



# Release Notes for the Cisco IAD2430 Series Integrated Access Devices for Cisco IOS Release 12.3(4)XD

---

April 12, 2005

Cisco IOS Release 12.3(4)XD4

OL-5172-01 Rev. C1

These release notes for the Cisco IAD2430 Series Integrated Access Devices (IAD) describe the product-related enhancements provided in Cisco IOS Release 12.3(4)XD4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(4)XD4, see “[Caveats](#)” section on [page 11](#). See also *Caveats for Cisco IOS Release 12.3 T*, which is updated for every maintenance release and is located on [Cisco.com](#) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.3 T* located on [Cisco.com](#) and the Documentation CD-ROM.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at [http://www.cisco.com/warp/customer/tech\\_tips/index/fn.html](http://www.cisco.com/warp/customer/tech_tips/index/fn.html). If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).

## Contents

These release notes describe the following topics:

- [Inheritance Information, page 2](#)
- [Introduction, page 2](#)
- [Early Deployment Releases, page 4](#)
- [System Requirements, page 5](#)
- [New and Changed Information, page 8](#)
- [Limitations and Restrictions, page 10](#)



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

OL-5172-01 Rev. C1

Copyright © 2004 - 2005. Cisco Systems, Inc. All rights reserved.

- [Current MIBs, page 10](#)
- [Field Notices and Bulletins, page 11](#)
- [Caveats, page 11](#)

## Inheritance Information

Cisco IOS Release 12.3(4)XD4, an early deployment release, is based on Cisco IOS Release 12.3(4)T, which in turn is based on Cisco IOS Release 12.3. Cisco IOS Release 12.3(4)T is the first early deployment maintenance release of Cisco IOS Release 12.3 T and is based on the mainline Cisco IOS Release 12.3. Refer to [Table 1](#) for more information.

All features in Cisco IOS Release 12.3(4)T are in Cisco IOS Release 12.3(4)XD4.

**Table 1** *References for the Cross-Platform Release Notes for Cisco IOS Release 12.3 T and Cisco IOS Release 12.3(4)T*

Topic	Location
<ul style="list-style-type: none"> <li>• Determining the Software Version</li> <li>• Upgrading to a New Software Release</li> </ul>	To view information about the topics in the left-hand column, click <b>Cross-Platform System Requirements</b> at: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123reqs.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123reqs.htm</a>
<ul style="list-style-type: none"> <li>• New and Changed Information (Feature Descriptions)</li> <li>• MIBs</li> <li>• Important Notes</li> </ul>	To view information about the topics in the left-hand column. For Cisco IOS Release 12.3 T, go to: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123newf.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123newf.htm</a> Scroll down and click <b>New Software Features in Cisco IOS Release 12.3(4)T</b> , or <b>MIBs</b> , or <b>Important Notes</b> .
<ul style="list-style-type: none"> <li>• Related Documentation</li> <li>• Obtaining Documentation</li> <li>• Obtaining Technical Assistance</li> </ul>	To view information about the topics in the left-hand column, go to: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123docs.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123docs.htm</a>

## Introduction

Cisco IOS Release 12.3(4)XD4 supports the Cisco IAD2430 series IAD.

The Cisco IAD2430 is the next generation integrated voice and data services platform for Service Providers, building on the industry leading Cisco IAD2420 series IAD. The Cisco IAD2430 series offers a major leap forward in price performance and enhanced software functionality such as MGCP SRST used to accelerate the migration from time division multiplexing (TDM) to VoIP cost efficiently. The Cisco IAD2430 series harnesses the maturity of the Cisco IAD2420 series software and enhances functionality by providing more capabilities such as denser interfaces (up to 24 FXS and up to 2 voice or 2 data T1s), encryption, and DC power back up while maintaining it's 1RU form factor for space saving Service Provider Managed Services deployment.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.3(4)XD4, see [New and Changed Information, page 8](#).

## Cisco 2430 Series Integrated Access Device

The Cisco IAD2430 Series Integrated Access Device consists of the following five models:

- Cisco 2430-24FXS IAD
- Cisco 2431-8FXS IAD
- Cisco 2431-16FXS IAD
- Cisco 2431-1T1E1 IAD
- Cisco 2432-24FXS IAD

The supported WAN interface cards (WICs) and Voice Interface Cards (VICs) are:

- VIC2-2FXO
- VIC2-2FXS
- VIC-4FXS/DID
- VIC2-2BRI-NT/TE
- WIC-1T
- WIC-1ADSL
- WIC-1SHDSL
- WIC-1ADSL-DG
- WIC-1SHDSL-V2
- VWIC-2MFT-T1
- VWIC-2MFT-E1

## Port Numbering

Port numbering conventions for the Cisco IAD2430 Series Integrated Access Device differs from the Cisco IAD2420 Series Integrated Access Device:

- An external compact flash card is numbered slot 0.
- 10/100Base-T Fast Ethernet ports are numbered Fast Ethernet 0/0 and Fast Ethernet 0/1 from right to left.
- T1/E1 ports are numbered T1 or E1 1/0 and T1 or E1 1/1 from right to left.
- The slot for WICs and VICs is numbered slot 0. WIC and VIC interfaces are numbered by interface face with this slot number and an interface number, beginning with 0 and running from right to left.
- FXS voice port numbering begins at 2/0 and extends to 2/7, 2/15, or 2/23, depending on the number of voice ports.

## MGCP Endpoint Naming Convention

The Media Gateway Control Protocol (MGCP) endpoint naming convention for Cisco IAD2430 Series IAD differs from the Cisco IAD2420 Series IAD. The MGCP naming convention for the Cisco IAD2430 Series IAD is the following:

**Cisco IAD2431-1T1E1**

S1/DS1-0/1@iad2430-digital  
 S1/DS1-0/2@iad2430-digital  
 ...  
 S1/DS1-0/24@iad2430-digital  
 S1/DS1-1/1@iad2430-digital  
 S1/DS1-1/2@iad2430-digital  
 ...  
 S1/DS1-1/24@iad2430-digital

**Cisco IAD2430-24FXS, IAD2431-8FXS, IAD2431-16FXS, IAD2432-24FXS**

AALN/S2/0@iad2430-analog  
 AALN/S2/1@iad2430-analog  
 ...  
 AALN/S2/23@iad2430-analog

**Voice Analog Ports**

AALN/S0/0@iad2430-analog  
 AALN/S0/1@iad2430-analog  
 AALN/S0/2@iad2430-analog  
 AALN/S0/3@iad2430-analog

# Early Deployment Releases

These release notes describe Cisco IOS Release 12.3(4)XD4 for the Cisco IAD2430 series IAD. Cisco IOS Release 12.3(4)XD4 is an early deployment (ED) release based on Release 12.3(4)T, which in turn is based on Cisco IOS Release 12.3. Early deployment releases contain fixes to software caveats as well as support for new Cisco hardware and software features. Feature support is cumulative from release to release, unless otherwise noted.

Table 2 lists new features supported by the Cisco IAD2430 series IAD in Cisco IOS Release 12.3(4)XD4. See “[Related Documentation](#)” section on page 2 for a list of the documentation specific to the Cisco IAD2430 series IAD.

**Table 2** Early Deployment Release New Features for the Cisco VG224 Analog Gateway

ED Release	Additional Software Features <sup>1</sup> and MIBs <sup>2</sup>	Additional Hardware	Hardware Availability
Cisco IOS Release 12.3(4)XD4	None	None	None
Cisco IOS Release 12.3(4)XD3	None	None	None
Cisco IOS Release 12.3(4)XD2	None	None	None
Cisco IOS Release 12.3(4)XD1	None	None	None

**Table 2** Early Deployment Release New Features for the Cisco VG224 Analog Gateway

ED Release	Additional Software Features <sup>1</sup> and MIBs <sup>2</sup>	Additional Hardware	Hardware Availability
Cisco IOS Release 12.3(4)XD	<a href="#">E1 Support on Cisco 2430 Series IAD</a> <a href="#">Configuring Network Clock</a> <a href="#">Configuring T1/E1 Interfaces</a> <a href="#">Configuring ATM-T1-WAN Ports</a>	None	Now

1. Only major features are listed.

2. MIB = Management Information Base

## System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(4)XD4 and includes the following sections:

- [Memory Recommendations, page 5](#)
- [Supported Hardware, page 5](#)
- [Feature Support, page 6](#)
- [Feature Support, page 6](#)

## Memory Recommendations

[Table 3](#) displays the memory recommendations of the Cisco IOS feature sets for the Cisco IAD2430 series IAD for Cisco IOS Release 12.3(4)XD4.

Cisco IAD2430 series IAD are available with a 32-MB Flash memory card.

**Table 3** Cisco Release 12.3(4)XD4 Memory Recommendations for the Cisco IAD2430 series IAD

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
IP subset/Voice	c2430-i6s-mz	32 MB	64 MB	RAM
IP subset/IPSEC 64bit/FW/Voice	c2430-i6k9o3s-mz	32 MB	64 MB	RAM
IP PLUS	c2430-is-mz	64 MB	128 MB	RAM
IP PLUS/IPSEC 64bit/FW/Voice	c2430-ik9o3s-mz	64 MB	128 MB	RAM

## Supported Hardware

Cisco IOS Release 12.3(4)XD4 supports the following platforms:

- Cisco IAD2430 series IAD

For detailed descriptions of the new hardware features, see the “[New and Changed Information](#)” section on page 8.

For information about supported hardware for this platform and release, refer to the Hardware/Software Compatibility Matrix in the [Cisco Software Advisor](#) at the following location:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswsmatrix.cgi>

## Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

To improve the usability of the release notes documentation, Cisco IOS Release 12.3(4)XD release notes no longer contains the feature set tables. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>



### Caution

---

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

---

## Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.3(4)XD4 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

- 
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
  - Step 2** To find a feature, choose either **Search by full or partial feature name** or **Browse features in alphabetical order**. Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list appear.
  - Step 3** Select a feature from the left text box and click **Add**.



**Note** To learn more about a feature in the list, click **Description**.

---

Repeat this step to add additional features. You can choose a maximum of 20 features for a single search.

- Step 4** Click **Continue**.
  - Step 5** From the Major Release drop-down menu, choose 12.3T.
  - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
  - Step 7** From the Platform Family drop-down menu, choose the appropriate hardware platform. All software images (feature sets) that support the features that you selected appear.
- 

## Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3(4)XD4, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

- 
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
  - Step 2** In the "Find the features in a specific Cisco IOS release, using one of the following methods:" box, choose 12.3 T from the Cisco IOS Major Release drop-down menu.
  - Step 3** Click **Continue**.
  - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
  - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
  - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. All features that are supported by the feature set (software image) that you selected appear.
-

## New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco IAD2430 series IAD in Cisco IOS Release 12.3(4)XD.

### New Hardware and Software Features in Release 12.3(4)XD3 to Release 12.3(4)XD4

No new hardware products or software features are supported in Cisco IOS Release 12.3(4)XD3 to Release 12.3(4)XD4.

### New Hardware and Software Features in Release 12.3(4)XD1 to Release 12.3(4)XD3

No new hardware products or software features are supported in Cisco IOS Release 12.3(4)XD1 to Release 12.3(4)XD3.

### New Hardware Features in Release 12.3(4)XD

No new hardware products are supported in Cisco IOS Release 12.3(4)XD.

### New Software Features in Release 12.3(4)XD

The following new software features are supported by the Cisco IAD2430 series IAD in Cisco IOS Release 12.3(4)XD:

- [E1 Support on Cisco 2430 Series IAD](#)
- [Configuring Network Clock](#)
- [Configuring T1/E1 Interfaces](#)
- [Configuring ATM-T1-WAN Ports](#)

#### E1 Support on Cisco 2430 Series IAD

The Cisco IAD series IAD supports the E1 WAN and E1 Digital PBX in Cisco IOS Release 12.3(4)XD.

##### Introduction of card type CLI

```
syntax: card type <t1/e1> <slot#>
e.g. card type t1 1
or card type e1 1
```

```
syntax: network-clock-participate <t1/e1> <slot/port>
e.g. network-clock-participate t1 1/0
or
network-clock-participate e1 1/0
```

```
syntax: network-clock-select <priority> <interface#>
```

e.g. `network-clock-sel 1 Serial0/0`

## Configuring Network Clock

At initialization, all controllers on the IAD2430, including onboard T1/E1 or VWIC T1/E1, are participated into the system clock domain. The default network clock algorithm selects one of the controllers present as a default network clock. The default network clock algorithm provides a best estimate of the clocking system. This is mainly for voice applications to be configured easily after power-up.

Cisco recommends that when you power up the system, it should be the your practice to make sure that network clocks are configured properly for the applications to work, with consideration for the specific network system requirements present at the moment.

If you wish to view the current primary clock, use the `show network-clocks` or `show run` command. Note that the `show network-clocks` and `show run` commands do not display the default network clock, which is selected by the default network clock algorithm.

To participate T1/E1 controller as a clock source for the system clock domain, use the **network-clock-participate** CLI. To make available as a candidate for a clock selection algorithm, use the **network-clock-select** CLI. If you have data applications that do not require clock participation or selection, use the `no` of the afore-mentioned CLIs.

## Configuring T1/E1 Interfaces

To configure an ISDN PRI, CAS (channel-associated signaling) interface, or T1/E1 multiflex trunk interface, use the configuration software provided with your Cisco IAD or network module (if any). Otherwise, for greatest power and flexibility use configuration mode (manual configuration). In this mode, you enter Cisco IOS commands at the prompt.

Before you begin, disconnect all WAN cables from the Cisco IAD to keep it from trying to run the AutoInstall process. The Cisco IAD tries to run AutoInstall whenever you power it on if there is a WAN connection on both ends and the Cisco IAD does not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for the Cisco IAD to determine that AutoInstall is not connected to a remote TCP/IP host.

## Configuring ATM-T1-WAN Ports

If your Cisco IAD has a T1-WAN port, a default ATM configuration is automatically enabled when you enter the **mode atm** controller command. The default ATM configuration has the following operating parameters:

- Maximum virtual path identifier (VPI)s per virtual channel identifier (VCI) (`atm vc-per-vc`)—1024
- No IP address
- ATM User to Network Interface (UNI) Version 3.0 is assigned
- ATM Integrated Local Management Interface (ILMI) keepalive is disabled
- No ATM PVCs are configured

To configure the ATM interface parameters for your application, you need the following information:

- IP addresses and subnet masks
- VPI/VCI numbers
- Any other information related to the routing protocol

# Limitations and Restrictions

Refer to each feature for individual limitations and restrictions.

## Current MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

## Supported MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.3(4)XD4 that can apply to the Cisco IAD2430 Series Integrated Access Devices.

## Initialization

At initialization, the default network clock algorithm selects one of the controllers present as a default network clock. The default network clock algorithm provides a best estimate of the clocking system. However, there is no guarantee that all applications relying on clock accuracy will work after initialization.

We recommend that when the user powers up the system, it should be the user's practice to make sure that network clocks are configured properly for the applications to work, with consideration for the specific network system requirements present at the moment.

If you wish to view the current primary clock, use the `show network-clocks` or `show run` command. Note that the `show network-clocks` and `show run` commands do not display the default network clock, which is selected by the default network clock algorithm.

## Field Notices and Bulletins

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at <http://www.cisco.com/warp/customer/770/index.shtml>. If you do not have a Cisco.com login account, you can find field notices at <http://www.cisco.com/warp/public/770/index.shtml>.
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml>.
- **What's New for IOS**—*What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

## 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 selected severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(4)XD4.

For information on caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T, see [Caveats for Cisco IOS Release 12.3 T](#). These documents lists severity 1 and severity 2 caveats and only selected severity 3 caveats, and are located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Release 12.3(4)XD4 are listed in this section.



### Note

If you have an account on Cisco.com, you can use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) by clicking the Log In button on the right side, go to the drop down menu on the top bar of the page and select **Technical Support: Tools & Utilities: Software Bug Toolkit (under Troubleshooting Tools)**. Another option is to enter the following URL in your web browser or go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## Open Caveats—Cisco IOS Release 12.3(4)XD4

There are no open caveats specific to Cisco IOS Release 12.3(4)XD4 that require documentation in the release notes.

## Resolved Caveats—Cisco IOS Release 12.3(4)XD4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 4 Resolved Caveats for Cisco IOS Release 12.3(4)XD4

DDTS ID Number	Description
CSCeb88239	<p>const2:crash RIPv6_input after sending 1 packet to FF02::9 M/cast Ad</p> <p>Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.</p> <p>Conditions: This symptom is observed when the <b>ipv6 debug rip</b> command is entered on the router. Malformed packets can normally be sent locally. However, when the <b>ipv6 debug rip</b> command is entered, the crash can also be triggered remotely.</p> <p><b>Note</b> RIP for IPv4 is not affected by this vulnerability.</p> <p>Workaround: None.</p>
CSCec79609	<p>MLPoA: Multilink interface comes up as Virtual-Access</p> <p>Symptoms: A Multilink PPP over ATM (MLPoA) bundle that is configured by using a multilink interface may come up as a virtual-access interface, but the multilink interface may remain inactive as an MLP bundle.</p> <p>Conditions: This symptom is observed after a bundle reset, which may be triggered by entering the <b>clear interface</b> user EXEC or privileged EXEC command for the multilink interface or for a virtual-access member.</p> <p>Workaround: None</p>
CSCec88490	<p>Cosmetic Display CLI Related Issues</p> <p>Symptom: When doing a line-mode 2-wire ? in ATM mode on WIC-1SHDSL-V2, the help text displays incorrect mapping between the line number &amp; the pins used.</p> <p>Explanation: When the DSL controller needs to be configured in 2-wire ATM mode, the line to be used has to be specified. In the help to choose the line, the pins used should be specified as: line-one Line one (RJ-11 pins 2&amp;5) line-zero Line zero (RJ-11 pins 3&amp;4)</p> <p>Instead the pins used are specified as: line-one Line one (RJ-11 pins 3&amp;4) line-zero Line zero (RJ-11 pins 2&amp;5)</p> <p>Conditions: WIC-1SHDSL-V2 in ATM mode.</p> <p>Workaround: None</p>

Table 4 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCed21034	<p>atmVclTable maps all PVCs to all subinterfaces</p> <p>Symptoms:</p> <ul style="list-style-type: none"> <li>-Each ATM PVC is linked to each ATM (sub)interface in the atmVclTable.</li> <li>-The atmVclTable is indexed by ifIndex. For a specific PVC, this should point to the ifIndex/interface on which this PVC is present. However, the atmVclTable contains one entry per ifIndex for each PVC.</li> </ul> <p>Conditions: These symptoms are observed in a Cisco IOS image that contains the fix for CSCea63829.</p> <p>Workaround: None</p>
CSCed78149	<p>TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts</p> <p>Symptoms: TCP connections may be vulnerable to spoofed ICMP packets. A spoofed ICMP packet may cause the TCP connection to use a very low segment size for 10 minutes at a time.</p> <p>Conditions: This symptom is observed when TCP connections are configured for PMTU discovery. Note that PMTU discovery is disabled by default on a router.</p> <p>Workaround: Disable PMTU discovery.</p>
CSCee14958	<p>Clock glitch in the Spock FPGA and SCC sync/idle flags correction</p> <p>Symptoms: A SAR on a DSL WIC may cause reduced throughput, an increase in delay, or both because the bandwidth that is configured for the VC may be corrupted.</p> <p>Conditions: This symptom is observed on a Cisco 3700 series.</p> <p>Workaround: None</p>
CSCee56149	<p>DSLSAR: Incorrect sequence of TSI and tail pointer in the TX path</p> <p>Symptoms: Acknowledgements coming from a WIC may be lost, and the transmission may lock up. The missing acknowledgements may be recovered if the number of acknowledgements is more than one.</p> <p>Conditions: This symptom is observed on a Cisco 2600 series that is configured with an ADSL or G.SHDSL WIC.</p> <p>Workaround: If the transmission locks up, reset the interface. However, you can prevent the lock up from occurring by entering the <b>tx-ring-limit ring-limit</b> command on the PVC and by entering 24, 6, 5, or 2 for the <i>ring-limit</i> argument.</p>

Table 4 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCef44193	<p>Line-Rate on Line 0 not reported correctly</p> <p>Symptom: <b>show controller DSL</b> may show incorrect line-rate on line 0, with Release 12.3(4)XD1. If the line trains at a slower rate than the configured rate, under certain conditions the router will display the configured rate rather than the trained rate.</p> <p>Workaround: None. This is fixed in all subsequent releases.</p>
CSCef46191	<p>Unable to telnet</p> <p>Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected. All other device services will operate normally.</p> <p>Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.</p> <p>Workaround: The detail advisory is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml</a></p>
CSCef66120	<p>ATM MIBs not working properly for DSL WICs on c2600</p> <p>Symptom: ATM Subinterfaces are not present in IF-MIB.</p> <p>Conditions: Customer has a SHDSLv2 WIC operating in ATM mode.</p> <p>Workaround: None</p>

**Table 4** Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCeg01135	SHDSL-T1/E1 Related Commands should be Disabled for Cisco 2691 or higher <b>Note</b> T1/E1 mode for WIC-1SHDSL-V2 cards is not supported. Commands related to T1/E1 should not be used.
CSCin70150	ATM subinterfaces are not added to ifTable in reformation images Symptoms: ATM-related MIBS cannot be used to monitor ATM subinterfaces. Conditions: This symptom is observed on a Cisco 2600 series and Cisco 3700 series when ATM subinterfaces are not added to the "ifTable" in ipbase-mz, ipvoice-mz, entbase-mz, and advsecurityk9-mz images of Cisco IOS software. Workaround: None. Note that the symptom does not occur in entservicesk9-mz images of Cisco IOS software.

## Caveat Advisories - Resolved Caveats

- CSCef60659: More stringent checks required for ICMP unreachable

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa59600: IPSec PMTUD not working [after CSCef44225]

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef43691: L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44225: IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44699: GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef61610: Incorrect handling of ICMPv6 messages can cause TCP performance problems

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa61864: Enhancements to L2TPv3 PMTUD may not work [Follow-up to CSCef43691]

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCed78149: TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa52807: L2TP doing PMTUD vulnerable to spoofed ICMP paks

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

## Open Caveats—Cisco IOS Release 12.3(4)XD3

There are no open caveats specific to Cisco IOS Release 12.3(4)XD3 that require documentation in the release notes.

## Resolved Caveats—Cisco IOS Release 12.3(4)XD3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

**Table 5** Open Caveats for Cisco IOS Release 12.3(4)XD3

DDTS ID Number	Description
CSCed84634	<p>Under High Link Utilization OAM may bring VC down on DSL ATM int</p> <p>Symptoms: Without the solution for this problem, some of the Operation, Administration, and Maintenance (OAM) packets may be lost over a permanent virtual circuit (PVC) configured on a digital subscriber line (DSL)(either ADSL or G.SHDSL) Interface which may result in the PVC flapping (going down and coming back up). The fix for this bug would introduce delay in sending the OAM requests/replies in the order of tens of milli seconds.</p> <p>Independent of this bug, the time required to send a OAM packet or respond to a OAM request packet from the far end depends the size of the data packets and the PVC bandwidth.</p> <p>Workaround: In order to improve OAM response times and as a potential means to prevent the PVC going down, configure a smaller TX RING on a PVC (which will reduce the head of line delay for OAM packets) and configure larger OAM timeouts using the <b>oam retry</b> command and/or reducing the frequency of the the OAM packets using the <b>oam-pvc manage &lt;loopback frequency in seconds&gt;</b> command under the PVC configuration.</p> <p>It is, however, important to note that for some applications, smaller TXRING values may introduce throughput loss. And the choice of TXRING value should be based on the delay requirements, if any, and the throughput.</p>
CSCee08584	<p>Cisco Internetwork Operating System (IOS) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for Cisco's IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.</p> <p>A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml</a></p> <p>Cisco has made free software upgrades available to address this vulnerability for all affected customers.</p> <p>This vulnerability is documented by Cisco bug ID CSCee08584.</p>

**Table 5** *Open Caveats for Cisco IOS Release 12.3(4)XD3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCee54372	<p>Perf. counters rollover on the DSLAM may bring the SHDSL line down</p> <p>Symptoms: The performance counter values (es, ses, crc, uas, losw) sent through the embedded operation channel (EOC) by the WIC-1SHDSL are occasionally interpreted as extremely high values by a third-party DSLAM.</p> <p>For example, even though the customer premise equipment (CPE) sends 0 as the CRC value, the DSLAM displays it as 65536. Depending upon the configuration of the DSLAM, the line may come DOWN due to perceived overflow of the counters, even though there is no real overflow.</p> <p>Workaround: There is no workaround.</p>
CSCee76166	<p>WIC-1-SHDSL-V2 may take long time to train with ECI DSLAM in 4-wire</p> <p>Symptoms: When multiple virtual circuits (VC) are configured, there is a possibility of losing bandwidth for one of the VCs. This may result in packet drops if the traffic on the VC pumped to the VC-configured bandwidth.</p> <p>Conditions: This will happens when more than 2 VC are configured with a specific bandwidth only.</p> <p>Workaround : Reordering the VC configuration may help. There is no workaround.</p>

## Open Caveats—Cisco IOS Release 12.3(4)XD2

There are no open caveats specific to Cisco IOS Release 12.3(4)XD2 that require documentation in the release notes.

## Resolved Caveats—Cisco IOS Release 12.3(4)XD2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

**Table 6** Open Caveats for Cisco IOS Release 12.3(4)XD2

DDTS ID Number	Description
CSCed72331	<p>Internal serial interface messages pop up on SHDSL interface reset</p> <p>Symptoms: The internal serial interface UP/DOWN message is seen on the console when <b>[no] mode atm</b> is configured in the WIC-1SHDSL-V2 module. This is seen only when the WAN interface card (WIC) is placed in a Cisco 2691 or Cisco 37xx motherboard. The internal serial interface message is not seen with Cisco 26xx and Fast Ethernet network module (FE NM) platforms.</p> <p>The same problem is seen with the WIC-1SHDSL module on the Cisco 2691 or Cisco 37xx platforms when the router boots up.</p> <p>Workaround: There is no workaround.</p>
CSCed29194	<p>Message Display Issue:aal2_vc_sar_info_remove</p> <p>Symptoms: A message “aal2_vc_sar_info_remove” appears while configuring the non AAL2 virtual circuit in a subinterface.</p> <p>Workaround: There is no workaround. This problem doesn't harm any functionality. For some customers, unwanted messages are not likely to be seen popping up during the permanent virtual circuit (PVC) configuration.</p>
CSCea58939	<p>Path confm fails on shut/no shut on WIC-GSHDSL with NM-HDV</p> <p>Symptom: Path confirmation failure messages are observed when VOIP calls are being setup and torn down by using Abacus tester, while the WIC-GSHDSL module (which is not in datapath) is <b>shut</b>; then, <b>no-shut</b>.</p> <p>Conditions:</p> <ul style="list-style-type: none"> <li>• Cisco 2600, Cisco 2691, and Cisco 3700 routers</li> <li>• Any existing images</li> <li>• VOIP calls are continually setup and torn down with the Abacus tester such that a high number of calls are made quickly. When more calls are made, this problem occurs more easily.</li> <li>• WIC-GSHDSL (which is not even in datapath) is <b>shut</b>, then enter the <b>no shut</b> command while these VOIP calls are being made.</li> </ul> <p>Workaround: Do not make VOIP call while issuing a <b>no-shut</b> command to the WIC-GSHDSL module. Wait until the WIC-GSHDSL is up.</p> <p>Further Problem Description:</p> <ul style="list-style-type: none"> <li>• The problem is likely to occur also on the WIC-1-ADSL and WIC-1-GSHDSL-V2 modules.</li> <li>• The problem is likely to be caused by xDSL WICs taking too much CPU time during the <b>no shut</b> command.</li> </ul>

**Table 6** Open Caveats for Cisco IOS Release 12.3(4)XD2 (continued)

DDTS ID Number	Description
CSCed50752	<p>sh controller dsl is up but atm interface is down.</p> <p>Symptoms: WIC-1-SHDSL-V2 DSL interface may be up but ATM is down.</p> <p>Conditions:</p> <ul style="list-style-type: none"> <li>• Cisco 2600, Cisco 2691, and Cisco 3700 routers</li> <li>• Any existing images</li> </ul> <p>Workaround: There is no workaround. The ATM interface does not come up with the <b>shut</b> and <b>no shut</b> commands.</p> <p>Further Problem Description: This is only specific to WIC-1-SHDSL-V2 WIC.</p>
CSCed71659	<p>CoS Configuration under ATM Interface after Reload Router</p> <p>Symptom: On the WIC-1SHDSL-V2 module with certain DSL data rates (rates greater than 2304), configured class services like VBR-NRT 3200 3200 1 could be missing after the router is reloaded.</p> <p>Workaround: Enable the missing configuration again after reload.</p>
CSCed14031	<p>EOC msg 17 not received by WIC-1SHDSL and WIC-1SHDSL-V2 from Alcatel DSLAM.</p> <p>Symptoms: Embedded operations channels (EOC) message 17 is not received by WIC-1SHDSL and WIC-1SHDSL-V2 even though a certain third-party digital subscriber line access multiplier (DSLAM) sends it periodically. This is because the said DSLAM sends message 11 and message 17 with one 7E in between. The GTI_EOM interrupt is generated by the firmware on two consecutive 7Es. Hence, message 17 is not processed by the customer premise equipment (CPE) (SHDSL WIC). The problem has no impact on functionality or user interface.</p> <p>Workaround: There is no workaround.</p>
CSCed81135	<p>Trace backs appear when WIC-1-SHDSL-V2 is connected to ECI DSLAM.</p> <p>Symptoms: This problem is seen with the ECI digital subscriber line access multiplier (DSLAM) when the WIC1-SHDSL-V2 module is configured in 4-wire mode. The problem is seen because of large number of embedded operations channels (EOC) messages. The problem does not impact any functionality. The problem has not been seen with other DSLAMs yet, but it could happen when there are large number of EOC messages or bad frame check sequence (FCS) EOC packets sent by the DSLAM.</p> <p>Workaround: There is no workaround.</p>
CSCed93090	<p>Line-mode CLI does not have option for auto line mode selection.</p> <p>Symptoms: DSL line training stops if digital subscriber line access multiplier (DSLAM) switches from two-wire to four-wire or four-wire to 2-wire.</p> <p>Conditions: The WIC-1-SHDSL-V2 module will not train with the DSLAM unless the line-mode configuration is changed. Unless the line-mode matches with the DSLAM, the line may not train if the DSLAM switches from 2-wire mode to 4-wire mode or 4-wire mode to 2-wire mode.</p> <p>Workaround: Change the CPE line-mode configuration to DSLAM line-mode configuration.</p>

## Open Caveats—Cisco IOS Release 12.3(4)XD1

There are no open caveats specific to Cisco IOS Release 12.3(4)XD1 that require documentation in the release notes.

## Resolved Caveats—Cisco IOS Release 12.3(4)XD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

**Table 7** Open Caveats for Cisco IOS Release 12.3(4)XD1

DDTS ID Number	Description
CSCed27956	<p>A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.</p> <p>All Cisco products which contain TCP stack are susceptible to this vulnerability.</p> <p>This advisory is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml</a>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.</p> <p>A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml</a>.</p>
CSCed38527	<p>A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.</p> <p>All Cisco products which contain TCP stack are susceptible to this vulnerability.</p> <p>This advisory is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml</a>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.</p> <p>A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml</a>.</p>

## Open Caveats—Cisco IOS Release 12.3(4)XD

There are no open caveats specific to Cisco IOS Release 12.3(4)XD that require documentation in the release notes.

## Resolved Caveats—Cisco IOS Release 12.3(4)XD

There are no resolved caveats specific to Cisco IOS Release 12.3(4)XD that require documentation in the release notes.

---

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0402R)

Copyright © 2004 - 2005, Cisco Systems, Inc.  
All rights reserved.