command, the image in bootflash is already being used as the bootstrap image; go to Step 15. Otherwise, go to Step 12 and enter the commands in Steps 12 through 14 to force the system to use **ni2-dboot-mz.121-5.bin** as the bootstrap image.
Step 12	`rommon> unset BOOTLDR`	Unset BOOTLDR to remove the variable.
Step 13	`rommon> sync`	Sync to save the state of rommon.
Step 14	`rommon> b`	When the NI-2 card boots, it uses **ni2-dboot-mz.121-5da.bin** as the bootstrap image.
Step 15	`DSLAM# `**`configure terminal`**	Enter global configuration mode, which has a prompt of `DSLAM(config)#`.
Step 16	`DSLAM(config)# `**`config-register`**` value`	Set the config-register to the value you recorded in Step 5.
Step 17	`DSLAM(config)# `**`exit`**	Return to enable mode. Go to the "Limitations and Restrictions" section on page 11.

Booting the Enhanced OC-3/OC-3 NI-2 Card

Before attempting to boot the DSLAM, consider the following:

- The new NI-2 cards (NI2-155SM-155SM2 and NI2-155MM-155MM2) work only with a new ni2-dboot2-mz image that is shipped preinstalled in the NI-2 bootflash. New NI-2 cards do not run with an old dboot image.

- Legacy NI-2 cards require an ni2-dboot-mz image; they do not run with the new dboot2 image.

⚠
Caution New NI-2 cards support Cisco IOS Release 12.2(12)DA and later, and release 12.1(7)DA2 to 12.2(10)DA. However, to run release 12.1(7)DA2 to 12.2(10)DA, you *must* load the dboot2 image before you load the Cisco IOS software image. Otherwise, the DSLAM becomes inoperable.

To boot the enhanced Cisco OC-3/OC-3 NI-2 card, follow the instructions in the *Configuration Guide for Cisco DSLAMs with NI-2*. See the section "Booting from Flash Memory Configuration Tasks" in chapter 9, "Loading System Software Images and Configuration Files," at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/rel122/config/04conf09.htm

Correcting Bootup Problems

If you attempt to run an incorrect dboot or dboot2 image, or you attempt to boot a new NI-2 card with legacy Cisco IOS software before booting the new dboot2 image, the DSLAM becomes inoperable. If this occurs, see the following sections for information about how to correct the problem and make the DSLAM operational:

Running Cisco IOS Release 12.1(7)DA2 to 12.2(10)DA on a New NI-2 Card

You can run Cisco IOS Releases 12.1(7)DA2 to 12.2(10)DA on the new NI-2 cards (NI2-155MM-155MM2 and NI2-155SM-155SM2). However, before you attempt to boot the Cisco IOS software from flash, you must first boot the ni2-dboot2-mz (dboot2) image from bootflash.

✎ **Note** To run Cisco IOS releases earlier than Release 12.2(12)DA on a new NI-2 card, do not boot from flash until you have booted the ni2-dboot2-mz image from bootflash. Otherwise, the DSLAM becomes inoperable.

If you encounter problems booting Cisco IOS Release 12.1(7)DA2 to 12.2(10)DA on the new NI-2 cards, perform the following steps to correct the problem and make the DSLAM operational:

Step 1 Issue the following command in to ensure that the correct dboot2 image is loaded in bootflash memory:

```
DSLAM> show ni2-switch register
```

Step 2 Check the command output to make sure the FPGA major revision is 3 (see highlighted text below). This indicates that the dboot2 image is loaded.

```
Upstream FPGA revision MAJ:3 Minor:0
```

Step 3 Issue the following command in global-configuration mode to set the configuration register to load the DSLAM image from the **boot system** commands in the startup configuration file:

```
DSLAM(config)# config-register 0x2102
```

Step 4 Exit configuration mode and reload (reboot) the DSLAM to make the DSLAM operational. This process loads the images in the correct order: dboot2 and then the legacy Cisco IOS software.

```
DSLAM(config)# end
DSLAM# reload
```

Using Rommon to Recover from Corrupted dboot2 Images

This procedure describes how to use ROM monitor (rommon) mode to recover from problems caused by an invalid or corrupt dboot2 image. This procedure uses the **xmodem** command to retrieve a valid dboot2 image from a PC or network server.

✎
Note The **xmodem** command used in this procedure is extremely slow. Therefore, only perform this procedure if all other attempts to obtain a dboot2 image fail. Also note that the command is supported only on the new NI-2 cards (NI2-155MM-155MM2 and NI2-155SM-155SM2).

Step 1 Log in to the DSLAM through a console port. The rommon prompt (`rommon>`) should be displayed. If it is not, get into configuration mode and issue the command **config-register 0x0 end write reload**.

Step 2 Issue the following command at the rommon prompt.

```
rommon> config-register 0x2102
```

Step 3 Issue the following command to manually boot the DSLAM from bootflash.

```
rommon> boot bootflash: [filename]
```

Step 4 If Step 3 worked, you need not perform the rest of this recovery procedure. Instead, you should boot the Cisco IOS software and proceed to Step 7.

If Step 3 did not work, the rommon prompt is returned and you must proceed to Step 5 to continue with the recovery procedure.

Step 5 If the correct dboot2 image is not in bootflash or the image is corrupt, perform the following steps to use the **xmodem** command to download a valid dboot2 image to use to boot the DSLAM:

a. Open a terminal emulation window (such as Hyper Terminal) on a PC that is connected to the DSLAM through a console port.

b. Configure the following terminal emulation settings: port = **com1** or **com2**, data rate = **9600**, bits = **8**, parity = **none**, stop bits = **1**. You must use these values for the recovery procedure to work.

c. Make sure that the PC contains a valid dboot2 image or is connected to a network where a dboot2 image is stored on a server.

d. On the DSLAM, issue the following command to copy the dboot2 image to the specified *filename*. The command creates a temporary copy of the dboot2 image on the DSLAM; therefore, you must copy the image to bootflash or it will be lost when you reload the DSLAM (Step 6).

```
rommon> xmodem filename
```

e. Wait for a prompt indicating that rommon is ready to receive the file.

f. In the Hyper Terminal window on the PC, click **Transfer** in the menu bar at the top of the window and select **Send File**.

g. Select **Xmodem** as the protocol, and specify the name of the dboot2 image to copy to the DSLAM.

h. Click **Send** to start the copy.

✎
Note It may take 1 hour or more for the copy to complete.

i. When the download completes, the DSLAM boots automatically.

Step 6 To complete the recovery procedure, copy the dboot2 image to bootflash memory (for example, using TFTP). If you do not perform this step, the dboot2 image will be lost when you reload the DSLAM.

Step 7 To finish booting the DSLAM, issue the following command:

```
DSLAM> reload
```

Limitations and Restrictions

The following sections describe the limitations and restrictions for Cisco IOS software DSLAM releases.

Redundant NI-2 Card Operation

When using NI-2 cards in a redundant fashion, we recommend that you issue the command **redundancy reload-peer** on the active NI-2 card after the system has loaded. This causes the redundant NI-2 to reload and ensures that the redundant configuration is operational.

In rare instances during testing, a redundant NI-2 card sometimes appeared to be functional but was not. Issuing the **redundancy reload-peer** command corrected the problem every time.

Attainable Bit Rate Is Conservative on 4xflexi-DMT and 8xDMT

The reported DMT aggregate bit rate is less than the true attainable bit rate.

Limitations

Due to line condition variations between trains, the effect of trellis encoding, interleave delay, FEC check bytes, and so forth, the attainable bit rate estimate is not always 100 percent accurate. A conservative approach was taken in making the estimate; therefore, in general, you can get a higher rate than what the estimate suggests. For a fast-path scenario, the results should track fairly closely for the downstream rate and err on the conservative side for the upstream rate. For an interleave path scenario, the results are highly dependent on configurations.

At a higher reach or where line conditions are not optimal, trellis encoding, interleave delay, and FEC check bytes can provide a much higher rate than was estimated (greater than 128 kbps).

Workaround

There is no workaround. The aggregate bit rate calculation is an estimate, which does not accurately model all of the line conditions that affect the true attainable bit rate for a given profile. The calculations for aggregate bit rate are performed as follows:

- The downstream capacity is obtained from the number of Reed-Solomon payload bytes per frame exchanged during line training, that is, the K value. The per-second estimate is then calculated from this K value. An extrapolated margin value is derived from the per-second estimate to make sure that if the line is trained at the estimated rate, it has an adequate margin.

- For upstream, unlike downstream, the Reed-Solomon payload bytes per frame is not readily available. Furthermore, unlike downstream, which requires a CPE EOC response to know the downstream margin, the upstream margin is readily available at the CO (upstream margin is measured at the CO end). Using this upstream margin and the number of bins utilized for upstream, an estimate of upstream attainable bit rate is made. (The associated DDTS numbers are CSCdv05351 and CSCdv05322.)

CPE Performance Issues with Overhead Framing Modes 0, 1 and 2

The CPE does not train or perform reliably when the Discrete Multitone (DMT) profile is set to use overhead framing mode 0, 1, or 2.

Overhead framing modes 0, 1, and 2 are not supported at this time.

Workaround

Overhead framing mode 3 is designed for use with ATM. While overhead framing mode 1, which is not currently supported, is designed for Synchronous Transport Module (STM) mode. Configure your profiles to use overhead framing mode 3. Overhead framing mode 3 uses only 32 bytes of administrative overhead. Compared with overhead framing mode 1, it allows more bandwidth to be allocated to user data.

Trellis Encoding Enable Default Recommendations

Trellis encoding is disabled by default on the NI-2 card because it is not supported on the 4xDMT (ATUC-1-4DMT) line card. However, trellis encoding is supported on the 4xFlexiDMT (ATUC-4FLEXIDMT) line card and the 8xDMT (ATUC-1-DMT8 and ATUC-1-DMT8-I) line cards.

- For 4xDMT (ATUC-1-4DMT) ports—Disable trellis encoding in the DSL profile for those ports.
- For 4xFlexiDMT (ATUC-4FLEXIDMT) ports—Enable trellis encoding, except with ADI chipset-based CPEs that use ADI firmware prior to ADI 3.1. This includes all Cisco 677 and Cisco 627 CPEs.
- For 8xDMT (ATUC-1-DMT8 and ATUC-1-DMT8-I) ports—The default DMT setting for trellis encoding is auto-sense, which means that the 8xDMT line card attempts to automatically configure itself for the type of encoding supported on the CPE. If the auto-sense feature does not work, you may have to enable trellis encoding in the DSL profile for these ports.

✎

Note   If you are unsure if your CPE supports trellis encoding, check with the manufacturer.

For information about how to change trellis encoding settings on the NI-2 card, see the documentation at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/rel122/config/04conf04.htm#xtocid1734531

Restrictions on IP Services

This section describes restrictions on the Cisco NI-2 card IP services.

Restricted Layer 3 Services

NI2 IOS releases do not support the following Layer 3 services (or else these services are limited, as noted):

- IP Quality of Service.
- IP Queueing.
- IP Multicast.
- L2TP Tunnel Priority and Limit sessions.

- L2TP Network Server (LNS).
- The maximum number of MPLS/VPN for PPPoA terminations is 25 VPNs for PPPoA and 1 VPN for PPPoE.
- We recommend that you use a virtual template for PPPoX termination rather than a dialer interface.
- MPLS LDP protocol is not supported in this release. Use TDP protocol.
- Up to 32 subinterfaces can be used for IP termination under the trunk or subtend ports.
- Each DSLAM can support up to 50 MPLS VPNs.

Integrated Routing and Bridging Not Supported

MPLS VPN mapping of RFC 1483 routed sessions must not be confused with Integrated Routing and Bridging (IRB). IRB is not supported by MPLS VPN mapping of RFC 1483 routed sessions.

VPN Interfaces Restricted to Trunk Interfaces

Do not configure subtended interfaces for MPLS VPN services. Only trunk interfaces support MPLS VPN mapping of RFC 1483 routed sessions.

MPLS ATM-Label Switch Router Functionality Not Supported

DSLAMs are not meant for use as MPLS ATM-Label Switch Routers (ATM-LSRs). When designing your network, keep in mind that DSLAMs act only as Label Edge Routers (LERs).

Performance Restrictions for MPLS VPN Traffic

MPLS VPN-enabled interfaces do not perform as well as switched VCs. Please take this into consideration when deploying MPLS VPNs in your networks.

Restricted MPLS Features

The following MPLS-related features are not part of the MPLS VPN mapping of RFC 1483 routed sessions:

- MPLS traffic engineering
- MPLS multicast

DSL Interface Limitations

In DSLAMs, each DSL interface can support multiple permanent virtual circuits (PVCs), but we recommend that you use one routed MPLS VC if a dynamic routing protocol (such as RIP) is used between the customer equipment and the provider equipment.

MPLS VPN Mapping Not Supported on the Eight-Port IDSL ITU-C Line Card

Routed termination of IDSL connections has not been supported since Cisco IOS Release 12.2(1b)DA.

# Frame Relay PVCs/Soft PVCs on an IDSL Interface

The number of Frame Relay PVCs/Soft PVCs on an IDSL interface is restricted to 1 if you use the default row in a frame-relay connection traffic table (FR-CTT).

When upgrading to Release 12.2(12)DA6 from earlier releases, you must first create a new row in the FR-CTT with the desired CIR value and use the resultant row number during PVC/Soft PVC creation. If you do not create a new row, the second FR PVC/Soft PVC command is not parsed and installed on the IDSL interface.

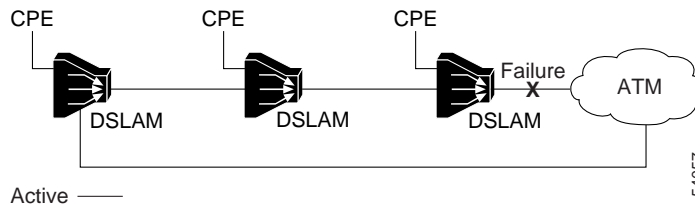# Use of a Ring Topology in a DSLAM Subtend Environment to Achieve ATM Trunk Redundancy

Ring topology is achieved when a node in the subtend tree is attached to the ATM access to provide a physically redundant loop. Thus, when the primary ATM access or one of the ATM trunks in the subtend tree fails, the soft permanent virtual circuits (SPVCs) can be dynamically rerouted through the use of Private Network-Network Interface (PNNI) (Figure 1).

Figure 1   SPVCs Prior to Failure
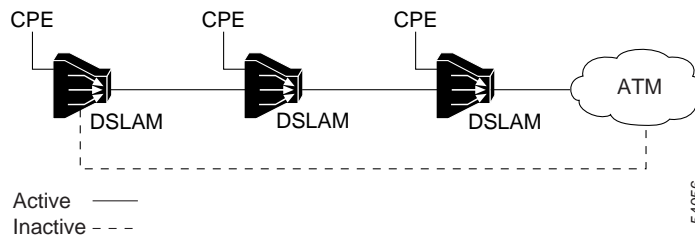
This redundancy requires the use of SPVCs. If you use permanent virtual circuits (PVCs) or permanent virtual paths (PVPs), redundancy cannot be provided. The use of the SPVCs allows traffic to be rerouted around the failed access point, because SPVCs leverage this feature of PNNI. When the failure occurs, the SPVCs are disconnected and dynamically reconnected across the new path (Figure 2).

Figure 2   SPVCs Dynamically Rerouted

Requirements

If you implement ring topology in a DSLAM subtend to achieve ATM trunk redundancy, the following requirements apply:

- You must use SPVCs, PNNI, ATM signaling, and Interim Local Management Interface (ILMI) to enable rerouting. PNNI, ATM signaling, and ILMI are enabled by default. Permanent connections such as PVCs and shaped virtual paths (VPs) do not benefit from the redundant link.

- You must make the redundant link's PNNI administrative weight higher than the PNNI weight of the primary trunk. Once you change the weight of the redundant link, the subtend tree uses this link only if a failure occurs.

Limitations

When the redundant link is active, the following occurrences are problems:

- Loss of subtending fairness.

- Increase in latency as well as an increase in cell delay variation (CDV) between the cells. Delay-sensitive traffic, such as voice and video, or traffic that is susceptible to jitter, such as constant bit rate (CBR) voice, might be compromised. This technique is best realized for unspecified bit rate (UBR) traffic, such as consumer internet access, where no strict quality of service (QoS) objectives are required.

Once the redundant link is active, the following occurrences are potential problems:

- Greater possibility of increased congestion in the DSLAM ATM switch fabric, which might cause loss of data.

- When the main link is restored, there is downtime while the path is being rerouted. After the SPVCs are rerouted to the redundant ATM trunk and the original trunk is repaired or brought back into service, you must manually intervene. You must flap (shut/noshut) the subtend port. Because of retries on the current path, you must keep the trunk down until the maximum retry interval expires.

Cisco DSL Manager

If you are using versions of Cisco DSL Manager (CDM) earlier than CDM Release 3.4—from CDM Release 1.0 to CDM Release 3.3(3)—do not upgrade the DSLAMs to this new Cisco IOS release.

If you use both the CDM network management application and the Cisco IOS command line interface to manage your Cisco DSLAMs, you should be aware of certain configuration and procedural implications. Refer to the *Release Notes for the Cisco DSL Manager, Release 3.4*, for this information.

Important Notes

This section provides important information about Cisco IOS software releases for DSLAMs.

Line Card Features

Table 2 shows which line card features are available on the 4xDMT, 4xFlexi, and 8xDMT line cards.

Table 2   Line Card Features

Feature	4xDMT	4xFlexi	8xDMT
Interleave	yes	yes	yes
Fastpath	no	yes	yes
Min rate blocking	alarm only	yes	yes
SNR margin	alarm only	alarm and retrain capable	alarm and retrain capable
Trellis encoding	no	yes Disable on ADI based CPEs.	yes Ignores profile setting. The line card firmware automatically controls trellis encoding based on the CPE type.
Overhead framing	Mode 0,1,2,3 with ADI based CPE Mode 3 is recommended with other CPE.	Mode 3 only	Mode 3 only
Power Management Additional Margin	no	no	T1.413 G.DMT
Operating mode	T1.413 G.DMT G.Lite Auto	T1.413 G.DMT G.Lite Auto	T1.413 G.DMT G.Lite Auto
Training mode	Quick recommended	No affect	No affect
Cisco 677 CPE support	yes	yes	yes
Cisco 678 CPE support	no	yes	yes
Alcatel-based CPEs	limited performance	yes	yes

NI-2 Card IP Services

During system startup, the following protocol warning messages display. You can ignore these messages.

- If RADIUS is configured:

```
%AAAA-4-SERVUNDEF: The server-group "radius" is not defined. Please define it.
```

- If VPN is configured:

```
% Can't create VRF
```

Soft PVC Address Changes upon Upgrade from Release 12.1(4)DA or Earlier

When you upgrade from Cisco IOS Release 12.1(4)DA or earlier to Release 12.2(12)DA6, the default soft PVC addresses on all interfaces change. This occurs only when you upgrade to Release 12.2(12)DA6 from Release 12.1(4)DA or earlier.

Workarounds:

Reconfigure the soft PVCs associated with all interfaces.

Assign a (nondefault) address to the interfaces.

Configuring Cisco Routers for Use with IDSL

If you wish to use a Cisco router for an IDSL application and the router is running a Cisco IOS release earlier than Release 12.1, you must configure the ISDN switch type. If you do not configure the ISDN switch type on the Cisco router, the router's BRI interface might not come back up after the IDSL line goes down and comes back up.

To prevent this problem from occurring, execute the **isdn switch-type basic-ni** command in global configuration mode on the router.

This problem does not occur if the Cisco router is running Cisco IOS Release 12.1 or later.

Assigning VPI Values to Shaped VP Tunnels

This release supports the full range of VPI values: 0 to 255. However, if you configure VP tunnels with traffic shaping, you can use only 32 VPIs out of that range. If you have not yet assigned any VPIs, all values from 0 to 255 are available. Once you start assigning VPIs, however, the assigned VPIs limit the VPIs that remain. (You assign VPIs using the **atm pvp** or **atm pvc** command.)

After a particular VPI value is assigned to a shaped VP tunnel, every 32nd VPI value above and below the first one is eliminated—that is, the original value modulo 32. For example, if you assign VPI 94 to a shaped VP tunnel, the following VPI values become unavailable for any purpose: 30, 62, 126, 158, 190, and 222.

To avoid problems, choose a block of 32 consecutive VPI values (for example, 0 to 31 or 101 to 132). The software rejects invalid VPI values.

Installing Multiple Cisco 6160 DSLAMs in an Equipment Rack

You can install multiple Cisco 6160 DSLAMs in a Telco equipment rack. A standard 7-foot equipment rack can house four Cisco 6160 DSLAMs, stacked one on top of another. This configuration maximizes the DSL density within a 7-foot rack. However, if space is available or you are interested in using any multiservice capabilities that the DSLAM might support in the future, we recommend that you install no more than three Cisco 6160 DSLAMs in a 7-foot rack. Leave a space of at least 2.5 rack units (4.375 inches, or 11.1 cm) beneath each DSLAM for future cable management use.

Console Logging

Turn console logging off if you plan to reboot the DSLAM. Turn console logging back on after the system comes up. (Console logging is turned on by default.) Use the global configuration commands **no logging console** (to turn the feature off) and **logging console** (to turn it on).

If console logging is on when the system reboots, the large volume of console messages consumes CPU time. As a result, the system comes back up more slowly and line cards might reload repeatedly, causing further delays.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Caveat numbers and brief descriptions are listed in the following tables. For details about a particular caveat and for information on caveats in previous Cisco IOS releases that also apply to this release, go to Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

To access this location, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://tools.cisco.com/RPF/register/register.do and follow the directions to set up an account.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats for a release. To reach Bug Navigator II, go to Cisco.com and click **Login**. Then go to **Software Center > Cisco IOS Software > Cisco Bugtool Navigator II**. Alternatively, you can go to:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.2. It is located on Cisco.com and the Documentation CD-ROM.

Resolved Caveats—Release 12.2(12)DA6

Table 3 lists the caveats resolved in Cisco IOS Release 12.2(12)DA6.

Table 3   Resolved Caveats in Cisco IOS Release 12.2(12)DA6

Caveat Number	Description
CSCdu53656	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCea28131	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCed74869	PVC created between two modem ports with each VC having different VPI/VCI values fails to pass traffic on the Enhanced NI2
CSCec80792	ATUC-8-DMT-1 (8xDMT) may have ATM port stuck in TRAINED state even though CPE is powered off/on
CSCed16832	Unable to establish new SVC's and Soft-VC's and the existing SVC's and Soft-VCs go down
CSCec74259	When executing: 'show atm vc conn-type soft-vc' continuously on the NI2 it could reload due to a bus error
CSCed66096	Repeated occurences of "%SMB-5-LENGTH_MISMATCH" messages may be seen on the NI2 console. This message is cosmetic only and does not describe an errored condition.
CSCec28330	SLOT-3-MODULE_DETECTED, SLOT-3-MODULE_MISSING, SMB-3-GETBUFFER_FAILED, SMB-5-CRC_ERROR, SMB-5-LENGTH_MISMATCH, SUNI_DUAL-3-LAIS system error messages undocumented.
CSCec27902	IMA_LINK-3-LCD system error message is undocumented.
CSCed27956	TCP checks should verify ack sequence number.
CSCed38527	TCP checks should verify syn sequence number.

Resolved Caveats—Release 12.2(12)DA5

Table 4 lists the caveats resolved in Cisco IOS Release 12.2(12)DA5.

Table 4   Resolved Caveats in Cisco IOS Release 12.2(12)DA5

Caveat Number	Description
CSCec39510	The interface configuration command "loopback diagnostic" is not operating correctly on certain DMT linecards.
CSCec16669	For some interfaces, the value of *ceAssetAlias* is null.
CSCeb60539	Frequent SVC deletion and recreation can lead to an I/O memory leak.

Resolved Caveats—Release 12.2(12)DA4

Table 5 lists the caveats resolved in Cisco IOS Release 12.2(12)DA4.

Table 5   Resolved Caveats in Cisco IOS Release 12.2(12)DA4

Caveat Number	Description
CSCea50015	A spurious warning message, "error: source idb not set", could be occasionally noticed while exiting IOS parser submode "config-if-atm-vc", if the PVC is deleted concurrently from an another user session.
CSCea72903	HEC errors per DSL interface are now shown under the corresponding input errors (ifInErrors) and output errors (IfOutErrors) in the IF-MIB.
CSCea79586	F4 end-to-end OAM cells may cause IO memory leak in certain situations.
CSCeb41246	NI2 show version Displays Incorrect CPU Information.
CSCeb45922	SNR alarms inserted and cleared when a interface is down and up.
CSCeb48534	ATM IMA interface counters are zero for both SNMP and "show interface" queries.
CSCeb61425	L2TP tunnel not established when domain is not specified.
CSCec08956	IDPROM FIELD FORMAT ERROR received for 8xDMT Annex A and B in the output of "show hardware slot x" command.

Resolved Caveats—Release 12.2(12)DA3

Table 6 lists the caveats resolved in Cisco IOS Release 12.2(12)DA3.

Table 6   Resolved Caveats in Cisco IOS Release 12.2(12)DA3

Caveat Number	Description
CSCeb40433	This DDTS has been created to track improvements in IP processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb40433.

Resolved Caveats—Release 12.2(12)DA2

Table 7 lists the caveats resolved in Cisco IOS Release 12.2(12)DA2.

Table 7   Resolved Caveats in Cisco IOS Release 12.2(12)DA2

Caveat Number	Description
CSCea14476	*crossInterface* can be seen correctly using CLI, but when using SNMP... *crossIfIndex* (1) is reported being the main interface (ATM0/1) instead of the logical interface (ATM0/1.1), ifIndex 187.
CSCdz89525	TraceBacks when trying to set *ciscoAtmIfIlmiAutoConfiguration*. Spurious accesses appear when configuring new customers.
CSCea50123	Ftp sessions on NI2 will abort the file transfers occasionally without any error messages or notifications to the user.
CSCdz65235	For 12.2(10) image, in 6015, traceback comes while rebooting the DSLAM and trying to initialize the interface. But it is not seen in any DSLAM other than 6015. This traceback does not appear in versions prior to 12.2(10).
CSCin37508	A mismatch between the customer cpe train status and the modem train status on the 8xDMT linecard of a DSLAM occurs sporadically.

Resolved Caveats—Release 12.2(12)DA1

Table 8 lists the caveats resolved in Cisco IOS Release 12.2(12)DA1.

Table 8   Resolved Caveats in Cisco IOS Release 12.2(12)DA1

Caveat Number	Description
CSCdz19438	A DSLAM reload no longer causes the SHDSL target margin in a DSL profile to be reset to 2 dB when adaptive rate is used.
CSCdz27867	Heavy traffic through the SAR chipset IDT77V252 no longer causes cell corruption in the Tx path. This problem previously occurred on NI-2 cards with the product numbers NI-2-DS3-T1E1 and NI-2-DS3-T1E1-H.
CSCdz45198	Issuing the **no slot** command in PVC submode now works correctly. Previously, concurrency issues caused the DSLAM to reload when the command was issued while another user session was active in PVC submode.

Resolved Caveats—Release 12.2(12)DA

Table 9 lists the caveats resolved in Cisco IOS Release 12.2(12)DA.

Table 9   Caveats Resolved in Cisco IOS Release 12.2(12)DA

Caveat Number	Description
CSCea38684	FTP fails with the traceback: SYS-2-LINEPROCDEAD: Killing process.
CSCdx60278	Clearing the interface counters on a Cisco 6260 DSLAM now works correctly. Previously, the counters might not have been cleared and could instead show high input and cyclic redundancy check (CRC) errors.
CSCdz05530	On an OC-3 interface, the **show interface** command "packets output" count does not match the **show controller** command "cells transmitted" count, but both should be the same. **Workaround:** None.
CSCdx92465	The **show dsl interface atm** command now shows the correct value for the Last Change field for G.SHDSL ports. Previously, if the system clock value was altered after the G.SHDSL port trained, this field might show an erroneous value.
CSCdy21341	Issuing the **clear counters** command on an OC-3 interface no longer causes SNMP to incorrectly show ifTable counters equal to 0.
CSCdy22386	SNMP now checks to ensure that you specify a valid value for Upstream Checkbytes on a DSL profile. Previously, SNMP allowed you to specify any value for cAdslAturDmtConfInterleaveFecSize (CISCO-ADSL-DMT-LINE-MIB), even though valid values are 0 through 16, in multiples of 2.
CSCdy70396	The 8xDMTISDN line card no longer drops the connection after it trains with a Cisco 826 CPE when the line card's downstream bit rate is less than 5504 kilobits per second (kbps). Previously, this problem caused constant link flapping.

Related Documentation

The software described in these release notes runs on several Cisco NI-2 DSLAM platforms, including the Cisco 6015, Cisco 6160, and Cisco 6260 DSLAMs.

A complete list of all DSL hardware product related documentation is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/index.htm

A complete list of all DSL Cisco IOS product related documentation is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/index.htm

In the Cisco ATM software manuals, look for information pertaining to the LightStream 1010, which uses the same software base as the Cisco NI-2 DSLAMs. ATM manuals are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/atm/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

    http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Step 1 All other trademarks mentioned in this document or Web site 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. (0304R)