



Release Notes for Catalyst 5000 Family ATM Module Release 12.0W5

Current Release: 12.0(28)W5(30b)

September 16, 2005

Previous Releases:

12.0(28)W5(30), 12.0(27)W5(29), 12.0(26)W5(28b), 12.0(26)W5(28a), 12.0(24)W5(26a), 12.0(22)W5(25), 12.0(20)W5(24a), 12.0(20)W5(24), 12.0(19)W5(23), 12.0(18)W5(22), 12.0(16)W5(21), 12.0(14)W5(20), 12.0(13)W5(19), 12.0(10)W5(18a), 12.0(9)W5(17a), 12.0(9)W5(17), 12.0(7)W5(15b), 12.0(4a)W5(10)



Note

Release 12.0(13)W5(19) is obsolete. You can use Release 12.0(14)W5(20) for the Catalyst 5000 family ATM module images.

Contents

These release notes include the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [Limitations and Restrictions, page 9](#)
- [Important Note, page 12](#)
- [Caveats, page 12](#)
- [Related Documentation, page 40](#)
- [Obtaining Documentation, page 41](#)
- [Documentation Feedback, page 42](#)
- [Obtaining Technical Assistance, page 43](#)
- [Obtaining Additional Publications and Information, page 44](#)



Corporate Headquarters:

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

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

Introduction

These release notes describe the Catalyst 5000 family ATM module Release 12.0(28)W5(30).

The Catalyst 5000 family includes the Catalyst 5002, the Catalyst 5000, the Catalyst 5505, the Catalyst 5509, and the Catalyst 5500 switches. Throughout this publication and all Catalyst 5000 family documents, the phrase “Catalyst 5000 family switches” refers to all Catalyst 5000 family switches, unless otherwise noted.

The following modules are supported in this release:

- ATM dual PHY OC-3 modules (WS-X5153, WS-X5154, WS-X5155, WS-X5156, WS-X5157, and WS-X5158)
- ATM dual PHY OC-12 modules (WS-X5161 and WS-X5162)
- ATM dual PHY OC-3 modules (WS-X5167 and WS-X5168)
- ATM Fabric Integration Module (WS-X5165)

The ATM dual PHY OC-3 modules (WS-X5153, WS-X5154, WS-X5155, WS-X5156, WS-X5157, and WS-X5158) use the c5atm-wl-mz image. These modules do not support Multiprotocol over ATM (MPOA). This image supports LAN Emulation (LANE) and RFC 1483 non-traffic-shaping permanent virtual connections (PVCs). If you want traffic-shaping PVC functionality, use the c5atm-wt-mz image.

The ATM dual PHY OC-12 modules (WS-X5161 and WS-X5162), the ATM dual PHY OC-3 modules (WS-X5167 and WS-X5168), and the ATM Fabric Integration Module (WS-X5165) use the c5atm-lc-mz image. These modules support MPOA, LANE, and RFC 1483 with traffic-shaping. The same software image supports all three features.

The Catalyst 5000 family ATM LANE modules are Year 2000 compliant in ATM Release 3.1 and later. For more information on Cisco’s Year 2000 compliance, visit this URL:
<http://www.cisco.com/warp/public/752/2000/>

System Requirements

This section describes the system requirements.

Supported Cisco IOS Trains by Feature

The modules supported by the c5atm-wl-mz, c5atm-lc-mz, and c5atm-wt-mz images are supported on the following release trains. [Table 1](#) lists the ATM module features and the applicable Cisco IOS train that supports each feature.

Table 1 Supported Cisco IOS Trains by Feature

Product Number	LANE	PVC Traffic-Shaping	Token Ring	MPOA	FSSRP	Fast PHY
WS-X5153 WS-X5154 WS-X5155	12.0	12.0	70.2(1)	Not supported	12.0	12.0
WS-X5156 WS-X5157 WS-X5158	12.0	12.0	70.2(1)	Not supported	12.0	12.0
WS-X5161 WS-X5162	12.0	12.0	Not supported	12.0	12.0	12.0
WS-X5165	12.0	12.0	Not supported	12.0	12.0	12.0
WS-X5166	Not supported	12.0	Not supported	Not supported	Not supported	Not supported
WS-X5167 WS-X5168	12.0	12.0	Not supported	12.0	12.0	12.0

**Note**

The Release 12.0-based image has new features, such as fast-PHY switchover and FSSRP.

For a list of Cisco IOS software caveats that apply to this release, refer to the *Caveats for Cisco IOS Release 12.0* publications. For Cisco IOS release notes that apply to this release, refer to the *Release Notes for Cisco IOS Release 12.0*. These documents are located on Cisco.com. For more information, see the Cisco.com section in this note.

For information on ATM module releases prior to Release 12.0(7)W5(15b), refer to this World Wide Web location:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/c5krm/atm_rns/index.htm

Release Images

[Table 2](#) lists the current release image names on Cisco.com for the Catalyst 5000 family ATM modules.

Table 2 Current Release Image Names for ATM Modules

ATM Module	Product Number	LANE SW Release	PVC Traffic-Shaping SW Release	Token Ring	LANE/MPOA/Traffic-Shaping SW Release	Latest Supervisor Engine SW Release
LANE Single PHY OC-3	WS-X5153 WS-X5154 WS-X5155	12.0W5(30b) c5atm-wl-mz.120-28.W5.30b.bin	12.0W5(30b) c5atm-wt-mz.120-28.W5.30b.bin	70.2(1) c5atm-trlane.70-2-1.bin	Not applicable	5.5(9)
LANE Dual PHY OC-3	WS-X5156 WS-X5157 WS-X5158	12.0W5(30b) c5atm-wl-mz.120-28.W5.30b.bin	12.0W5(30b) c5atm-wt-mz.120-28.W5.30b.bin	70.2(1) c5atm-trlane.70-2-1.bin	Not applicable	5.5(9)

Table 2 Current Release Image Names for ATM Modules (continued)

ATM Module	Product Number	LANE SW Release	PVC Traffic-Shaping SW Release	Token Ring	LANE/MPOA/Traffic-Shaping SW Release	Latest Supervisor Engine SW Release
Dual PHY OC-12	WS-X5161 WS-X5162	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	Not applicable	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	5.5(9)
Fabric Integration	WS-X5165	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	Not applicable	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	5.5(9)
Dual PHY DS3	WS-X5166	Not applicable	12.0W5(30b) c5atm-wt-mz.120-28.W5.30b.bin	Not applicable	Not applicable	5.5(9)
Dual PHY OC-3	WS-X5167 WS-X5168	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	Not applicable	12.0W5(30b) c5atm-lc-mz.120-28.W5.30b.bin	5.5(9)

Orderable Product Number Matrix

Table 3 lists the software version and applicable ordering information for the Catalyst 5000 family ATM module software.

Table 3 Software Version/Orderable Product Number Matrix

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
3.2(4)	c5000-atm.3-2-4.bin	SFC5K-ATM-3.2.4	SWC5K-ATM-3.2.4=
3.2(5)	cat5000-atm.3-2-5.bin	SFC5K-ATM-3.2.5	SWC5K-ATM-3.2.5=
3.2(6)	cat5000-atm.3-2-6.bin	SFC5K-ATM-3.2.6	SWC5K-ATM-3.2.6=
3.2(7)	cat5000-atm.3-2-7.bin	SFC5K-ATM-3.2.7	SWC5K-ATM-3.2.7=
12.0W5(10)	c5atm-wblane.120-4a.W5.10.bin	SFC5K-ATML-5.10	SWC5K-ATML-5.10=
12.0W5(15b)	c5atm-wblane.120-7.W5.15b.bin	SFC5K-ATML-5.15B	SWC5K-ATML-5.15B=
12.0W5(17)	c5atm-wblane.120-9.W5.17.bin	SC5K-ATML-5.17	SC5K-ATML-5.17=
12.0W5(17a)	c5atm-wblane.120-9.W5.17a.bin	SC5K-ATML-5.17A	SC5K-ATML-5.17A=
12.0W5(18a)	c5atm-wl-mz.120-10.W5.18a.bin	SC5AWL-12.0.10W	SC5AWL-12.0.10W=
12.0W5(19)	c5atm-wl-mz.120-12.W5.19.bin	SC5AWL-12.0.12W	SC5AWL-12.0.12W=
12.0W5(10)	c5atm-wtall.120-4a.W5.10.bin	SFC5K-ATMLM-5.10	SWC5K-ATMLM-5.10=
12.0W5(15b)	c5atm-wtall.120-7.W5.15b.bin	SFC5K-ATMLM-5.15B	SWC5K-ATMLM-5.15B=
12.0W5(17)	c5atm-wtall.120-9.W5.17.bin	SC5K-ATMLM-5.17	SC5K-ATMLM-5.17=
12.0W5(17a)	c5atm-wtall.120-9.W5.17a.bin	SC5K-ATMLM-5.17A	SC5K-ATMLM-5.17A=
12.0W5(18a)	c5atm-lc-mz.120-10.W5.18a.bin	SC5ALC-12.0.10W	SC5ALC-12.0.10W=
12.0W5(19)	c5atm-lc-mz.120-12.W5.19.bin	SC5ALC-12.0.12W	SC5ALC-12.0.12W=

Table 3 Software Version/Orderable Product Number Matrix (continued)

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
12.0W5(18a)	c5atm-wt-mc.120-10.W5.18a.bin	SC5AWT-12.0.10W	SC5AWT-12.0.10W=
12.0W5(19)	c5atm-wt-mc.120-13.W5.19.bin	SC5AWT-12.0.13W	SC5AWT-12.0.13W=
12.0W5(20)	c5atm-lc-mz.120-14.W5.20.bin	SC5ALC-12.0.14W	SC5ALC-12.0.14W=
12.0W5(20)	c5atm-wl-mz.120-14.W5.20.bin	SC5AWL-12.0.14W	SC5AWL-12.0.14W=
12.0W5(20)	c5atm-wt-mc.120-14.W5.20.bin	SC5AWT-12.0.14W	SC5AWT-12.0.14W=
12.0W5(21)	c5atm-lc-mz.120-16.W5.21.bin	SC5ALC-12.0.16W	SC5ALC-12.0.16W=
12.0W5(21)	c5atm-wl-mz.120-16.W5.21.bin	SC5AWL-12.0.16W	SC5AWL-12.0.16W=
12.0W5(21)	c5atm-wt-mc.120-16.W5.21.bin	SC5AWT-12.0.16W	SC5AWT-12.0.16W=
12.0W5(22)	c5atm-lc-mz.120-18.W5.22.bin	SC5ALC-12.0.18W	SC5ALC-12.0.18W=
12.0W5(22)	c5atm-wl-mz.120-18.W5.22.bin	SC5AWL-12.0.18W	SC5AWL-12.0.18W=
12.0W5(22)	c5atm-wt-mc.120-18.W5.22.bin	SC5AWT-12.0.18W	SC5AWT-12.0.18W=
12.0W5(23)	c5atm-lc-mz.120-19.W5.23.bin	SC5ALC-12.0.19W	SC5ALC-12.0.19W=
12.0W5(23)	c5atm-wl-mz.120-19.W5.23.bin	SC5AWL-12.0.19W	SC5AWL-12.0.19W=
12.0W5(23)	c5atm-wt-mc.120-19.W5.23.bin	SC5AWT-12.0.19W	SC5AWT-12.0.19W=
12.0W5(24)	c5atm-lc-mz.120-20.W5.24.bin	SC5ALC-12.0.20W	SC5ALC-12.0.20W=
12.0W5(24)	c5atm-wl-mz.120-20.W5.24.bin	SC5AWL-12.0.20W	SC5AWL-12.0.20W=
12.0W5(24)	c5atm-wt-mc.120-20.W5.24.bin	SC5AWT-12.0.20W	SC5AWT-12.0.20W=
12.0W5(24a)	c5atm-lc-mz.120-20.W5.24a.bin	SC5ALC-12.0.20W	SC5ALC-12.0.20W=
12.0W5(24a)	c5atm-wl-mz.120-20.W5.24a.bin	SC5AWL-12.0.20W	SC5AWL-12.0.20W=
12.0W5(24a)	c5atm-wt-mc.120-20.W5.24a.bin	SC5AWT-12.0.20W	SC5AWT-12.0.20W=
12.0W5(25)	c5atm-lc-mz.120-22.W5.25bin	SC5ALC-12.0.22W	SC5ALC-12.0.22W=
12.0W5(25)	c5atm-wl-mz.120-22.W5.25.bin	SC5AWL-12.0.22W	SC5AWL-12.0.22W=
12.0W5(25)	c5atm-wt-mc.120-22.W5.25.bin	SC5AWT-12.0.22W	SC5AWT-12.0.22W=
12.0W5(26a)	c5atm-lc-mz.120-24.W5.26a.bin	SC5ALC-12.0.24W	SC5ALC-12.0.24W=
12.0W5(26a)	c5atm-wl-mz.120-24.W5.26a.bin	SC5AWL-12.0.24W	SC5AWL-12.0.24W=
12.0W5(26a)	c5atm-wt-mc.120-24.W5.26a.bin	SC5AWT-12.0.24W	SC5AWT-12.0.24W=
12.0W5(28a)	c5atm-lc-mz.120-26.W5.28a.bin	SC5ALC-12.0.26W	SC5ALC-12.0.26W=
12.0W5(28b)	c5atm-wt-mz.120-26.W5.28b.bin	SC5AWT-12.0.26W	SC5AWT-12.0.26W=
12.0W5(29)	c5atm-wt-mz.120-27.W5.29.bin	SC5AWT-12.0.27W	SC5AWT-12.0.27W=
12.0W5(29)	c5atm-wl-mz.120-27.W5.29.bin	SC5AWL-12.0.27W	SC5AWL-12.0.27W=
12.0W5(29)	c5atm-lc-mz.120-27.W5.29.bin	SC5ALC-12.0.27W	SC5ALC-12.0.27W=
12.0W5(30)	c5atm-wt-mz.120-28.W5.30.bin	SC5AWT-12.0.28W	SC5AWT-12.0.28W=
12.0W5(30)	c5atm-wl-mz.120-28.W5.30.bin	SC5AWL-12.0.28W	SC5AWL-12.0.28W=
12.0W5(30)	c5atm-lc-mz.120-28.W5.30.bin	SC5ALC-12.0.28W	SC5ALC-12.0.28W=
12.0W5(30b)	c5atm-wt-mz.120-28.W5.30b.bin	SC5AWT-12.0.28W	SC5AWT-12.0.28W=

Table 3 Software Version/Orderable Product Number Matrix (continued)

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
12.0W5(30b)	c5atm-wl-mz.120-28.W5.30b.bin	SC5AWL-12.0.28W	SC5AWL-12.0.28W=
12.0W5(30b)	c5atm-lc-mz.120-28.W5.30b.bin	SC5ALC-12.0.28W	SC5ALC-12.0.28W=

New and Changed Information

These sections describe the new and changed information for the Catalyst 5000 family ATM module.

New Software Features in Release 12.0(28)W5(30b)

There are no new software features in Release 12.0(28)W5(30b).

New Software Features in Release 12.0(28)W5(30)

There are no new software features in Release 12.0(28)W5(30).

New Software Features in Release 12.0(26)W5(28b)

There are no new software features in Release 12.0(26)W5(28b).

New Software Features in Release 12.0(26)W5(28a)

There are no new software features in Release 12.0(26)W5(28a).

New Software Features in Release 12.0(24)W5(26a)

There are no new software features in Release 12.0(24)W5(26a).

New Software Features in Release 12.0(22)W5(25)

There are no new software features in Release 12.0(22)W5(25).

New Software Features in Release 12.0(20)W5(24a)

There are no new software features in Release 12.0(20)W5(24a).

New Software Features in Release 12.0(20)W5(24)

There are no new software features in Release 12.0(20)W5(24).

New Software Features in Release 12.0(19)W5(23)

There are no new software features in Release 12.0(19)W5(23).

New Software Features in Release 12.0(18)W5(22)

There are no new software features in Release 12.0(18)W5(22).

New Software Features in Release 12.0(16)W5(21)

There are no new software features in Release 12.0(16)W5(21).

New Software Features in Release 12.0(14)W5(20)

There are no new software features in Release 12.0(14)W5(20).

New Software Features in Release 12.0(13)W5(19)

There are no new software features in Release 12.0(13)W5(19).

New Software Features in Release 12.0(10)W5(18a)

Release 12.0(10)W5(18a) supports PVC traffic-shaping on the Catalyst 5000 family ATM modules, and it is the first maintenance release for the PVC traffic-shaping feature supported on the Catalyst 5000 family ATM modules.

New Software Features in Release 12.0(9)W5(17a)

There are no new software features in Release 12.0(9)W5(17a).

New Software Features in Release 12.0(9)W5(17)

There are no new software features in Release 12.0(9)W5(17).

New Software Features in Release 12.0(7)W5(15b)

There are no new software features in Release 12.0(7)W5(15b).

New Software Features in Release 12.0(4a)W5(10)

This section contains new feature information, usage guidelines, and restrictions for Release 12.0(4a)W5(10).

New Features

Release 12.0(4a)W5(10) supports these new features:

- Fast Simple Server Redundancy Protocol (FSSRP)
- Fast physical sublayer (PHY) switchover

FSSRP

FSSRP differs from the current Simple Server Redundancy Protocol (SSRP) in that all configured LAN Emulation Servers (LESs) (the master LES, as well as the secondary LESs) of an Emulated LAN (ELAN) can accept join requests from any FSSRP-aware client. The benefit of establishing connections with all the LES broadcast and unknown server (BUS) pairs is that an LEC can switch over to a new LES/BUS in the event of a failure and without any noticeable delay. The fast switchover is made possible by handing out all the configured LES addresses (in the order in which they are configured) to the LAN Emulation Clients (LECs) in the configuration response through a Cisco proprietary type-length-value (TLV). The list of configured LES addresses (a maximum of four addresses) includes the address that is returned in the configuration response, all the FSSRP-capable LES addresses, and an old-style LES (if that is the master LES).

LECs can join an FSSRP LES by including the FSSRP TLV in the join request, which uniquely identifies the client's capability to the LES. The master LES also tracks any FSSRP-unaware clients that have joined the ELAN and redirects them to a new master LES in the event of a switchover (a preempt configuration). With FSSRP implemented, only FSSRP-unaware clients need to go to LECs to get the new (master) LES address and rejoin the ELAN. All LESs know if they are the master LES or a secondary LES.

There is only one new command for this feature. Use the **lane fssrp** command to enable FSSRP.

Defaults

By default, FSSRP is not enabled.

Syntax Description

Cisco IOS ATM command.

Command Modes

Interface configuration.

Usage Guidelines

Use the **lane fssrp** command from the major interface configuration level to enable all LESs, LECs, and BUSs on the subinterfaces configured on that major interface.

When you enable FSSRP on a major interface, all LECs and LES/BUS pairs configured on the subinterfaces of that major interface become FSSRP enabled.

Examples

This example shows how to enable FSSRP on the major interface:

```
ATM#config term
Enter configuration commands, one per line. End with CNTL/Z.
ATM(config)#interface atm0
ATM(config-if)#lane fssrp
ATM(config-if)#
ATM#
```

There are also modifications to the **show lane client** display output:

- If the LEC is in the active state, it displays information for the active LES/BUS; otherwise, it displays information for the master LES/BUS.
- Extend the display with a keyword, **show lane client detail**, to display all the LES/BUS information.

Fast PHY Switchover

In previous releases, when switching from the active PHY to the redundant PHY, the link went down on all the LECs. The Catalyst 5000 family supervisor engine received a message for every VLAN configured on the module. This operation updated the spanning tree in the supervisor engine. After the redundant PHY became the active PHY, new LECs were created and a message was sent to the supervisor engine for every VLAN. Traffic was stopped while these changes were taking place.

With Release 12.0(4a)W5(10), fast PHY switchover reduces the time to restore traffic flow when traffic switches from the active PHY to the redundant PHY in the Catalyst 5000 family dual PHY ATM modules.

There are no new or modified commands for this feature.

Limitations and Restrictions

This section describes the limitations and restrictions for the Cisco IOS Release 12.0W5:

- CSCdk00214
The Catalyst 5000 family ATM modules take a long time to boot if too many PVCs (for example, 4000 PVCs) are bound to 2 VLANs.
Workaround: None.
- CSCdm22640
The Catalyst 5000 family LANE modules may freeze if a **show memory** command is issued with the term length set to 0.
Workaround: Ensure that the term length is set to a non-zero value prior to entering the command.
- CSCds21577
The WS-X5161 and WS-X5162 modules produce CPUHOG messages if the interface shuts down and is brought up with a high number of PVCs configured on the ATM interface. This problem occurs when approximately 2400 or more PVCs are configured on the interface.
- CSCdt72269
On the Catalyst 5000 family ATM modules (WS-X516x except WS-X5166), if the last (or only) LAN Emulation Client (LEC) is present on a subinterface, and traffic is removed, your session into the ATM module may fail. The diagnostic port remains functional.

To prevent this problem, before removing a sub-interface where the last (or only) LEC is present, do the following:

- Shut down the main interface using the **shut** command.
- Wait for 20 seconds.
- Remove the subinterface using the **no int atm0.xx** command.
- Make the main interface operational using the **no shut** command.

Workaround: Using the diagnostic port, configure an LEC.

- CSCdt23011

The recommended image for the WS-X5166 (DS3) ATM module is c5atm-wt-mz only. It is possible to download a c5atm-wl-mz image on the WS-X5166 ATM module, but the module does not come up.

Workaround: Set the hardware download jumper and load the c5atm-wt-mz image.

- CSCdt00227

When using the PVC traffic-shaping image (c5atm-wt-mz) with WS-X515xx and the WS-X5166 modules, the performance for 64-byte packets is below 70 Kpps.

Workaround: Use a WS-X5167/WS-X5168 module.

- CSCdt14600

Changing the traffic-shaping values for a PVC when traffic is heavy can lead to these error messages on the OC-3 and OC-12 ATM modules:

```
17:54:46: ## ATMDRV ERROR REPORT ## THost: Host Response Status:
P1CMDS_TX_VC_CLEAR(3) Response Status = P1CMDS_STATUS_SAR_TIMEOUT(12)
```

```
17:54:46: ## ATMDRV ## msg = 0x03000CB5 0x00104D08 0x409C1140 0x40122214 0x40538F3C
0x407067A0 0x00000064 0x00000007
```

Binding for the PVC being changed will go off, and if you try to bind again, you may receive this message:

```
00:31:40: ## ATMDRV ERROR REPORT ## THost: Host Response Status:
P1CMDS_BIND_LEC_TO_VC(12 or 0x0c) Response Status =
P1CMDS_STATUS_WRONG_TYPE(10)00:31:40: ## ATMDRV ## msg = 0x0C000AD3 0x00200020
0x000C0040 0xC00C0000 0x00000000 0x00370000 0x00000020 0x40867A2E
```

Workaround: None. Reload the module. Unbind the PVC before changing the traffic-shaping values, and then bind back the PVC.

- For the ATM dual PHY OC-12 module, when the (nonactive) redundant PHY connects to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time only one PHY is active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. For this reason, we recommend that you perform single downloads to the ATM Fabric Integration Modules if approximately 100 LECs are configured on the module.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10) and later:
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.

- The **set preferred phy** command is not supported.
- The **show controller** command output does not display the PHY error counters for the internal ATM port.
- If you download a configuration that creates more than 4000 PVCs with OAM enabled to a Catalyst 5000 family OC-12 ATM module using the **copy tftp running** command, the ATM module may reset.
- Due to cell-rate granularity, the actual PCR value may differ from the value you specify. Only certain output rate values are supported. The output rate is (line-rate)/N (where N is an integer), a value that is less than or equal to the rate you specified.
- The LE_ARP cache entry reverification process requires supervisor engine release 3.2(2) or later but is not available in supervisor engine release 4.1(x). If the supervisor engine software does not meet these requirements, reverification is performed by sending actual LE_ARPs.
- To fully support the ATM Fabric Integration Module (WS-X5165), the Catalyst 5500 switch must run supervisor engine release 4.3 or later, and the LightStream 1010 ASP must run Cisco IOS Release 12.0(1)W5(5) or later.
- The **show version** command displays different release numbers depending on which command-line interface (CLI) you use.
 - From the Catalyst 5000 family supervisor engine CLI (prior to supervisor engine release 4.1), this ATM release displays as follows:
 - 3.2(14) for the ATM dual PHY OC-3 modules (WS-X5153, WS-X5154, WS-X5155, WS-X5156, WS-X5157, and WS-X5158)
 - 4.12 for the ATM dual PHY OC-12 modules (WS-X5161 and WS-X5162), the ATM dual PHY OC-3 modules (WS-X5167 and WS-X5168), and the ATM Fabric Integration Module (WS-X5165)
 - From the Catalyst 5000 family supervisor engine CLI (supervisor engine release 4.1 and later), the Cisco IOS Release 12.0(4a)W5(10) is displayed.
 - From the Catalyst 5000 family ATM module CLI, the Cisco IOS Release 12.0(4a)W5(10) is displayed.

All three releases are identical.

- The minimum peak-cell rate (PCR) is 64 kbps. If you specify a PCR greater than 0 and less than 64 kbps, the rate specified is 64 kbps.
- If you install an ATM module using Release 12.0(4a)W5(10) or later and a Route Switch Module (RSM) in the same chassis, you must use RSM Release 11.2(12a)P1 or later. The maximum number of ATM and RSM modules in a chassis is seven.
- Octet counters are supported on a per-physical-interface basis only. Octet counters per virtual LAN (VLAN) or per LEC are not supported.
- CSCdj32249

When you use the Hot Standby Router Protocol (HSRP) with the Catalyst 5000 family ATM module, we recommend that you also use the **standby use-bia** command when configuring the routers. This command speeds up the HSRP switchover time.

- CSCdk22518

If system time synchronization is not supported, the following message displays during the ATM module startup time:

```
ATM_INSTANCE message does not contain timestamp info.
```

If you receive this message, use the **set clock** command to set the system clock.



Note The ATM Fabric Integration Module does not support the **set clock** command.

- If you have a LAN Emulation Configuration Server (LECS), LES, or BUS configured on an ATM module, and you replace the supervisor engine module or move the ATM module from one slot to another, you will modify the default ATM address network service access points (NSAPs). Be sure to update the LECS database configuration with the new NSAP values.
- When you insert or replace ATM modules, enter the **clear config mod_num** command to clear the ATM module configuration information in the supervisor engine and to obtain the correct spanning tree parameters for the modules. Enter this command from the supervisor engine command prompt.

Important Note

Release 12.0(13)W5(19) is obsolete. You can use Release 12.0(14)W5(20) for the Catalyst 5000 family ATM module images.

Caveats

These sections describe open and resolved caveats:

- [Release 12.0\(28\)W5\(30b\), page 13](#)
- [Release 12.0\(28\)W5\(30\), page 13](#)
- [Release 12.0\(27\)W5\(29\), page 15](#)
- [Release 12.0\(26\)W5\(28b\), page 16](#)
- [Release 12.0\(26\)W5\(28a\), page 17](#)
- [Release 12.0\(24\)W5\(26a\), page 18](#)
- [Release 12.0\(20\)W5\(24a\), page 22](#)
- [Release 12.0\(20\)W5\(24\), page 23](#)
- [Release 12.0\(19\)W5\(23\), page 23](#)
- [Release 12.0\(18\)W5\(22\), page 25](#)
- [Release 12.0\(16\)W5\(21\), page 26](#)
- [Release 12.0\(14\)W5\(20\), page 28](#)
- [Release 12.0\(13\)W5\(19\), page 31](#)
- [Release 12.0\(10\)W5\(18a\), page 33](#)
- [Release 12.0\(9\)W5\(17a\), page 34](#)
- [Release 12.0\(9\)W5\(17\), page 35](#)
- [Release 12.0\(7\)W5\(15b\), page 36](#)
- [Release 12\(4a\)W5\(10\), page 39](#)

Release 12.0(28)W5(30b)

These sections describe the open and resolved caveats in Release 12.0(28)W5(30b) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(28\)W5\(30b\), page 13](#)
- [Resolved Caveats in Release 12.0\(28\)W5\(30b\), page 13](#)

Open Caveats in Release 12.0(28)W5(30b)

There are no open caveats in ATM software Release 12.0(28)W5(30b).

Resolved Caveats in Release 12.0(28)W5(30b)

This section describes the resolved caveats in Release 12.0(28)W5(30b):

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCei76358

Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

Release 12.0(28)W5(30)

These sections describe the open and resolved caveats in Release 12.0(28)W5(30) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(28\)W5\(30\), page 13](#)
- [Resolved Caveats in Release 12.0\(28\)W5\(30\), page 13](#)

Open Caveats in Release 12.0(28)W5(30)

There are no open caveats in ATM software Release 12.0(28)W5(30).

Resolved Caveats in Release 12.0(28)W5(30)

This section describes the resolved caveats in Release 12.0(28)W5(30):

- CSCed27956

A vulnerability in Transmission Control Protocol specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in much shorter time than was previously publicly discussed. This can lead to a Denial of Service attack. Depending upon the attacked protocol, a successful attack may have additional

consequences beyond terminated session, which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (e.g., router, switch, computer) and not to the sessions that are only passing through the device (e.g., transit traffic that is being routed by a router).

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040421-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

- CSCed38527

A vulnerability in Transmission Control Protocol specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in much shorter time than was previously publicly discussed. This can lead to a Denial of Service attack. Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated session, which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (e.g., router, switch, computer) and not to the sessions that are only passing through the device (e.g., transit traffic that is being routed by a router).

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040421-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

- CSCdx03821

An ATM LANE module WS-X5161 running Cisco IOS software Release 12.1(10)E or Release 12.0(20)W5(24a) displays an incorrect five-minute output rate when you enter the **show interface atm0** command. For single-mode fiber (SMF) modules, this problem is corrected in Release 12.0(28)W5(30). For multimode fiber (MMF) modules, this problem is corrected in Release 12.0(26)W5(28a). This problem does not appear in Release 12.0(10)W5(18a) and earlier Cisco IOS software releases.

- CSCed15907

A Catalyst 5000 WS-X515X ATM module that is configured for ATM PVCs fails to come online and operate if any administratively shut down subinterfaces are configured on the module.

If the module is reset under these conditions, the module will come online but will place the E0 and ATM0 interfaces in a shutdown state, resulting in the inability to session to the module or pass traffic. If the ATM interface is not connected to anything, the module will come online with the E0 interface up, but as soon as a link is established on the ATM interface, the E0 and ATM0 interfaces will shut down, and the ability to session to the module or pass any traffic through the module will be lost.

Workaround: Remove any administratively shut down subinterfaces from the configuration (or eliminate the use of subinterfaces completely), and configure all PVCs under the main ATM interface.

Release 12.0(27)W5(29)

These sections describe the open and resolved caveats in Release 12.0(27)W5(29) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(27\)W5\(29\), page 15](#)
- [Resolved Caveats in Release 12.0\(27\)W5\(29\), page 15](#)

Open Caveats in Release 12.0(27)W5(29)

There are no open caveats in ATM software Release 12.0(27)W5(29).

Resolved Caveats in Release 12.0(27)W5(29)

This section describes the resolved caveats in Release 12.0(27)W5(29):

- CSCdu53656

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCdz72808

Frames with a size of 1534 bytes are supported on the following c5atm modules:

- WS-X5167/8—Both LANE and PVCs support frames of size 1534 bytes.
- WS-X5161/2—Both LANE and PVCs support frames of size 1534 bytes.
- WS-X5157/8—Only PVCs support frames with a size of 1534 bytes. LANE does not support this size.

Only the traffic-shaping image supports frames with a size of 1534 bytes. The LANE image does not support frames of this size.

Workaround: None.

- CSCeb48807

When you create a PVC on a LANE ATM module WS-X5158 in a Catalyst 5000 switch, the following informational message is displayed on the console if the rate-queue total in Kbps exceeds the interface bandwidth, which is 155 Mbps:

```
Interface ATM0: Total rateq allocation 157500Kbps exceeded maximum plim rate of 155Mbps.
```

If the PVC is configured with a value lower than 2081 Kbps, this message is not displayed.

Workaround: None. This message is informational and does not alter the manner in which resources are allocated to the PVC or how the PVC is shaped.

- CSCin46045

When you perform an SNMP walk or a Get Next query, an unexpected delay (of a few seconds) or a timeout might be observed by the Network Management Station (NMS) for responses to some of the MIB objects. This problem occurs when a Catalyst 6000 family ATM module is present in a Catalyst 6000 switch chassis or when a Catalyst 5000 ATM module is present in a Catalyst 5000 family switch chassis and when there are no LANE servers or LANE configuration servers configured or running on the module. This problem may also occur when there are no LANE clients configured or running on the module.

Workaround: None. Make sure that the supervisor engine is running the following releases:

- Catalyst software release 7.6(2) or later for the Catalyst 6000 family switch.
- Catalyst software release 5.5(20) or release 6.4(4) or later for the Catalyst 5000 family switch.

Release 12.0(26)W5(28b)

These sections describe the open and resolved caveats in Release 12.0(26)W5(28b) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(26\)W5\(28b\), page 16](#)
- [Resolved Caveats in Release 12.0\(26\)W5\(28b\), page 17](#)

Open Caveats in Release 12.0(26)W5(28b)

This section describes the open caveats in Release 12.0(26)W5(28b):

- CSCeb48807

When creating a permanent virtual circuit (PVC) on a Catalyst 5000 family switch module WS-X5158, an informational message appears on the console if the total number of rate queues (in Kbps) exceeds the interface bandwidth of 155 Mbps. If the PVC is configured with a value lower than 2081 Kbps and contributes to the total number of rate queues exceeding the maximum bandwidth, the information message does not appear on the console. This message is informational and does not alter the shaping of the PVC or the way resources are allocated to the PVC.

Workaround: None.

Resolved Caveats in Release 12.0(26)W5(28b)

This section describes the resolved caveats in Release 12.0(26)W5(28b):

- CSCdy57980
ATM modules WS-X5158 and WS-X5156 lock up, and no traffic passes through when the lockup occurs.
Workaround: Reset the ATM module.
- CSCin54235
The Catalyst 5000 family ATM OC-3 modules WS-X5157 and WS-X5158 lose buffers at the receiving segmentation and reassembly stage (RxSAR) upon removal of the PVC-VLAN bindings when the PVCs are receiving traffic.
Workaround: None.

Release 12.0(26)W5(28a)

These sections describe the open and resolved caveats in Release 12.0(26)W5(28a) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(26\)W5\(28a\), page 17](#)
- [Resolved Caveats in Release 12.0\(26\)W5\(28a\), page 17](#)

Open Caveats in Release 12.0(26)W5(28a)

This section describes the open caveats in Release 12.0(26)W5(28a):

- CSCdy88796
When sending packets between an ATM network and a Frame-Relay network, and the ATM side is a LANE module, the Frame-Relay router running integrated routing and bridging (IRB) is not able to handle incoming packets that have a SNAP Protocol Identifier (PID) of 0007. When the Frame-Relay side has a priority that makes it the root, the switch recognizes the router as the root. If the priority on the switch for the VLAN is changed to make it the root, the router still shows itself as the root.
Workaround: Set the router to be the root.

Resolved Caveats in Release 12.0(26)W5(28a)

This section describes the resolved caveats in Release 12.0(26)W5(28a):

- CSCdu53656
A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.
Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCdz72344

An ATM LANE module WS-X5158 or WS-X5161 operating in a Catalyst 5000 family switch will incorrectly display the maximum datagram size as 1580 when you enter the **show atm interface atm0** command. This display does not indicate a problem and is present in all Cisco IOS releases for the Catalyst 5000 family LANE modules. The maximum datagram size that these modules currently support is 1514 bytes.

- CSCdx03821

An ATM LANE module WS-X5161 running Cisco IOS software Release 12.1(10)E or Release 12.0(20)W5(24a) displays an incorrect five-minute output rate when you enter the **show interface atm0** command. This problem does not appear in Release 12.0(10)W5(18a) and earlier Cisco IOS software releases.

- CSCin46045

An SNMP walk or a Get Next query might time out at the network management system (NMS) in response to some MIB objects. This problem occurs when a Catalyst 6500 ATM module is present in a Catalyst 6500 series chassis or when a Catalyst 5000 ATM module is present in the Catalyst 5000 family chassis and when there are no LANE servers or LANE-configured servers that are configured or running on the module.

Workaround: The supervisor engine must run the following software releases:

- Catalyst operating system software release 7.6(2) or later for the Catalyst 6500 series switches
- Catalyst operating system software release 5.5(20) and release 6.4(4) or later for the Catalyst 5000 family switches

Release 12.0(24)W5(26a)

These sections describe the open and resolved caveats in Release 12.0(24)W5(26a) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(24\)W5\(26a\), page 18](#)
- [Resolved Caveats in Release 12.0\(24\)W5\(26a\), page 19](#)

Open Caveats in Release 12.0(24)W5(26a)

This section describes the open caveats in Release 12.0(24)W5(26a):

- CSCdx03821

A WS-X5161 LANE module running Release 12.1(10)E or Release 12.0(20)W5(24a) displays an incorrect five-minute output rate when you enter the **show interface atm0** command. This problem does not appear in Release 12.0(10)W5(18a) or earlier releases.

Workaround: None

- CSCdw62710

The CAM table on a Catalyst 5000 family switch with a LANE module points to a nonexistent virtual circuit. This situation occurs only occasionally.

Workaround: Clear the CAM.

- CSCdy57980

Catalyst 5000 family ATM LANE modules WS-X5158 and WS-X5156 might lock up and not allow traffic to pass when the lockup occurs.

Workaround: Reset the ATM LANE module.

- CSCdz05943

ATM module WS-X5157/8 in Catalyst 5509 switch memory gets fragmented, and malloc failures occur.

Workaround: None.

Resolved Caveats in Release 12.0(24)W5(26a)

This section describes the resolved caveats in Release 12.0(24)W5(26a):

- CSCea02355

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at this URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>

This problem is resolved in Release 12.0(24)W5(26a).

- CSCdw78193

A Catalyst 5000 family LANE module running Release 12.0(20)W5(24) might display CPUHOG messages similar to the following:

```
Feb 16 01:35:06: %SYS-3-CPUHOG: Task ran for 2448 msec (0/0), process = ATM
Periodic, PC = 400A77BC.
-Traceback= 400A7768 400A77C4 401D3534 401D3AA6
```

Workaround: None.

- CSCin17871

If you enter a **show mem** command on Catalyst 5000 family ATM module WS-X5158, the ATM module might freeze.

Workaround: Reset the ATM module.

- CSCdy26050

Under heavy traffic conditions (when the ATM LANE module is subscribed to 80 percent of its capacity), you may not be able to session in to the LANE module. Heavy traffic might also cause the MPOA-capable LANE modules to drop BPDUs that are meant to be sent over LANE. This problem is not present if the LANE module is configured for PVCs. The problem occurs only if the LANE module is configured for LANE.

Workaround: None.

Release 12.0(22)W5(25)

These sections describe the open and resolved caveats in Release 12.0(22)W5(25) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(22\)W5\(25\), page 21](#)
- [Resolved Caveats in Release 12.0\(22\)W5\(25\), page 22](#)

Open Caveats in Release 12.0(22)W5(25)

This section describes the open caveats in Release 12.0(22)W5(25):

- CSCdw78193

A Catalyst 5000 family LANE module running Release 12.0(20)W5(24) can display CPUHOG messages similar to this:

```
Feb 16 01:35:06: %SYS-3-CPUHOG: Task ran for 2448 msec (0/0), process = ATM
Periodic, PC=400A77BC.
-Traceback=400A7768 400A77C4 401D3534 401D3AA6
```

Workaround: None.

- CSCdx27805

When you try to connect the console port of the WS-X5158 module, this message appears:

```
%% Low on memory: try again later
%% Low on memory: try again later
```

After the ATM module is reset, this alarm appears:

```
ATM#sh run
ATM#
Mar 17 10:12:32.075: %SYS-2-MALLOCFAIL: Memory allocation of 130042
bytes failed from 0x400303C4, pool Processor, alignment 0
-Process= "Virtual Exec", ipl= 0, pid= 53
-Traceback= 4009BD9E 4009CFCA 400303CC 40053952 40042DF0 40056906
```

Workaround: None. Try to connect to the console port at a later time.

- CSCdx22874

When an LEC on a Cisco device receives wrongly formatted LANE control frames, this message is generated:

```
%LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
```

Workaround: You do not need to bring down the LEC because this message usually appears only a few times. However, if the message keeps reappearing, you can restart the LEC or move the LEC from the Catalyst 5000 family ATM module to another device.

Resolved Caveats in Release 12.0(22)W5(25)

This section describes the resolved caveats in Release 12.0(22)W5(25):

- CSCdx10571

When using traffic-shaping code on a WS-X515 series LANE module in a Catalyst 5000 chassis, bridged AAL5SNAP frames will not be padded to the minimum Ethernet frame size. The resulting frame then becomes shorter than the valid minimum packet length, so the packet is dropped by the next receiving device. This condition greatly affects the AppleTalk and IPX protocols.

Workaround: You can use the LANE code on the WS-X515 series LANE modules (which limits you from being able to regulate the traffic on the PVCs), or use a WS-X516 series LANE module.

- CSCin05574

When 2000 PVCs (or greater) in 1000 VLANs are configured on the WS-X6101-OC12-MMF module, and ILMI and signalling PVCs are removed, the interface goes down and comes up, and then the module crashes. If the module has no PVCs other than the ILMI and signalling PVCs, the interface goes down and comes up when those PVCs are removed.

Workaround: None.

- CSCdp02052

When you enter a **show lane client** command, part of the command output includes a statement that indicates how long the LEC has been operating, such as "LEC up for 8 hours 41 minutes." The current MIBS, such as interface MIBS, ATM MIBS, and the LEC MIB do not have this support.

Workaround: None.

Release 12.0(20)W5(24a)

These sections describe the open and resolved caveats in Release 12.0(20)W5(24a) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(20\)W5\(24a\), page 22](#)
- [Resolved Caveats in Release 12.0\(20\)W5\(24a\), page 23](#)

Open Caveats in Release 12.0(20)W5(24a)

This section describes the open caveats in Release 12.0(20)W5(24a):

- CSCdw65903

An error can occur with management protocol processing. Use this URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

- CSCds22874

When an LEC on a Cisco device receives wrongly formatted LANE control frames, this message is generated:

```
%LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
```

When the message is generated, LECs may be shut down and brought up again.

Workaround: None.

Resolved Caveats in Release 12.0(20)W5(24a)

This section describes the resolved caveats in Release 12.0(20)W5(24a):

- CSCdw65903

An error can occur with management protocol processing. Use the following URL for further information: <http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

Release 12.0(20)W5(24)

These sections describe the open and resolved caveats in Release 12.0(20)W5(24) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(20\)W5\(24\), page 23](#)
- [Resolved Caveats in Release 12.0\(20\)W5\(24\), page 23](#)

Open Caveats in Release 12.0(20)W5(24)

This section describes the open caveats in Release 12.0(20)W5(24):

- CSCds22874

When an LEC on a Cisco device receives wrongly formatted LANE control frames, the following message is generated:

```
%LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
```

When the message is generated, LECs may be shut down and brought up again.

Workaround: None.

Resolved Caveats in Release 12.0(20)W5(24)

This section describes the resolved caveats in Release 12.0(20)W5(24):

- CSCdv38277

Under rare circumstances, the Catalyst 5000 ATM LANE module x5161 running Release 12.0(14)W5(20) continues to generate the following messages on enabling the **debug lane client state** command:

```
state ACTIVE event LEC_CTL_TOPO_CHANGE => ACTIVE
```

This message indicates that it may be considering all BPDUs to be Topology Change messages.

Workaround: None.

Release 12.0(19)W5(23)

These sections describe the open and resolved caveats in Release 12.0(20)W5(24) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(19\)W5\(23\), page 24](#)
- [Resolved Caveats in Release 12.0\(19\)W5\(23\), page 24](#)

Open Caveats in Release 12.0(19)W5(23)

This section describes the open caveats in Release 12.0(19)W5(23):

- CSCds22874

When an LEC on a Cisco device receives wrongly formatted LANE control frames, the following message is generated:

```
%LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
```

When the message is generated, LECs may be shut down and brought up again.

Workaround: None.

- CSCdt07993

In a Catalyst 5000 family switch that contains an ATM module (WS-X516xx), the CAM entry for a MAC address may change from LANE Data Direct VC to LANE BUS VC, or vice versa, and it may update the CAM entry with the LANE Data Direct VC when there is traffic to that MAC address.

Workaround: None.

Resolved Caveats in Release 12.0(19)W5(23)

This section describes the resolved caveats in Release 12.0(19)W5(23):

- CSCdu79955

When there are many PVC to VLAN bindings, the ATM module will not come back on line when the module is reloaded.

Workaround: Copy the startup configuration to the running configuration using the **copy startup-config running-config** command on ATM module.

- CSCdu79572

When using the **show running-config** command, the ATM modules display a random listing of PVCs.

- CSCdu47929

The ATM module is not connected for some VLANs when the module running the Release 12.x is reloaded. This problem occurs in the following situations:

- When the Catalyst 5500 switches contain the SM OC-3 dual PHY ATM (WS-X5157) or the MM OC-3 Dual-Phy ATM (WS-X5158) modules.
- When the ATM module is running LANE instead of PVCs.
- When spanning tree is disabled on the switch.

Workaround:

Clear this problem as follows:

- Remove the VLAN from the trunk, and then reinstall that same VLAN onto the trunk.
- Remove the binding from the ATM configuration, and then replace the binding.

- CSCdv45391

On Catalyst 5000 family and Catalyst 6000 family ATM modules, when the startup configuration has shut down for an interface, the ATM PVC and VLAN bindings are lost from the running configuration when the **no shut** command is performed. This problem has been fixed.

Workaround: Copy a configuration from the TFTP location without the **shut** command, or load an older image.

- CSCdv22085

When VBR-nrt traffic shaping is configured on an ATM module without a maximum burst size (MBS) value, a value of 0 is assigned to that module. Traffic sent on this permanent virtual circuit (PVC) never spikes at peak cell rate (PCR) since MBS is always 0.

- CSCdv12211

When a Catalyst 5500 switch is using an OC-3 ATM LAN Emulation (LANE) module (WS-X5158) that is running Cisco IOS Release 12.0(16)W5(21), the default rate queue cannot be configured if both of the special rate queues have already been configured.

This error message displays when you attempt to add additional PVCs:

```
Not creating vc:xx interface: ATM0 is out of rate queues.
```

Workaround: None.

- CSCdv02245

When you configure many sub-interfaces on the LANE module, reloading the module with 12.0(14)W5(20) software causes the LANE module to lock up, preventing access to the module from the supervisor. This problem is fixed in Release 12.0(19)W5(23) and Release 12.1(10)E.

Workaround: None.

Release 12.0(18)W5(22)

These sections describe the open and resolved caveats in Release 12.0(18)W5(22) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(18\)W5\(22\), page 25](#)
- [Resolved Caveats in Release 12.0\(18\)W5\(22\), page 26](#)

Open Caveats in Release 12.0(18)W5(22)

This section describes the open caveats in Release 12.0(18)W5(22):

- CSCds22874

When an LEC on a Cisco device receives wrongly formatted LAN emulation control frames, this message is generated:

```
%LANE-3-LEC_CONTROL_MSG: Received bad control message on interface ATM1/0.101
```

When the message is generated, LECs may be shut down and brought up again.

Workaround: None.

- CSCdt07993

In a Catalyst 5000 family switch that contains an ATM module (WS-X516xx), the CAM entry for a MAC address may change from LANE Data Direct VC to LANE BUS VC, or vice versa, and it may update the CAM entry with the LANE Data Direct VC when there is traffic to that MAC address.

Workaround: None.

Resolved Caveats in Release 12.0(18)W5(22)

This section describes the resolved caveats in Release 12.0(18)W5(22):

- CSCds07238

According to RFC 1573, support for 64-bit octet counters in the ifXTable is required for the ATM module interface. However, although 32-bit counters in the ifTable are supported, support for the corresponding 64-bit counter variables is missing.

Workaround: None.

- CSCdt93862

When you enable an HTTP server and use local authorization, it is possible, under some circumstances, to bypass the authentication and execute any command on the device. In that case, the user will be able to have complete control over the device. All commands will be executed with the highest privilege (level 15).

All Cisco IOS software releases, starting with release 11.3 and later, are vulnerable. All mainstream Cisco routers and switches running Cisco IOS software are affected by this vulnerability.

Products that are not running Cisco IOS software are not vulnerable.

Workaround: Disable the HTTP server on the router or use Terminal Access Controller Access Control System (TACACS+) or RADIUS for authentication.

Release 12.0(16)W5(21)

These sections describe the open and resolved caveats in Release 12.0(16)W5(21) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(16\)W5\(21\), page 26](#)
- [Resolved Caveats in Release 12.0\(16\)W5\(21\), page 27](#)

Open Caveats in Release 12.0(16)W5(21)

This section describes the open caveats in Release 12.0(16)W5(21):

- CSCds07238

According to RFC 1573, support for 64-bit octet counters in the ifXTable is required for the ATM module interface. However, although 32-bit counters in the ifTable are supported, support for the corresponding 64-bit counter variables is missing.

Workaround: None.

- CSCdt07993

In a Catalyst 5000 family switch that contains an ATM module (WS-X516xx), the CAM entry for a MAC address may flip between LANE Data Direct VC and LANE BUS VC, and it may update the CAM entry with the LANE Data Direct VC when there is traffic to that MAC address.

Workaround: None.

Resolved Caveats in Release 12.0(16)W5(21)

This section describes the resolved caveats in Release 12.0(16)W5(21):

- CSCdj81449

The **show atm interface atm0** command does not display the special rate queues with data rates less than 2081 kbps for OC-3 interfaces and less than 2354 kbps for DS3 interfaces.

- CSCdm80818

With any module from the WS-X516xx line, the following message could appear in the log while the switch is running MPOA.

```
Aug 7 17:54:12 202.40.192.20 23: Aug 7 17:53:31: %MPOA-3-MPC_ERROR:
mpc_hw_get_vc_local_index: tke_aalsap_get_local_index for port 0 vcd 64
failed: returned error 9
```

However, this message does NOT change the existing functionality of LANE/MPOA. This message is converted as a debug message in Release 12.0(16)W5(21) and later.

- CSCds79580

On Catalyst 5000 family platforms, the system CAM entries created by MPOA are not removed when the ATM module is removed, reset, reloaded, or when the ATM module hangs.

Workaround: Reload the Catalyst 5000 family platform.

- CSCdt93822

The following configuration is on WS-X516* WS-515xx:

- interface ATM0
- atm pvc 1 0 5 qsaal
- atm pvc 2 0 16 ilmi

This configuration appears in the running configuration even when it does not appear in the startup configuration. This problem exists in Release 12.0(14)W5(20) and earlier releases. It has been fixed in Release 12.0(16)W5(21). You must set up QSAAL and ILMI PVCs, either in the startup configuration or in the running configuration using CLI.

- CSCdt79947

A BGP configuration with route-map configured is susceptible to memory corruption.

- CSCdt62368

On Catalyst 5500 switches, the FIM module (WS-X5165) loses the ILMI prefix. This problem occurs when more than 30 LECs are configured and when the LECs go down.

- CSCdt31428

In the Catalyst 5000 family ATM modules, the ATM PVC to VLAN binding is lost when you perform repeated **shut** and **no shut** commands on the main interface. This problem has occurred on the Release 12.0(13)W5(19) image.

Workaround: If you used the **wr mem** command prior to the problem, the PVC to VLAN bindings can be restored from the NVRAM configuration using the **copy startup running** command.

- CSCdt19422

A WS-X6101 configured as a LANE v2 client in a multivendor LANE environment may experience interoperability problems when the LECS and LES/BUS services reside on the third-party equipment. The WS-X6101 will send out a tag value in the LAN destination field of the flush request that is not recognized as an appropriate value by the third party BUS.

Workaround: Disable the flush request sent by the client on the WS-X6101.

Release 12.0(14)W5(20)

These sections describe the open and resolved caveats in Release 12.0(14)W5(20) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(14\)W5\(20\), page 28](#)
- [Resolved Caveats in Release 12.0\(14\)W5\(20\), page 28](#)

Open Caveats in Release 12.0(14)W5(20)

This section describes the open caveats in Release 12.0(14)W5(20):

- CSCdt07993
In a Catalyst 5000 family switch that contains an ATM module (WS-X516*), the CAM entry for a MAC address may flip between LANE Data Direct VC and LANE BUS VC and update the CAM entry with the LANE Data Direct VC when there is traffic to that MAC address.
Workaround: None
- CSCdt31428
In the Catalyst 5000 family ATM modules, the ATM PVC to VLAN binding is lost when you perform repeated **shut** and **noshut** commands on the main interface. This problem has occurred on the Release 12.0(13)W5(19) image.
Workaround: If you used the **wr mem** command prior to the problem, the PVC to VLAN bindings can be restored from the NVRAM configuration using the **copy startup running** command.
- CSCds07238
According to RFC 1573, support for 64-bit octet counters in the ifXTable is required for the ATM module interface. However, although 32-bit counters in the ifTable are supported, support for the corresponding 64-bit counter variables is missing.
- CSCds79580
On Catalyst 5000 family platforms, the system CAM entries created by MPOA are not removed when the ATM module is removed, reset, reloaded, or when the ATM module hangs.
Workaround: Reload the Catalyst 5000 family platform.
- CSCds21577
The WS-X5161 and WS-X 5162 modules produce CPUHOG messages if the interface shuts down and is brought up with a high number of PVCs configured on the ATM interface. This problem occurs when there are approximately 2,400 or more PVCs configured on the interface.

Resolved Caveats in Release 12.0(14)W5(20)

This section describes the resolved caveats in Release 12.0(14)W5(20):

- CSCdr54230
A Border Gateway Protocol (BGP) update contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the extended length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems in the segment. The path segment value contains the list of autonomous systems (each autonomous system is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of autonomous systems in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of autonomous systems (without having to use the extended length bit) is 126 [= (255-2)/2]. If the update is propagated across an autonomous system boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The problem was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a notification message (update malformed) to reset their session.

The average maximum AS_PATH length in the Internet is between 15 and 20 autonomous systems, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

(Part of the text was taken from RFD 1771.)

- CSCdr54231

When BGP sessions get reset with log neighbor-changes, the event is error logged. Turn on debugging to find out why there was a reset. This fix will automatically error log the notification message when the sessions are reset. This feature will be turned on by the same log-neighbor-changes knob.

- CSCds04747

Cisco Security Advisory:

Cisco IOS Software TCP Initial Sequence Number Randomization Improvements

Revision 1.0: INTERIM

For Public Release 2001 February 27 20:00 US/Eastern (UTC+0500)

Summary

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

- CSCdt36407

In the Catalyst 5000 family ATM OC-3 module (WS-X5167), switchover does not happen on an ILMI keepalive failure in c5atm-lc-mz Release 12.0(14)W5(19).

- CSCdt35074

On the WS-X5167 module, the SNMP set operation on cadpStatAdminActivePhy MIB variable fails. The ATM preferred physical sublayer (PHY) cannot be changed using SNMP. This set operation works fine with WS-X5158, WS-X5161, and WS-X5166 ATM modules but fails with the WS-5167 module.

Workaround: Use the **atm preferred phy** command on the command-line interface.

- CSCds76508

When the BUS, RSAR (3.2.1.2) is oversubscribed, it continuously drops packets and it never recovers. LECs or any PVCs present go down and all incoming traffic is dropped.

- CSCdt35067

In the Catalyst 5000 family ATM DS3 module (WS-X5166) and OC-3 module (WS-X5158), the command **atm bind pvc vlan x y** does not work properly on major interface in c5atm-wt-mz and c5atm-wl-mz Release 12.0(14)W5(19).

- CSCdt15587

Switchover does not happen on an ILMI keepalive failure.

Workaround: Use images from 12.1(6)E or 12.0(14)W5(20) or later releases on the ATM modules.

- CSCdt13237

In the Catalyst 5000 family ATM DS3 module (WS-X5166), the command **atm bind pvc vlan x y** does not work properly in the c5atm-wt-mz Release 12.0(14)W5(19).

- CSCdt00616

In the Catalyst 5000 family ATM DS3 module (WS-X5166), the command **atm ds3-scramble** does not program the PHY chip in the scrambling mode. This problem causes data loss if the other end is in scrambling mode.

Workaround: Disable scrambling at the other end.

- CSCdt11082

SNMP fails on the WS-X5165 module. None of the MIB variables can be queried from this module.

Release 12.0(13)W5(19)

These sections describe the open and resolved caveats in Release 12.0(13)W5(19) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(13\)W5\(19\), page 32](#)
- [Resolved Caveats in Release 12.0\(13\)W5\(19\), page 32](#)

Open Caveats in Release 12.0(13)W5(19)

This section describes the open caveats in Release 12.0(13)W5(19):

- CSCds21577
The WS-X5161 and WS-X 5162 modules produce CPUHOG messages if the interface shuts down and is brought up with a high number of PVCs configured on the ATM interface. This problem occurs when approximately 2,400 or more PVCs are configured on the interface.
- CSCds07238
According to RFC 1573, support for 64-bit octet counters in the ifXTable is required for the ATM module interfaces. However, although 32-bit counters in the ifTable are supported, support for the corresponding 64-bit counter variables is missing.

Resolved Caveats in Release 12.0(13)W5(19)

This section describes the resolved caveats in Release 12.0(13)W5(19):

- CSCdm84276
PVC performance may decrease below the 176 Kpps line rate to 131 Kpps under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).
- CSCdp78464
Occasionally, the interface speed is shown as zero for an ATM link connecting a Catalyst 5000 family switch and a LightSpeed 1010 switch.
- CSCdr81332
An MPOA client configured on WS-X516X modules installed in a Catalyst 5509 or a Catalyst 5550 switch might not forward the packets over an MPOA shortcut or might drop the packets under the following conditions:
 - When the supervisor engine on the Catalyst 5000 family switch creates system CAM entries for MPOA.
 - When the MPOA configuration is done while the packets are forwarded through LANE data direct VCCs.

Workaround: Reboot the Catalyst 5000 family switch after the MPOA configuration is done.

Upgrade the software on WS-X516X modules and the Catalyst 5000 family supervisor engine image to the latest releases. Valid supervisor engine images are 4-5-10, 5-5-4, 6-1-2, and later releases. Valid releases for WS-X516X images are 12.0-13.W5.19, 12.1(4)E1, and later releases.
- CSCdr97857
Currently, the PVC-shaping feature on the Catalyst 5000 family LANE modules supports queuing of 20 packets per VC only. The PVC shaping feature should support configuring the depth of the per-VC queues.
- CSCdr12489
When several 1483 traffic-shaped PVCs with different rate queues are configured, the WS-X515X modules might send out frames that fail the AAL5 CRC performed by connecting devices.
- CSCds19513
The WS-X5158 module may respond to LE-ARPs in VLANs that are in the blocking state. This problem may lead to intermittent connectivity problems.

- CSCds21593

If you configure a high number (2500) of traffic-shaped PVCs on a WS-X5162 or WS-X5161 module and allow very high traffic on the PVCs, the LANE module performance degrades and resets. The last reset reason indicates a TXHOST timeout.

- CSCds52050

On a WS-X515x LANE or WS-X516x module running Release 12.0(10)W5(18a) with the **lane config config-atm-address** <47.....> command or the **lane config fixed-config-atm-address** command configured, entering the **shut** and **no shut** commands on the ATM interface causes the module to get stuck in a constant boot process that cannot be stopped by any break sequence.

Workaround: Configure the LECS address in the ATM switch using the following command: **atm lecs-address-default** *lecs NSAP address*.

Release 12.0(10)W5(18a)

These sections describe the open and resolved caveats in Release 12.0(10)W5(18a) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(10\)W5\(18a\), page 33](#)
- [Resolved Caveats in Release 12.0\(10\)W5\(18a\), page 34](#)

Open Caveats in Release 12.0(10)W5(18a)

This section describes the open caveats in Release 12.0(10)W5(18a).

- CSCdm84276

PVC performance may decrease below the 176 Kpps line rate to 131 Kpps under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).

- For the ATM dual PHY OC-12 module, when the (nonactive) redundant PHY is connected to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time there is only one PHY active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. We recommend that you perform single downloads to the ATM Fabric Integration Modules if there are more than 100 LECs.
- When a large number of VLANs are configured on the ATM Fabric Integration Module, doing a fast switchover of the supervisor engines can cause the LECs to go down and come up.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10) and later:
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.
 - The **set preferred phy** command is not supported.
 - The **show controller** command output does not display the PHY error counters for the internal ATM port.

Resolved Caveats in Release 12.0(10)W5(18a)

This section describes the open caveats in Release 12.0(10)W5(18a):

- CSCdj57154
The current VC counters value displayed by the **show interface atm0** and the **show atm interface atm0** commands are incorrect. Use the **show atm vc** command instead.
- CSCdr26349
The WS-X5167 module resets after you enter a writeNet SNMP request.
- CSCdr06796
The CLI does not allow users to disable the LEC LE-Flush mechanism. The new **[no] lane client flush** command in Release 12.0(10)W5(18a) resolves this problem.

Release 12.0(9)W5(17a)

These sections describe the open and resolved caveats in Release 12.0(9)W5(17a) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(9\)W5\(17a\), page 34](#)
- [Resolved Caveats in Release 12.0\(9\)W5\(17a\), page 35](#)

Open Caveats in Release 12.0(9)W5(17a)

This section describes the open caveats in Release 12.0(9)W5(17a):

- CSCdm84276
PVC performance may decrease below the 176 Kpps line rate to 131 Kpps under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).
- For the ATM dual PHY OC-12 module, when the (nonactive) redundant PHY is connected to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time there is only one PHY active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. We recommend that you perform single downloads to the ATM Fabric Integration Modules if there are more than 100 LECs.
- When you configure a large number of VLANs on the ATM Fabric Integration Module, doing a fast switchover of the supervisor engines can cause the LANE servers and LECs to go down and come up.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10) and later:
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.
 - The **set preferred phy** command is not supported.
 - The **show controller** command output does not display the PHY error counters for the internal ATM port.

- CSCdj57154

The current VC counters value displayed by the **show interface atm0** and the **show atm interface atm0** commands are incorrect. Use the **show atm vc** command instead.

Resolved Caveats in Release 12.0(9)W5(17a)

This section describes the open caveats in Release 12.0(9)W5(17a).

- CSCdr36952

A defect in multiple versions of Cisco IOS software will cause a Cisco router or switch to stop and reload if the Cisco IOS http service is enabled and an attempt is made to browse to `http://<router-ip`. This defect can be exploited to produce a denial of service (DoS) attack. This defect has been discussed on public mailing lists and is public information.

The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS Release 11.1 through Release 12.1. The vulnerability has been corrected, and Cisco is making fixed versions available to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect.

Workaround: Nullify the vulnerability by disabling the Cisco IOS HTTP server, by preventing access to the port in use by the HTTP server on the affected router or switch, or by applying an access-class option to the service itself. The Cisco IOS HTTP server is not enabled by default except on a small number of router models in specific circumstances.

See <http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml> for the latest complete version of this security advisory.

Release 12.0(9)W5(17)

These sections describe the open and resolved caveats in Release 12.0(9)W5(17) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(9\)W5\(17\), page 35](#)
- [Resolved Caveats in Release 12.0\(9\)W5\(17\), page 36](#)

Open Caveats in Release 12.0(9)W5(17)

This section describes the open caveats in Release 12.0(9)W5(17).

- CSCdm84276

PVC performance may decrease below the 176 Kpps line rate to 131 Kpps under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).

- For the ATM dual PHY OC-12 module, when the (nonactive) redundant PHY is connected to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time there is only one PHY active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. We recommend that you perform single downloads to the ATM Fabric Integration Modules if there are more than 100 LECs.

- When you configure a large number of VLANs on the ATM Fabric Integration Module, doing a fast switchover of the supervisor engines can cause the LANE servers and LAN Emulation Clients to go down and come up.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10) and later:
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.
 - The **set preferred phy** command is not supported.
 - The **show controller** command output does not display the PHY error counters for the internal ATM port.
- CSCdj57154

The current VC counters value displayed by the **show interface atm0** and the **show atm interface atm0** commands are incorrect. Use the **show atm vc** command instead.

Resolved Caveats in Release 12.0(9)W5(17)

This section describes the open caveats in Release 12.0(9)W5(17).

- CSCdp11306

Fast Simple Server Redundancy Protocol (FSSRP) does not scale well when there are more than 30 LES/BUS pairs configured on a LANE module. In a configuration with over 30 LES/BUS pairs, some LECs might fail if there is an LES/BUS switchover.

Workaround: Limit the number of LES/BUS pairs per LANE module to 30.
- CSCdp96261

Catalyst 5000 family ATM modules WS-X5161, WS-X5165, and WS-X5167 running Release 12.0(7)W5(15b) are sometimes unable to send or receive traffic on a data direct VC.
- CSCdp82703

In Catalyst 5000 family ATM modules WS-X5161, WS-X5165, and WS-X5167, packets smaller than 64 bytes sent over RFC 1483 PVCs are forwarded to the backplane without being padded for the minimum length (64 bytes).
- CSCdr25351

When a **getmany** operation is performed on SNMP Version 2C variables supported in the Catalyst 5000 family ATM modules, a memory leak is observed.

Release 12.0(7)W5(15b)

These sections describe the open and resolved caveats in Release 12.0(7)W5(15b) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12.0\(7\)W5\(15b\), page 37](#)
- [Resolved Caveats in Release 12.0\(7\)W5\(15b\), page 37](#)

Open Caveats in Release 12.0(7)W5(15b)

This section describes the open caveats in Release 12.0(7)W5(15b).

- CSCdk41799
If you download a configuration that creates more than 4000 PVCs with OAM enabled to a Catalyst 5000 family OC-12 ATM module using the **copy tftp running** command, the ATM module may reset.
- CSCdm84276
PVC performance may decrease below the 176 Kpps line rate to 131 Kpps under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).
- CSCdp11306
Fast Simple Server Redundancy Protocol (FSSRP) does not scale well when there are more than 30 LES/BUS pairs configured on a LANE module. In a configuration with over 30 LES/BUS pairs, some LECs might fail if there is a LES/BUS switchover.
Workaround: Limit the number of LES/BUS pairs per LANE module to 30.
- For the ATM dual PHY OC-12 module, when the (nonactive) redundant PHY is connected to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time there is only one PHY active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. We recommend that you perform single downloads to the ATM Fabric Integration Modules if there are more than 100 LECs.
- When you configure a large number of VLANs on the ATM Fabric Integration Module, doing a fast switchover of the supervisor engines can cause the LANE servers and LAN Emulation Clients to go down and come up.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10):
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.
 - The **set preferred phy** command is not supported.
 - The **show controller** command output does not display the PHY error counters for the internal ATM port.
- CSCdj57154
The current VC counters value displayed by the **show interface atm0** and the **show atm interface atm0** commands are incorrect. Use the **show atm vc** command instead.

Resolved Caveats in Release 12.0(7)W5(15b)

This section describes the open caveats in Release 12.0(7)W5(15b).

- CSCdp25461
When the LECS goes down, some of the LECs lose their connections to some of the servers. This problem might result in the LECs going down when the LECS comes up again, even if FSSRP is enabled.

- CSCdp66265
In some situations, an LES receives a configuration response with the FSSRP TLV not containing its address. This problem causes the LES to tear down all its connections, which might bring down an LEC.
- CSCdk76407
When PVCs are configured on a subinterface on the Catalyst 5000 family ATM module, entering **shutdown** and **no shutdown** commands on that subinterface deletes and recreates all configured PVCs in that subinterface. The PVCs stop transmitting and receiving packets and they lose their bindings to VLANs.
Workaround: Enter the **atm pvc vlan** command to manually create the PVC-to-VLAN bindings. We recommend that you configure PVCs on the major interfaces; do not perform **shutdown** and **no shutdown** commands on the subinterfaces.
- CSCdp26510
On a Catalyst 5000 family ATM module, you cannot create PVCs using the multistep process defined in CISCO-ATM-PVC-MIB.
- CSCdm60158
The OC-12 MPOA/LANE module failed to respond to an LE-ARP request because of a Fast-PHY switchover. When the LEC is removed and then quickly configured, the port status change does not take place. The LEC comes up with spanning tree in the blocked state, but the supervisor engine does not move the LEC port into the forwarding state.
- CSCdm61379
Traffic is sent over the BUS VC even though a data direct VC is established. In some cases, an LE-ARP may be requested for a MAC address when a MAC address already exists.
- CSCdm87739
The following warning message appears on the screen when there are more than 4000 ingress/egress caches:

```
%SYS-3-CPUHOG:Task ran for 3060 msec (0/0), process =  
MPOA Client, PC = 40095C82.
```
- CSCdp01039
An LEC is stuck in initialState after SSCOP failure.
- CSCdp04835
MPC does not work correctly on the blocked VLAN. If an LEC is blocked, no data should be switched on this interface. Because of this bug, the MPC bound on this subinterface is still working and MPOA packets are still switched.
- CSCdp07158
The **atm PVC bind** command reappears after it is deleted when the fiber connection is disconnected and then reconnected again.
- CSCdp80442
When an MPS has been removed but packets are still arriving destined for that MPS, the following error message displays:

```
%MPOA-3-MPC_ERROR:mpc_process_flow_t:imac from cookie 258 not found
```

This error message is generated because the transmit host is not aware that the MPS has been removed. The error message disappears after the transmit host learns of the MPS configuration change.

- CSCdp12241

If only LANE is configured and if the LECID is not zero, the system runs out of memory and crashes.

- CSCdp16491

A problem with the compare routine causes the egress cache (dest_mac_t) to be out of order. This problem may cause the system to crash.

- CSCdp34774

The Catalyst 5000 family ATM module does not provide the ATM switch connected to it with the supervisor engine IP address.

Release 12(4a)W5(10)

These sections describe the open and resolved caveats in Release 12.0(4a)W5(10) for the Catalyst 5000 series ATM modules:

- [Open Caveats in Release 12\(4a\)W5\(10\), page 39](#)
- [Resolved Caveats in Release 12\(4a\)W5\(10\), page 40](#)

Open Caveats in Release 12(4a)W5(10)

This section describes open caveats in Release 12.0(4a)W5(10):

- CSCdm84276

PVC performance may decrease below the 176K packets per second line rate to 131K packets per second under heavy traffic with more than one Fast Ethernet stream on the OC-3 MMF and SMF modules (WS-X5167 and WS-X5168).

- For the ATM dual PHY OC-12 module when the (nonactive) redundant PHY is connected to a LightStream 1010 OC-12 PAM, that LightStream 1010 OC-12 PAM's port may show a red alarm LED because at any time there is only one PHY active in the ATM dual PHY OC-12 module. This red alarm LED does not indicate a loss-of-frame condition.
- When you have a large number (more than 100) of LECs on the ATM Fabric Integration Module, downloading a Flash image to multiple ATM Fabric Integration Modules can increase the time it takes the modules to come online. We recommend that you perform single downloads to the ATM Fabric Integration Modules if there are more than 100 LECs.
- When a large number of VLANs are configured on the ATM Fabric Integration Module, performing a fast switchover of the supervisor engines can cause the LANE servers and LAN Emulation Clients to go down and come up.
- The following applies to the ATM Fabric Integration Module in Release 12.0(4a)W5(10):
 - The **set clock** command is not supported.
 - The **set sonet mode** command is not supported.
 - The **set preferred phy** command is not supported.
 - The **show controller** command output does not display the PHY error counters for the internal ATM port.

- CSCdk76407
When PVCs are configured on a subinterface on the Catalyst 5000 family ATM module, entering **shutdown** and **no shutdown** commands on that subinterface deletes and recreates all configured PVCs in that subinterface. PVCs stop transmitting and receiving packets and they lose their bindings to VLANs.
Workaround: Enter the **atm pvc vlan** command to manually create the PVC-to-VLAN bindings. We recommend that you configure PVCs on the major interfaces: do not perform **shutdown** and **no shutdown** commands on the subinterfaces.
- CSCdj81931
Octet counters are not supported.
- CSCdj57154
The current VC counters value displayed by the **show interface atm0** and the **show atm interface atm0** commands are incorrect. Use the **show atm vc** command instead.

Resolved Caveats in Release 12(4a)W5(10)

There are no resolved caveats in Release 12(4a)W5(10).

Related Documentation

The following documents are available for the Catalyst 5000 family switch:

- *Catalyst 5000 Family Quick Software Configuration*
- *Catalyst 5000 Family Installation Guide*
- *Catalyst 5000 Family Module Installation Guide*
- *Catalyst 5000 Family Software Configuration Guide*
- *Catalyst 5000 Family Command Reference*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 5000 Family Release Notes*
- *Enterprise MIB User Quick Reference* (online only)

For information on how to install and configure the Catalyst 5000 family ATM modules, refer to the *Catalyst 5000 Family Module Installation Guide*.

For information on how to access the ATM module command-line interface (CLI) and customize the configuration from the terminal and from nonvolatile RAM (NVRAM), refer to these publications:

- *Catalyst 5000 Family Software Configuration Guide*
- *Catalyst 5000 Family Command Reference*

For quick software configuration procedures for the Catalyst 5000 family switches, refer to the *Quick Software Configuration Guide* for your switch. For detailed software configuration information and procedures, refer to the *Software Configuration Guide* for your switch.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

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

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

© 2000—2005 Cisco Systems, Inc. All rights reserved.