Release Notes for Cisco IOS Release 12.2(10)DA9 for Cisco DSLAMs with NI-2

September 23, 2008

These release notes describe features and caveats in Cisco IOS Release 12.2(10)DA9 for the Cisco 6015, Cisco 6160, and Cisco 6260 digital subscriber line access multiplexers (DSLAMs).

Note When you upgrade from Cisco IOS 12.1(5)DA2 or earlier images on the NI-2 card to Release 12.2(10)DA9, you must format the bootflash on the NI-2 card before loading the 12.2(10)DA9 dboot image. See the "Update the Image in Bootflash to the 12.2(10)DA9 dboot Image" section on page 4.

For pointers to more information about the Cisco 6015, Cisco 6160, Cisco 6260, and their software, refer to the "Related Documentation" section on page 19. To learn more about caveats, visit the Cisco web site—see the "Obtaining Documentation" section on page 19 for details. Information about electronic documentation can be found in both the "Obtaining Documentation" section on page 19 and the "Documentation CD-ROM" section on page 20.

Contents

This document contains the following topics:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

Cisco IOS Release 12.2(10)DA9 runs on these DSLAM systems:

- Cisco 6015
- Cisco 6160
- Cisco 6260

New and Changed Information

The following sections provide new and changed information for Cisco IOS Release 12.2(10)DA9, 12.2(10)DA8, 12.2(10)DA7, 12.2(10)DA6, 12.2(10)DA5, 12.2(10)DA4, 12.2(10)DA3, 12.2(10)DA2, and 12.2(10)DA.

Cisco IOS Release 12.2(10)DA9

Cisco IOS Release 12.2(10)DA9 is based on Cisco IOS Release 12.2(10)DA8 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(10)DA9" section on page 14.

New Hardware Features in Release 12.2(10)DA9

No new hardware features were introduced in Cisco IOS Release 12.2(10)DA9.

New Software Features in Release 12.2(10)DA

The following new software features were introduced in Cisco IOS Release 12.2(10)DA. No new features were introduced in Release 12.2(10)DA9.

DMT Power-Management–Additional-Margin

The 8xDMT line card can run in power-management mode in the G.dmt or the T1.413 mode. The resulting power cutback produces a reduction in power dissipation and crosstalk. Only 8xDMT line cards support power management. All CPE may not support the DSL functionality for power management to function correctly. Check with a Cisco customer representative to verify CPE compatibility with the 8xDMT power management.

You control the Power Management feature by issuing a **dmt power-management-additional-margin** command inside a profile and assigning that profile to a line card interface. This IOS command allows you to set the additional margin for each channel from 0 dB (off) to 15 dB. This sets the additional margin that will be added to the target margin. If the sum of the target margin and additional margin exceeds 15dB, it is capped at 15dB. If the actual margin of the line is higher than the sum of the configured target and additional margin, and all the above conditions are met, then power management attempts to reduce the actual margin, and as a consequence the power level as well.

Not all CPE support power management. If you connect an unsupported CPE to a port on which power management is turned on, you will not see a reduction in the actual margin or power level. The operating modes supported by power management are T1.413and g-992-1 (G.DMT). Table 1 shows the CPE and specifies which operating mode supports them.

Table 1 CPEs and Power Management Support

CPE	G.DMT	T1.413
Cisco 677	not supported	not supported
Cisco 678	not supported	supported
Cisco SOHO 77/Cisco 827	supported	supported
ADSL WAN Interface Card (WIC)	supported	supported
Alcatel chipset based modem	supported	supported

A reduction in the power level occurs if there is excess margin on the line. For the downstream direction, if there is excess margin, then IOS displays a reduction in margin for the modes listed above, and a reduction in transmit power for T1.413 mode. For the upstream direction, if there is excess margin, then IOS displays a reduction in the margin for g-992-1 mode only. IOS will not display a reduction in transmit power for the upstream direction.

ATM OAM Cells Supported in Fast Path Mode

The NI-2 now supports atm oam cells through fast path mode. Also, you can now use the **ping atm** utility command in fast path mode.

Enhanced ATM OAM Segment Cells Support

A new command, **atm oam intercept segment**, allows you to enable or disable receiving atm oam segment cells on valid connections. By default, the atm oam cells received on unconfigured or down connections are dropped. For more information, see the *Command Reference for Cisco DSLAMs with NI-2*.

MIB Object Changes

This release contains changes to the following Management Information Base (MIB) objects:

The power management feature is configurable via the CISCO-ADSL-DMT-LINE-MIB. The mib object cAdslAtucDmtConfPMAddSnrMgn configures the downstream component and the mib object cAdslAturDmtConfPMAddSnrMgn configures the upstream component on that particular dsl profile. Both objects default to 0 and can be configured from 0 to 150 tenths of dBs in increments of 10. Setting the objects to 0 explicitly via SNMP will disable the power management feature on the ports.

Installation Notes

Update the Image in Bootflash to the 12.2(10)DA9 dboot Image

When you upgrade from Cisco IOS Release 12.1(5)DA2 or earlier images on the NI-2 card to Release 12.2(10)DA9, you must reformat the bootflash on the NI-2 card.

Note If you are upgrading from Cisco IOS Release 12.1(6)DA, 12.1(6)DA2, 12.1(7)DA, 12.1(7)DA2, 12.1(7)DA3, 12.2(1b)DA, 12.2(1b)DA1, 12.2(5)DA, 12.2(5)DA1, 12.2(7)DA, 12.2(10)DA, 12.2(10)DA1, 12.2(10)DA2, 12.2(10)DA3, 12.2(10)DA4, 12.2(10)DA5, 12.2(10)DA6, 12.2(10)DA7, or 12.2(10)DA8, 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 highly 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 update the boot image, perform the following steps in privileged EXEC mode:

	Command	Purpose
Step 1	`DSLAM# dir bootflash:`	Verify that the bootflash image is **ni2-dboot-mz.121-5.DA9** or **ni2-dboot-mz.121-4.da**. If it is neither, go to the "Upgrade the Bootflash Image on the NI-2 Card to the 12.1(5)DA2 dboot Image" section on page 5 and perform the instructions there, and then return to this step. This is required because of a problem (CSCdr89374) in old bootflash images.
Step 2	`DSLAM# dir flash:`	Display the name of the Flash file that begins **ni2-** and use it as *filename* in Step 3.
Step 3	`DSLAM# delete flash:`*filename*	Delete the Flash file name found in Step 2. Repeat Step 2 and Step 3 until all files in the Flash file have been deleted.
Step 4	`DSLAM# squeeze flash:`	Recover available space in Flash memory.
Step 5	`DSLAM# copy tftp://`*tftpserver*`:TFTPBOOT/ni2-dsl-mz.122-10.DA9 flash:`	Copy the Cisco IOS image from a TFTP server to Flash.

Step 6	`DSLAM# configure terminal`
	`DSLAM (config)# no boot system`
	`DSLAM (config)# boot system flash:ni2-dsl-mz.122-10.DA9`
	`DSLAM# end`
		Enter global configuration mode.
		Disable the boot from system.
		Specify the name of the system image to load at startup.
		End global configuration mode.

Step 7	`DSLAM# copy running-config startup-config`	Save your changes to the startup configuration.
Step 8	`DSLAM# reload`	Reload the system to upgrade the image.

	Command	Purpose
Step 9	`DSLAM# show version`	Confirm that the running image is **ni2-dsl-mz.122-10.DA9**. If it is not, go to Step 5.
Step 10	`DSLAM# format bootflash:`	Erase all information in bootflash memory. Answer **y** to all confirm questions. When the DSLAM returns you 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 11	`DSLAM# copy tftp://`*tftpserver*`:TFTPBOOT/ni2-dboot-mz.122-10.DA9 bootflash:`	Copy the boot image from a TFTP server to the bootflash.
Step 12	`DSLAM# reload`	Reload the system to upgrade the image.

Upgrade the Bootflash Image on the NI-2 Card to the 12.1(5)DA2 dboot Image

When you upgrade from Release 12.1(3)DA or earlier images on the NI-2 card to Release 12.1(5)DA2, 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, perform the following steps:

	Command	Purpose

Step 1	`DSLAM> enable`
	`Password: <password>`
	`DSLAM#`
		Enter enable mode.
		Enter the password.
		You have entered enable mode when the prompt changes to 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.da2 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.
Step 6	`DSLAM# configure terminal`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `DSLAM(config)#`.
Step 7	`DSLAM(config)# config-register 0`	Set the config register to 0x0000 so that the NI-2 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.

	Command	Purpose
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 boots, it uses **ni2-dboot-mz.121-5da.bin** as the bootstrap image.
Step 15	`DSLAM# configure terminal`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `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 "Update the Image in Bootflash to the 12.2(10)DA9 dboot Image" section on page 4.

Limitations and Restrictions

This section describes the limitations and restrictions for Cisco IOS DSLAM releases.

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 coding, 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, the effect of having trellis coding, 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 will still have 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 customer premises equipment (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 in Asynchronous Transfer Mode (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 Coding Enable Default Recommendations

Trellis coding is disabled by default on the NI-2 because it is not supported on the 4xDMT (ATUC-1-4DM) card. However, trellis coding is supported on the 4xFlexiDMT (ATUC-4FLEXIDMT) and 8xDMT (ATUC-1-DMT8) line cards. Additionally, trellis coding should be enabled for the 4xFlexiDMT and 8xDMT line cards.

For all 4xDMT (ATUC-1-4DMT) ports in the DSLAM, make sure that trellis coding is disabled in the dsl-profile for those ports. For all 4xFlexiDMT and 8xDMT ports in the DSLAM, make sure that trellis coding is enabled except with ADI chipset based CPE using ADI F/W prior to ADI 3.1. This includes all Cisco 677 and Cisco 627 CPEs.

See the documentation at the following location for details on the commands used to change trellis coding settings on the NI-2:

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

Restrictions on NI-2 IP Services

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

Restricted Layer 3 Services

Cisco IOS Release 12.2(10)DA does 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 use of 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 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 CE and the PE.

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

Routed termination of IDSL connections is not 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(10)DA9 from previous 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). See 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. See 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) before 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. Please 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 DSLAM releases.

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 CPE.	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
677 CPE support	yes	yes	yes
678 CPE support	no	yes	yes
Alcatel-based CPE	limited performance	yes	yes

NI-2 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(10)DA9, the default soft PVC addresses on all interfaces change. This occurs only when you upgrade to Release 12.2(10)DA9 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 prior to 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 Chassis in an Equipment Rack

You can install multiple Cisco 6160 chassis in a telco equipment rack. A standard 7-foot equipment rack can house four Cisco 6160 chassis, stacked one on top of another. This configuration maximizes the DSL density within a 7-foot rack. However, if space is available or if you are interested in using multiservice capabilities that the chassis will support in the future, we recommend that you install no more than three Cisco 6160 chassis within a 7-foot rack. Leave a space of at least 2.5 rack units (4.375 inches, or 11.1 cm) beneath each chassis 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. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included here.

This section contains only open, closed, and resolved caveats for the current Cisco IOS release.

Caveat numbers and brief descriptions are listed in Table 3, Table 4, Table 5, Table 6, Table 7, Table 8, Table 9, Table 10, Table 11, Table 12, and Table 13. 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://www.cisco.com/register 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 of any severity for any 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

This software release is based on Cisco IOS Release 12.2. 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(10)DA9

Table 3 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA9.

Table 3 Resolved Caveats in Cisco IOS Release 12.2(10)DA9

Caveat Number	Description
CSCsj98957	Traceback observed on DSLAM with fair queue and ima version 1.1 commands
CSCsk34240	ALIGN traceback appears with PVP delete
CSCsd95616	Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

Resolved Caveats—Release 12.2(10)DA8

Table 4 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA8.

Table 4 Resolved Caveats in Cisco IOS Release 12.2(10)DA8

Caveat Number	Description
CSCsj44081	Improvements in diagnostics and instrumentation
CSCsb28407	IP Protocol 54 (NHRP) appears open without configuration
CSCin95836	NHRP does not handle error conditions gracefully

Resolved Caveats—Release 12.2(10)DA7

Table 5 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA7.

Table 5 Resolved Caveats in Cisco IOS Release 12.2(10)DA7

Caveat Number	Description
CSCed09685	IOS should not send passwords and sensitive information to ACS logs
CSCse04560	tftp-server allows for information disclosure
CSCsc64976	HTTP server should scrub embedded HTML tags from cmd output
CSCsg70355	Adopt new default summer-time rules from Energy Policy Act of 2005
CSCse05736	A router running RCP can be reloaded with a specific packet
CSCsg40567	Memory leak found with malformed tls/ssl packets in http core process(AP)
CSCdz65235	6015 emits traceback during system init

Resolved Caveats—Release 12.2(10)DA6

Table 6 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA6.

Table 6 Resolved Caveats in Cisco IOS Release 12.2(10)DA6

Caveat Number	Description
CSCsf07847	CDP may fail to discover neighbor information in releases wh CSCse85200
CSCse85200	Inadequate validation of TLV's in CDP

Resolved Caveats—Release 12.2(10)DA5

Table 7 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA5.

Table 7 Resolved Caveats in Cisco IOS Release 12.2(10)DA5

Caveat Number	Description
CSCei62762	GRE: IP GRE Tunnel packet with Routing Present Bit is not dropped.

Resolved Caveats—Release 12.2(10)DA4

Table 8 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA4.

Table 8 Resolved Caveats in Cisco IOS Release 12.2(10)DA4

Caveat Number	Description
CSCef46191	Unable to telnet
CSCeg15044	Not able to telnet to card (No Free TTYs error)
CSCdx69995	BGP: insufficient chunk messages with many VPN routes
CSCeh13489	BGP shouldn't propagate an update with excessive AS Path >255

Resolved Caveats—Release 12.2(10)DA3

Table 9 lists the caveats that have been resolved in Cisco IOS Release 12.2(10)DA3.

Table 9 Resolved Caveats in Cisco IOS Release 12.2(10)DA3

Caveat Number	Description
CSCed38527	TCP checks should verify syn sequence number
CSCed27956	TCP checks should verify ack sequence number
CSCeb56909	Crafted packet causes reload on Cisco routers
CSCec86420	Undebug all stops traffic with IPsec+GRE+CEF
CSCea28131	Router crashes upon rcv invalid packet
CSCdu53656	Router crashes on receiving malformed packet

Table 9 Resolved Caveats in Cisco IOS Release 12.2(10)DA3 (continued)

Caveat Number	Description
CSCee43765	Enhancement on the crashinfo file
CSCee43760	Exception Memory Minimum command for I/O
CSCeb16876	Bad getbuffer, crash, tag input, fragmentation
CSCdx92043	IOS accepts wrong ICMP redirects
CSCed40563	Malicious cfg reload neighbor routers by <show cdp entry * protocol>
CSCin67568	Memory leak in CDP process with long host names
CSCdz32659	%SYS-2-MALLOCFAIL: -Process= CDP Protocol
CSCec25430	IOS may reload from specific packet
CSCed78149	TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts
CSCef44699	GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets
CSCef60659	More stringent checks required for ICMP unreachables
CSCee67450	BGP error msg traceback

Resolved Caveats—Release 12.2(10)DA2

Table 10 lists the caveats that have been resolved in Cisco IOS Release 12.2(12)DA2.

Table 10 Resolved Caveats in Cisco IOS Release 12.2(10)DA2

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.

Open Caveats—Release 12.2(10)DA1

All the caveats listed in Table 11 are open in Cisco IOS Release 12.2(10)DA1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 11 Open Caveats for Cisco IOS Release 12.2(10)DA1

Caveat Number	Description
CSCdx53819	8xDMT cards with interleaving delay configurations of 2000us and below have problems holding train and/or having less than expected upstream train rates. **Workaround:** Avoid interleaving delay values of 2000us and below with 8xDMT cards. Interleaving mode configurations should use 4000us delay or above. If lower delays are required, Fastpath mode can be used if supported by CPE being used.
CSCdx57259	The connection between the modem on a 4xDMT line card and the CPE is lost when an NI-2 redundancy switchover occurs. **Workaround:** None.

Table 11 Open Caveats for Cisco IOS Release 12.2(10)DA1

Caveat Number	Description
CSCdx67720	When you copy a configuration file from a tftp server to the startup_config through snmp, ccCopyState (CISCO-CONFIG-COPY-MIB) will be in "running" state ever after. It will not change to "Failed" state. The **show startup** command displays the following output: %% Non-volatile configuration memory is being accessed, Try again **Workaround**: Make sure that there is enough space available in the nvram before copying, using snmp or use cli.
CSCdx84898	Upgrades from Cisco IOS 12.1(7) DA to newer IOS images cause G.SHDSL ports to occasionally drop and retrain. The error is listed as LOSQ (Loss of Signal Quality) due to CRC errors detected or LOS when Loss of Frame Sync. is detected. **Workaround:** Newer versions of G.SHDSL firmware have been adjusted to meet the ratified standards. This may require some fixed-rate loops to not hold train at the current configured rate used with Cisco IOS 12.1.(7)DA. Reducing the configured rate in some cases will resolve the issue. Random drops may still occur on some ports.
CSCea56851	3db downstream margin configured ports on 8xDMT do not achieve max configured downstream rate on loops that should achieve max configured downstream rate. **Workaround:** Use of DSL's recommended 6db downstream margin will achieve max configured rate on loops expected to achieve max rate.

Resolved Caveats—Release 12.2(10)DA1

Table 12 lists the caveats that have been resolved in Cisco IOS Release 12.2(12)DA1.

Table 12 Resolved Caveats in Cisco IOS Release 12.2(10)DA1

Caveat Number	Description
CSCea38684	FTP fails with the traceback: SYS-2-LINEPROCDEAD: Killing process
CSCea50123	Ftp sessions on NI2 will abort the file transfers occasionally without any error messages or notifications to the user.

Resolved Caveats—Release 12.2(10)DA

The problems listed in Table 13 are fixed in Cisco IOS Release 12.2(10)DA.

Table 13 Caveats Resolved in Cisco IOS Release 12.2(10)DA

Caveat Number	Description
CSCdp00996	Periodically, the system generates a serial management bus cyclic redundancy check (SMBCRC) error message such as this: %NI2-5-LC_NOTICE:Slot[15] SMBCRC (1 days, 3 hours, 37 minutes, 6 seconds) These messages are informational only and do not affect performance.
CSCdu04045	The entry for the atmSoftPVccRetryThreshold feature has an incorrect default value of 0, rather than the default value of 1 that is shown in the ATM Soft PVC Management Information Base (MIB). A value of zero indicates that an infinite number of call attempts are required to increment the atmSoftPvcCallFailures object and thus disables alarms for the Soft PVCC.
CSCdu40049	Adding and deleting a profile from different sessions (for example, in two telnet sessions, one user is adding while at the same time another is deleting the same profile) has the potential of causing an unexpected system reload.
CSCdu42394	The ceAssetTag cannot be set for 8xDMT and SHDSL line cards.
CSCdv56813	Following a redundancy switchover, the standby card may reload twice before reaching the STANDBY-READY state. Once the standby is in the STANDBY-READY state it will not continue to reload.
CSCdv73591	Some VCs (PVCs/PVPs/Soft PVCs/Soft PVPs) are missing on reload even when they are stored in the startup configuration. This problem occurs if you create VC's by using internal CTT rows that do not appear in the **show running-config** command but do appear in the **show atm connection-traffic-table** command.
CSCdw53009	When you configure the ATUC-1-4DMT line card for loopback diagnostic, cells are dropped by the interface.
CSCdw67176	The commands **no tag-switching ip** and **tag-switching ip** from the global configuration mode remove the **tag-switching atm vp-tunnel 13 vci-range 33-65535** line on the sub interfaces.
CSCdw73531	Not all IMA group/link alarms are shown in the event browser.
CSCdw87272	If you try to enable tag-switching ip, the following message is returned: %VP-tunnel vpi is not free for Tag-switching.
CSCdw91698	The NI-2 does not support OAM F5 seg-loopback cells, in the fast path.
CSCdx16449	PNNI fails to establish a connection. The **show atm controller atm 0/0** command displays a status of C.
CSCdx19656	Unable to train with 3Com OCR-810. With the 4xDMT line card, the CPE had a number of line errors or fails to train with 12.2(7)DA. Trellis coding is enabled in the DSL profile.
CSCdx34262	When you change the operation of the linecard from ATUC-1-DMT8 to STUC-8-TCPAM, the indexes appear in the incorrect order.
CSCdx43027	System hangs indefinitely after provisioning/unprovisioning slots.

Table 13 Caveats Resolved in Cisco IOS Release 12.2(10)DA (continued)

Caveat Number	Description
CSCdx64312	In Cisco IOS images 12.2(7)DA, the value of the "Microseconds handling network interrupts" is not saved correctly to the NVRAM when configured via the **scheduler allocate** exec command.
CSCdx65171	The NI-2 unexpectedly reloads when you try to clear a card mismatch from CLI using the command **no slot** x, where x is the slot number.
CSCdy02467	Adtran CPE do not train with the Cisco 6260 running Cisco IOS 12.2(7)DA.

Related Documentation

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

Hardware Documentation

A complete list of all DSL hardware product related documentation is available on the World Wide Web at

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

Software Documentation

A complete list of all DSL Cisco IOS product related documentation is available on the World Wide Web at

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 NI-2 DSLAMs. ATM manuals are on the World Wide Web at

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

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package that ships with your product. The Documentation CD-ROM is updated monthly and is available as a single unit or through an annual subscription.

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order the Documentation CD-ROM through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).
- For assistance with ordering, contact your distributor or see the Cisco Technical Assistance Center website at:

  http://www.cisco.com/tac

Documentation Feedback

If you are a registered Cisco.com user, you can submit technical comments electronically.

- To report problems, click **Feedback** in the toolbar at the top of any document web page and select Report a Problem. Under Problem Type, select **CD/Online Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

- To send your opinion of the DSL documentation, go to the following URL:

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

  and click **here** at the top of the page in the sentence “Is this Cisco documentation helpful? Click here to give us your feedback.” This produces a Documentation Survey that you can complete and send to Cisco electronically.

To submit your comments by mail, write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.