

# Release Notes for Cisco 7304 router for Cisco IOS Release 12.1 EX

---

July 17, 2003

Cisco IOS Release 12.1(13)EX3

OL-1793-13

These release notes for the Cisco 7304 router describe the enhancements provided in Cisco IOS Release 12.1(13)EX3. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.1(13)EX3, see the [“Important Notes” section on page 25](#) and *Caveats for Cisco IOS Release 12.1*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.1* located on Cisco.com and the Documentation CD-ROM.

## Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 10](#)
- [MIBs, page 24](#)
- [Important Notes, page 25](#)
- [Caveats for Cisco IOS Release 12.1 EX, page 29](#)
- [Related Documentation, page 65](#)
- [Obtaining Documentation, page 71](#)
- [Obtaining Technical Assistance, page 72](#)



---

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

Copyright © 2002-2003. Cisco Systems, Inc. All rights reserved.

# System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(13)EX3 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 7](#)
- [Determining the Software Version, page 7](#)
- [Upgrading to a New Software Release, page 7](#)
- [Feature Set Tables, page 8](#)

## Memory Recommendations

**Table 1** Images and Memory Recommendations for Cisco IOS Release 12.1(13)EX3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
	Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM

**Table 2** Images and Memory Recommendations for Cisco IOS Release 12.1(13)EX2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 3** Images and Memory Recommendations for Cisco IOS Release 12.1(13)EX1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 4 Images and Memory Recommendations for Cisco IOS Release 12.1(13)EX**

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 5 Images and Memory Recommendations for Cisco IOS Release 12.1(12c)EX1**

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 6** Images and Memory Recommendations for Cisco IOS Release 12.1(12c)EX

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 7** Images and Memory Recommendations for Cisco IOS Release 12.1(10)EX2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 56	c7300-io3s56i-mz	64 MB	128 MB	RAM
		IP/FW/IDS IPSec 3DES	c7300-ik2o3s-mz	64 MB	128 MB	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS IPSec 56	c7300-jo3s56i-mz	64 MB	128 MB	RAM
		Enterprise/FW/IDS IPSec 3DES	c7300-jk2o3s-mz	64 MB	128 MB	RAM
Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM	

**Table 8** Images and Memory Recommendations for Cisco IOS Release 12.1(10)EX1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM

**Table 9** Images and Memory Recommendations for Cisco IOS Release 12.1(10)EX

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM
	Enterprise/SNASW Standard Feature Set	SNASW	c7300-a3js-mz	64MB	128MB	RAM

**Table 10** Images and Memory Recommendations for Cisco IOS Release 12.1(9)EX3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM

**Table 11** Images and Memory Recommendations for Cisco IOS Release 12.1(9)EX2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM

**Table 12** Images and Memory Recommendations for Cisco IOS Release 12.1(9)EX1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7300 Series	IP Standard Feature Set	IP	c7300-is-mz	64MB	128MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64MB	128MB	RAM

## Supported Hardware

Cisco IOS Release 12.1(13)EX3 supports the following Cisco 7000 platform:

- Cisco 7304 router

For detailed descriptions of the new hardware features, see the “[New and Changed Information](#)” section on page 10.

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7304 router, log in to the Cisco 7304 router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7304 software image with Cisco IOS Release 12.1(13)EX3:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7304 Software (c7300-is-mz), Version 12.1(13)EX3, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to Software Advisor located at: <http://tools.cisco.com/Support/Fusion/FusionHome.do>

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.1(13)EX3 supports the same feature sets as Cisco IOS Release 12.1, but Cisco IOS Release 12.1(13)EX3 can include new features supported by the Cisco 7304 router.



### Caution

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

Table 13 through Table 14 lists the features and feature sets supported by the Cisco 7304 router in Cisco IOS Release 12.1(13)EX3 and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (10)EX2 means a feature was introduced in 12.2(10)EX2.

**Table 13 Feature List by Feature Set for the Cisco 7304 Series**

Features	In	Software Images by Feature Sets			
		IP	Enterprise	IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES
<b>PXF Processor Accelerated</b>					
ACL Accounting	(10)EX	Yes	Yes	No	No
Cisco IOS IEEE 802.1Q Support	(10)EX1	Yes	Yes	No	No
Frame Relay Interfaces for PXF Support	(10)EX2	Yes	Yes	Yes	Yes
Generic Routing Encapsulation	(13)EX	Yes	Yes	Yes	Yes
ICMP Handling	(10)EX	Yes	Yes	No	No
MPLS Experimental Bit Matching and Marking on PXF	(12c)EX1	Yes	Yes	Yes	Yes
Multiprotocol Label Switching (MPLS) and MPLS VPN on PXF	(12c)EX	Yes	Yes	Yes	Yes
Netflow Version 5 on PXF	(13)EX	Yes	Yes	Yes	Yes
Network Address Translation on PXF	(12)EX	Yes	Yes	Yes	Yes
Parallel eXpress Forwarding (PXF)	(9)EX1	Yes	Yes	No	No
Traffic Policing	(10)EX1	Yes	Yes	No	No
Quality of Service for Parallel eXpress Forwarding	(9)EX2	Yes	Yes	No	No
Unicast Reverse Path Forwarding	(10)EX1	Yes	Yes	No	No
Weighted Random Early Detection	(10)EX2	Yes	Yes	Yes	Yes

**Table 13 Feature List by Feature Set for the Cisco 7304 Series**

Features	In	Software Images by Feature Sets			
		IP	Enterprise	IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES
<b>IOS Based</b>					
Cisco 7300 Series High Availability NSE Redundancy	(10)EX2	Yes	Yes	Yes	Yes
Cisco 7300 Series Power-On Diagnostics	(10)EX2	Yes	Yes	Yes	Yes
FPGA Bundling and Update	(10)EX	Yes	Yes	No	No
POS Alarm Trigger Delay	(12c)EX1	Yes	Yes	Yes	Yes
show redundancy command enhancements	(12c)EX1	Yes	Yes	Yes	Yes
T3 Bit Error Rate Testing	(12c)EX1	Yes	Yes	Yes	Yes
T3 Maintenance Data Link Messages on the Cisco 7304 Router	(13)EX	Yes	Yes	Yes	Yes
Increased number of traffic classes per policy map in PXF	(12c)EX1	Yes	Yes	Yes	Yes
MPLS Load Balancing on PXF	(12c)EX1	Yes	Yes	Yes	Yes

**Table 14 Feature List by Feature Set for the Cisco 7304 Series, Part 2 (continued)**

Features	In	Software Images by Feature Sets			
		Enterprise/ FW/IDS IPSec 56	Enterprise/F W/IDS IPSec 3DES	SNASW	
<b>PXF Processor Accelerated</b>					
ACL Accounting	(10)EX	No	No	Yes	
Cisco IOS IEEE 802.1Q Support	(10)EX1	No	No	Yes	
Frame Relay Interfaces for PXF Support	(10)EX2	Yes	Yes	Yes	
Generic Routing Encapsulation	(13)EX	Yes	Yes	Yes	
ICMP Handling	(10)EX	No	No	Yes	
MPLS Experimental Bit Matching and Marking on PXF	(12c)EX1	Yes	Yes	Yes	
Multiprotocol Label Switching (MPLS) and MPLS VPN on PXF	(12c)EX	Yes	Yes	Yes	
Netflow Version 5 on PXF	(13)EX	Yes	Yes	Yes	
Network Address Translation on PXF	(12c)EX	Yes	Yes	Yes	
Parallel eXpress Forwarding (PXF)	(9)EX1	No	No	No	
Quality of Service for Parallel eXpress Forwarding	(9)EX2	No	No	No	
Traffic Policing	(10)EX1	No	No	Yes	
Unicast Reverse Path Forwarding	(10)EX1	No	No	Yes	
Weighted Random Early Detection	(10)EX2	Yes	Yes	Yes	

**Table 14 Feature List by Feature Set for the Cisco 7304 Series, Part 2 (continued)**

Features	In	Software Images by Feature Sets			
		Enterprise/ FW/IDS IPSec 56	Enterprise/F W/IDS IPSec 3DES	SNASW	
<b>IOS Based</b>					
Cisco 7300 Series High Availability NSE Redundancy	(10)EX2	Yes	Yes	Yes	
Cisco 7300 Series Power-On Diagnostics	(10)EX2	Yes	Yes	Yes	
FPGA Bundling and Update	(10)EX	No	No	Yes	
POS Alarm Trigger Delay	(12c)EX1	Yes	Yes	Yes	
show redundancy command enhancements	(12c)EX1	Yes	Yes	Yes	
T3 Bit Error Rate Testing	(12c)EX1	Yes	Yes	Yes	
T3 Maintenance Data Link Messages on the Cisco 7304 Router	(13)EX	Yes	Yes	Yes	
Increased number of traffic classes per policy map in PXF	(12c)EX1	Yes	Yes	Yes	
MPLS Load Balancing on PXF	(12c)EX1	Yes	Yes	Yes	

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7304 router for Cisco IOS Release 12.1EX.

### New Hardware Features in Cisco IOS Release 12.1(13)EX3

There are no new hardware features supported in Cisco IOS Release 12.1(13)EX3.

### New Software Features in Cisco IOS Release 12.1(13)EX3

There are no new software features supported in Cisco IOS Release 12.1(13)EX3.

### Hardware Features in Cisco IOS Release 12.1(13)EX2

There are no new hardware features supported in Cisco IOS Release 12.1(13)EX2.

### New Software Features in Cisco IOS Release 12.1(13)EX2

There are no new software features supported in Cisco IOS Release 12.1(13)EX2.

## New Hardware Features in Cisco IOS Release 12.1(13)EX1

There are no new hardware features supported in Cisco IOS Release 12.1(13)EX1.

## New Software Features in Cisco IOS Release 12.1(13)EX1

There are no new software features supported in Cisco IOS Release 12.1(13)EX1.

## New Hardware Features in Cisco IOS Release 12.1(13)EX

There are no new hardware features supported in Cisco IOS Release 12.1(13)EX.

## New Software Features in Cisco IOS Release 12.1(13)EX

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(13)EX:

### Generic Routing Encapsulation

Platforms: Cisco 7304 routers

Generic Routing Encapsulation (GRE) is now available in PXF starting in Cisco IOS Release 12.1(13)EX.

GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

### Netflow Version 5 on PXF

Platforms: Cisco 7304 routers

Netflow Version 5 was introduced for PXF in Cisco IOS Release 12.1(13)EX.

NetFlow switching provides network administrators with access to “call detail recording” information from their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting and departmental chargebacks, ISP billing, data warehousing and data mining for marketing purposes. NetFlow also provides a highly-efficient mechanism with which to process security access lists without paying as much of a performance penalty as is incurred with other available switching methods.

## T3 Maintenance Data Link Messages on the Cisco 7304 Router

Platforms: Cisco 7304 routers

MDL messages are used to communicate identification information between local and remote ports. The type of information included in MDL messages includes the equipment identification code (EIC), location identification code (LIC), frame identification code (FIC), unit, Path Facility Identification (PFI), port number, and Generator Identification numbers. The values for each piece of MDL message identification can be defined only by a network administrator and are discussed in ANSI T1.107.

## New Hardware Features in Cisco IOS Release 12.1(12c)EX1

There are no new hardware features supported in Cisco IOS Release 12.1(12c)EX1.

## New Software Features in Cisco IOS Release 12.1(12c)EX1

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(12c)EX1:

### Increased number of traffic classes per policy map in PXF

Platforms: Cisco 7304 routers

The number of queues allocated for traffic classes per policy map in PXF has been increased from four to eight in Cisco IOS Release 12.1(12c)EX1. Of these eight traffic class queues, one traffic class queue is still allocated for the default traffic class and another queue is allocated for priority queuing.

### MPLS Experimental Bit Matching and Marking on PXF

Platforms: Cisco 7304 routers

MPLS Experimental Bit Matching and Marking (the **match mpls experimental** command in class map configuration mode, and the **set mpls experimental** command in policy map configuration mode) became available in the PXF-switching path in Cisco IOS Release 12.1(12c)EX1.

For information on this and other PXF features, see the “PXF Features” section of the *Cisco 7304 Troubleshooting and Configuration Notes* document.

### MPLS Load Balancing on PXF

Platforms: Cisco 7304 routers

The ability to load balance MPLS traffic in the PXF path is now available.

For information on this and other PXF features, see the “PXF Features” section of the *Cisco 7304 Troubleshooting and Configuration Notes* document.

## POS Alarm Trigger Delay

Platforms: Cisco 7304 routers

A trigger is an alarm which, when asserted, causes the line protocol to go down.

When one or more triggers are asserted, the line protocol of the interface goes down. The POS Alarm Trigger Delay feature provides the option to delay triggering of the line protocol of the interface from going down when an alarm triggers the line protocol to go down. For instance, if you configure the POS alarm delay for 150 ms, the line protocol will not go down for 150 ms after receiving the trigger. If the trigger alarm stays up for more than 150 ms, the link is brought down as it is now. If the trigger alarm clears before 150 ms, the line protocol is not brought down.

For additional information on POS Alarm Trigger Delay for the Cisco 7304, see the POS Alarm Trigger Delay for the Cisco 7304 document. (Need to insert link when available).

## show redundancy command enhancements

Platforms: Cisco 7304 routers

The show redundancy command has been enhanced in Release 12.1(12c)EX1 to include the following outputs: Operating mode, system up time, active up time, and the number of standby failures.

## T3 Bit Error Rate Testing

Platforms: Cisco 7304 routers

The ratio of received bits on an interface that contain errors is called the bit error rate (BER). A Bit Error Rate Test (BERT) is used to check the BER. This feature introduces BERT for T3 line cards on the Cisco 7304 router.

T3 BERT testing is used on the Cisco 7304 to check communication between local and remote DS-3 ports. If traffic is not being transmitted or received on a DS-3 port, T3 BERT can be used to test the port.

For additional information on the T3 BERT on the Cisco 7304 router, see the T3 Bit Error Rate Testing on the Cisco 7304 document. (provide link later).

## New Hardware Features in Cisco IOS Release 12.1(12c)EX

There are no new hardware features supported in Cisco IOS Release 12.1(12c)EX.

## New Software Features in Cisco IOS Release 12.1(12c)EX

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(12c)EX:

## Multiprotocol Label Switching (MPLS) and MPLS VPN on PXF

Platforms: Cisco 7304 routers

Multiprotocol Label Switching (MPLS) is now available in the PXF-switching path on the Cisco 7304 router. In the initial implementation for the Cisco 7304 on PXF, MPLS Basic and MPLS VPN support have been made available in the PXF-switching path.

Cisco IOS® Multiprotocol Label Switching (MPLS) fuses the intelligence of routing with the performance of switching by labeling traffic and using the labels to forward traffic across MPLS domains. MPLS provides significant benefits to networks with a pure IP architecture as well as those with IP and ATM or a mix of other Layer 2 technologies.

For MPLS Basic and MPLS VPN configuration examples, see the “PXF Configuration Examples” section of the *Cisco 7304 Router Troubleshooting and Configuration Notes* document.

## Network Address Translation on PXF

Platforms: Cisco 7304 routers

Network Address Translation (NAT) is now available in the PXF-switching path for the Cisco 7304 router.

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address.

The **show c7300 pxf nat statistics** command was introduced as part of this feature to allow users to view NAT-related statistics occurring in the PXF-switching path.

NAT can be implemented using various methods. For NAT configuration examples and explanations, see the “PXF Configuration Examples” section of the *Cisco 7304 Router Troubleshooting and Configuration Notes* document.

## New Hardware Features in Cisco IOS Release 12.1(10)EX2

There are no new hardware features supported in Cisco IOS Release 12.1(10)EX2.

## New Software Features in Cisco IOS Release 12.1(10)EX2

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(10)EX2:

## Cisco 7300 Series Power-On Diagnostics

Platforms: Cisco 7304 routers

With the Cisco 7300 Series Power-On Diagnostics feature you can configure your Cisco 7300 series router to run diagnostic tests on the installed network services engines (NSEs) installed in your system. Use the diagnostic level power-on command to enable power on diagnostics. The power-on diagnostics run only when the system is in the process of booting from a power on or is rebooting after a system crash. User-initiated system reloads do not initiate power on diagnostics to be performed though the diagnostic level power-on command has been configured.




---

**Note** Note Any failure in the power-on diags results in the boot of the software being aborted.

---

## Cisco 7300 Series High Availability NSE Redundancy

Platforms: Cisco 7304 routers

### NSE Redundancy

The Cisco 7300 Series High Availability NSE Redundancy feature adds support for a second dual-wide NSE installed in a Cisco 7300 series router. Previously only one dual-wide NSE could be installed in slots 0 and 1. NSE redundancy enables an NSE to be installed in slots 2 and 3. This NSE can be the only NSE installed in the system, or it can be a second NSE. The NSE installed in slots 0 and 1 is the preferred active NSE. Upon bootup the NSE in slots 0 and 1 assumes the role of the active NSE. The standby NSE in slots 2 and 3 waits for 45 seconds for the NSE in slots 0 and 1 to assume the role of active NSE. If there is no NSE installed in slots 0 and 1, the NSE in slots 2 and 3 bypasses the 45 second wait and automatically assumes the role of active NSE.

Upon booting, the system recognizes the NSE installed in slot 0 and slot 1 as the active NSE unless there is some error condition existing on this NSE. If the active NSE does not respond upon bootup, or you enter the redundancy force-switchover command, the standby NSE becomes the active NSE.

You do not need to configure anything on the router to activate the Cisco 7300 Series High Availability NSE Redundancy feature. Installing a second NSE in the chassis automatically creates NSE redundancy in the system. Make sure that you have Cisco IOS images that support high availability installed on both the active and the standby NSEs. We strongly recommend that you install the same Cisco IOS release image on both the active and standby NSE. You should also make sure that the Config-register is properly configured.

### Fast Software Upgrade

This feature also introduces Fast Software Upgrade (FSU), for the Cisco 7304 router. Using FSU you can reduce planned downtime. With FSU, you can configure the system to switch over to a standby NSE that is preloaded with an upgraded Cisco IOS software image. FSU reduces outage time during a software upgrade by transferring functions to the standby NSE that has the upgraded Cisco IOS software pre-installed. The only downtime with a Fast Software Upgrade is the time required for the standby NSE to take control during the switchover. You can also use FSU to downgrade a system to an older version of Cisco IOS or have a backup system loaded for downgrading to a previous image immediately after an upgrade.




---

**Note** You must also install a boot image that supports High Availability.

---

### Management Port

The FastEthernet port on the Cisco 7300 routers is the default management port. When two NSEs are installed in your system, the FastEthernet management port is configured as FastEthernet 0, not FastEthernet 0/0. This facilitates configuration synching between the active and standby NSE. If you already have configurations in your system for the management port configured as FastEthernet 0/0, the configuration is still recognized as valid. New configuration changes will not accept FastEthernet 0/0, only FastEthernet 0. All configurations displayed by the show running-config command are displayed as FastEthernet 0.

### Compact Flash Disk Commands with Cisco 7300 Series High Availability NSE Redundancy

With the introduction of the Cisco 7300 Series NSE Redundancy feature, you can configure many Cisco IOS file system commands from the active NSE to display and configure information on the standby NSE by using the standby- prefix.

For more information about using file system commands, see the Cisco IOS File System Commands part of the Cisco IOS Configuration Fundamentals Command Reference, Release 12.1.

For more information about basic software commands you can use with the compact Flash Disk in a Cisco 7300 series router, see the “Removing and Installing the NSE” chapter of the Network Services Engine Installation and Configuration Guide.

## Frame Relay Interfaces for PXF Support

Platforms: Cisco 7304 routers

IP traffic entering Frame Relay interfaces and subinterfaces on the Cisco 7304 router is now processed using the PXF processor.

The Frame Relay implementation used on the Cisco 7304 router supports the Cisco, IETF, and IETF SNAP encapsulation types, and it is important to note that the Frame Relay implementation on the Cisco 7304 router does not support Frame Relay switching and non-IP Frame Relay traffic in PXF. Instead, Frame Relay switching and non-IP Frame Relay traffic is processed using the Route Processor.

For additional Frame Relay restrictions on the Cisco 7304 router, see the “Frame Relay Restrictions” section of the Cisco 7304 Installation and Troubleshooting notes.

## Weighted Random Early Detection

Platforms: Cisco 7304 routers

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets

prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED) on the Cisco 7304 router drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

## New Hardware Features in Cisco IOS Release 12.1(10)EX1

The following new hardware features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(10)EX1:

### 2xOC3 ATM Line Card

Platforms: Cisco 7304 routers

The OC3 ATM line card provides the Cisco 7304 router with two OC-3 (155.52-Mbps) ATM interfaces on a single card. You must use the appropriate optical fiber cables to connect the OC3 ATM line card with an external OC-3 network. (See the “Fiber-Optic Transmission Specifications” section and the “Cables and Connectors” section in the OC3 ATM Line Card documentation for more information on optical fiber cables.)

### 2xOC3 POS

Platforms: Cisco 7304 routers

The OC3 POS line card interface provides a direct connection between the Cisco 7304 router and external networks. You must use the appropriate optical fiber cables to connect the OC3 POS line card with an external OC-3 network.

The 2xOC3 POS is a 2 port version of the 4 port OC3 POS. (See the “OC3 POS Line Card Optical Fiber Specifications” section and the “Cables and Connectors” section in the OC3 POS Line Card documentation for more information on optical fiber cables.)

### 2xOC12 POS

Platforms: Cisco 7304 routers

The OC12 POS line cards provide the Cisco 7304 router with single or dual 622.080-Mbps POS interfaces on a single card. You must use the appropriate optical fiber cables to connect the OC12 POS line card with an external OC-12 network. (See the “OC12 POS Line Card Optical Fiber Specifications” section and the “Cables and Connectors” section in the OC12 POS Line Card documentation for more information on optical fiber cables.)

## New Software Features in Cisco IOS Release 12.1(10)EX1

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(10)EX1:

### Cisco IOS IEEE 802.1Q Support

Platforms: Cisco 7304 routers

The Cisco IOS IEEE 802.1q VLAN encapsulation method is now available on the Cisco 7304 router. IEEE 802.1q VLAN sub-interfaces can now be created on a GigabitEthernet interface and traffic received from or destined to these VLANs can be processed in the PXF processor.

## Traffic Policing

Platforms: Cisco 7304 routers

Traffic Policing is now available for PXF-processor switched traffic on the Cisco 7304 router.

Traffic Policing is used to limit the input or output transmission rate of a class of traffic received on an interface through the use of a token bucket algorithm. The token bucket algorithm determines if the traffic is transmitted to its destination, dropped, or marked.

Traffic Policing is configured using the **police** command in policy map class configuration mode.

## Unicast Reverse Path Forwarding

Platforms: Cisco 7304 routers

The Unicast Reverse Path Forwarding (RPF) feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

On the Cisco 7304 router, the following configuration options are available for RPF:

- **ip verify unicast reverse-path [allow-self-ping] [list]**

The **ip verify unicast reverse-path** command configures RPF verification on an interface. In this configuration, the router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. If the source address of the packet does not match the interface on which the packet was received, the packet is dropped if no access list is specified or filtered by the access list if an access list is specified in the command line. An access list is specified for packets failing the RPF by specifying a previously configured access list number using the *list* option in the command line.

A hole exists in the verification check to allow the router to ping its own interface. This hole could be exploited by attackers to spoof packets and attack the router. To prevent this type of DoS attack, the **allow-self-ping** option has to be configured for a router to ping its own interface.

- **ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [list]**

The **ip verify unicast source reachable-via any** command configures RPF to accept the incoming packet if the source IP address exists in the router's Forwarding Information Base (FIB), while the **ip verify unicast source reachable-via rx** command configures RPF to insure the source IP address is reachable via the interface on which the packet was received. The **allow-default** option is used to signal that RPF can lookup the default route on a router and use it for RPF verification.

The **show c7300 pxf accounting** command can be used to show the number of packets dropped on account of a failed RFP check, and the **show c7300 pxf interface all** command will show the RPF Verification Drops (the packets dropped by RPF check) and RPF Suppressed Drops (the packets dropped by RPF but permitted by the configured access list.) The **show ip access-command** will show the number of packets dropped by RPF and permitted/denied by the configured access list.

## New Hardware Features in Cisco IOS Release 12.1(10)EX

The following new hardware features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(10)EX:

### Clear Channel 6-Port T3 (DS3) Line Card

Platforms: Cisco 7304 routers

The 6T3 line card provides a full-duplex operation at T3 (45 Mbps) speed and provides up to 24 network interfaces per Cisco 7304 router.

The 6T3 line card provides the following features:

- Single-wide line card for the Cisco 7304 router
- Full-duplex synchronous serial DS3 interface
- High-Level Data Link Control (HDLC) data
- Integrated data service unit (DSU) functionality
- Support for 16- and 32-bit cyclic redundancy checks (CRCs)
- Support for HDLC and PPP serial encapsulations
- Support for DS3 MIB (RFC 1407)
- Support for remote and local loopbacks
- Six independent T3 ports
- Subrate DS3 support for Cisco, Kentrox, Larscom, and Digital Link formats along with the associated scrambling. In some modes, the scrambling is optional.
- Clear-channel DS3 (framed but unchannelized)
- M23 and C-bit-parity DS3 frame formats
- Extraction of BOCs on the C-bit far-end alarm and control (FEAC) code
- Detects and counts remote alarm indication (RAI), parity errors, far-end block error (FEBE), line code violation (LCV), loss of light (LOL), out of frame
- (OOF), framing errors, loss of frame (LOF), loss of signal (LOS)
- One-second performance monitoring counters
- Generates AIS and FEAC
- Generates F-, X-, P-, and M-bit errors; LCVs; all zeros; RAI; and FEBE for testing
- Line, payload, and diagnostic loopbacks
- One bicolor LED per T3 port
- Drives up to 900 feet of 75-ohm coaxial cable RG-59U or equivalent, 450 feet to DSX-3 demarcation point (DSX)
- 75-ohm SMB-type coaxial connections over ATT 734/728, 75-ohm coaxial cable
- B3ZS line coding

## OC12 Packet Over SONET Line Card

Platforms: Cisco 7304 routers

The OC12 POS line card provides the Cisco 7304 router with a single 622.080-Mbps POS interface on a single card. You must use the appropriate optical fibercables to connect the OC12 POS line card with an external OC-12 network.

Three models of the OC12 POS line card are available:

- 7300-1OC12POS-MM—Multi-mode
- 7300-1OC12POS-SMI—Single-mode, intermediate reach
- 7300-1OC12POS-SML—Single-mode, long reach

The OC12 POS line card has the following features:

- Short-reach (7300-1OC12POS-MM), intermediate-reach (7300-1OC12POS-SMI), and long-reach (7300-1OC12POS-SML) optical interface with single-mode optical fiber
- Online insertion and removal (OIR) in the Cisco 7304 router, allowing you to remove, add, or replace an OC12 POS line card online
- Support for 16-bit and 32-bit cyclic redundancy checking (CRC-16 and CRC-32)
- Support for Synchronous Payload Envelope (SPE) scrambling
- Supports HDLC encapsulation

## New Software Features in Cisco IOS Release 12.1(10)EX

The following new software features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(10)EX:

### FPGA Bundling and Update

Platforms: Cisco 7304 routers

Field-Programmable Gate Array (FPGA) is a programmable memory device. Cisco 7304 routers have field-programmable gate array (FPGA) images that were previously separate (or unbundled) from the IOS image for the Network Services Engine (NSE) and for all line cards. With the introduction of the FPGA Bundling and Update feature, FPGA images are bundled with IOS images. This eliminates possible conflicts between the IOS image and the FPGA image, or between line card or NSE components and the FPGA image. During system boot up, the need to update the FPGA is automatically detected. If it is determined that the FPGA image for a line card or NSE needs to be updated, you are prompted to update the FPGA image. If you proceed with an FPGA image update for a line card, the line card is set to redownload the new FPGA image from flash. If you proceed with an FPGA image update for an NSE, a system reset is performed.

Automatic FPGA version checking and update is performed during every system startup for all line cards and NSEs in the system. Automatic FPGA version checking and update is performed for a line card after an online insertion and removal (OIR) insertion of that line card.

Some line cards and NSEs may require different FPGA images depending on the version of that line card or NSE. If an FPGA image is not available in the IOS bundle for that line card or NSE, a warning message is displayed and the FPGA update is skipped.

You may need to update the FPGA image in order to add new features or incorporate caveat fixes. You can manually initiate the FPGA image update process by entering the **upgrade fpga all** command.

FPGA images have major and minor versions. FPGA 0.3, for example, is major version 0 and minor version 3. A major version change requires corresponding Cisco IOS changes; a major version may not be backward compatible with an older Cisco IOS version. When a new major version is released, you should upgrade to the latest FPGA version. A minor version change can include caveat fixes and other minor changes. You may choose to skip a minor version update if you are certain you do not need that particular update.

## ACL Accounting

Platforms: Cisco 7304 routers

Access Control List Accounting keeps internal statistics and reports so network managers can ascertain which ACLs have been tested. This knowledge provides network managers with an understanding of how intruders are attempting to enter their enterprise networks. ACL accounting provides source and destination address information, source and destination port numbers, and packet counts. Use the **show ip access-lists** [*access-list-number* | *name*] command to view how many times a particular ACL has permitted or denied packets. For example:

```
Router# show ip access-lists source_only
Extended IP access list source_only (Compiled)
  permit udp host 1.1.1.3 eq snmp host 2.1.1.3 (994598 matches)
  permit udp host 1.1.1.3 eq snmptrap host 2.1.1.3 (994598 matches)
  permit udp host 1.1.1.3 eq domain host 2.1.1.3 (994598 matches)
  permit udp host 1.1.1.3 eq bootps host 2.1.1.3 (994598 matches)
  .
  .
  .
```

## ICMP Handling

Platforms: Cisco 7304 routers

Cisco 7304 router can now handle common Internet Control Message Protocol (ICMP) messages through PXF instead of through the Route Processor (RP.) Echo Reply, Host Unreachable, Fragmentation Required but DF Set, ACL Deny, and Time Exceeded messages are now generated in PXF to reduce packet punting to the RP.



### Note

If the **debug icmp** command is enabled via the **exec** command, all ICMP messages are handled by the RP. This includes generation of echo replies to incoming echo requests as well as handling of host unreachables, fragmentation when DF set, ACL denials, and TTL expiry cases.

## New Hardware Features in Cisco IOS Release 12.1(9)EX3

There are no new hardware features supported in Cisco IOS Release 12.1(9)EX3.

## New Software Features in Cisco IOS Release 12.1(9)EX3

There are no new software features supported in Cisco IOS Release 12.1(9)EX3.

## New Hardware Features in Cisco IOS Release 12.1(9)EX2

There are no new hardware features supported in Cisco IOS Release 12.1(9)EX2.

## New Software Features in Cisco IOS Release 12.1(9)EX2

The following software feature is supported by the Cisco 7304 router for Cisco IOS Release 12.1(9)EX2:

### Quality of Service for Parallel eXpress Forwarding

The following Quality of Service (QoS) features for Parallel eXpress Forwarding (PXF) are available in Cisco IOS Release 12.1(9)EX2:

- Match ACL (match access-group command)
- Marking IP Precedence (set ip precedence command)
- Marking IP DSCP (set ip dscp command)
- Priority and Standard queueing

For more information about these PXF features, including configuration notes and examples, see the *Cisco 7304 Router and Troubleshooting Configuration Notes*:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm>

## New Hardware Features in Cisco IOS Release 12.1(9)EX1

The following new hardware features are supported by the Cisco 7304 router for Cisco IOS Release 12.1(9)EX:

### Cisco 7300 Series Router Platform

Platforms: Cisco 7304 routers

The Cisco 7304 router is a high-performance Enterprise Edge LAN/WAN integration and service provider aggregation router.

The Cisco 7304 router supports the following features:

- Online insertion and removal (OIR)—Provides the capability to add, replace, or remove line cards without interrupting the system
- Environmental monitoring and reporting functions—Provides the capability to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation
- Downloadable software—Provides the capability to load new images into Flash memory remotely, without having to physically access the router, for fast, reliable upgrades

- Front to back airflow—Provides the capability to mount the router from either front or back into telco or 19-inch racks
- Small form-factor—Provides four rack-units high with stacking capability: 6.94 in. x 17.6 in. x 20.5 in. (17.63 cm x 44.70 cm x 52.07 cm)

The Cisco 7304 router uses high speed point-to-point serial link technology to interconnect the processor card (NSE) and each line card. An NSE provides connectivity to three physical Ethernet ports, two Gigabit Ethernet ports and one FastEthernet/Ethernet management port.

A fully configured Cisco 7304 router comes equipped with one AC-input power supply that supplies 540w of power to the router. A Cisco 7304 router, however, can operate two power supplies on a single chassis. The additional power supply provides a hot-swappable, load-sharing redundant power supply. Redundant power is useful as a fail-over; if a situation occurs where one power supply is down (for instance, a power supply fails or a new power supply needs to be installed), the router can continue to run properly using the other power supply.

## New Software Features in Cisco IOS Release 12.1(9)EX1

The following new software feature is supported by the Cisco 7304 router for Cisco IOS Release 12.1(9)EX:

### Parallel eXpress Forwarding (PXF)

Platforms: Cisco 7304 router

Cisco Parallel eXpress Forwarding (PXF) enables forwarding performance on the order of millions of packets per second. PXF makes use of the expedited IP look-up and forwarding algorithms introduced with Cisco Express Forwarding (CEF), while offering expanded functionality and accelerated performance through the implementation of a parallel architecture.

PXF supports sophisticated IP service functionality with minimal impact on throughput. The PXF forwarding engine applies the combination of parallel processing and pipelining techniques to the CEF algorithms to efficiently handle a variety of complex services and operations.

PXF incorporates the advances of CEF with optimized implementations using advanced, reprogrammable ASIC technology for faster throughput and optimal flexibility.

For more information about the PXF features for the Cisco 7304 router, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7300/trouble/1270note.htm>

# MIBs

## Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-\* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 15](#).

**Table 15** *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.1(13)EX that can apply to the Cisco 7304 router.

### Bundled FPGAs for Cisco IOS Release 12.1(13)EX3

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.1(13)EX3. All Cisco IOS Release 12.1(13)EX3 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.1(13)EX2.

### Network Services Engine 100 Hardware Revision IOS Compatibility Note

If you are using an NSE-100 with a hardware revision of 5.0 or later, Cisco IOS Release 12.1(12c)EX1 is required to operate your router.

To check your hardware revision number, enter the **show diag slot-number** command (where the *slot-number* is the slot containing the NSE-100) and view the hardware revision output. If your hardware revision number is greater than 5.0 and you are not running Cisco IOS Release 12.1(12c)EX1 or later, upgrade your IOS to a supported release.

The output below shows how to view the hardware revision number. When viewing the revision number, ensure that you are viewing the NSE hardware revision and not a revision number for another component.

```
Router(boot) #show diag 0
Slot 0/1:
    NSE Card state:Primary
    Insertion time:00:00:28 ago
C7300 NSE Mainboard EEPROM:
    Hardware Revision      :5.0
    PCB Serial Number     :CAB0529JQGB
    Part Number           :73-5198-02
...
```

### Bundled FPGAs for Cisco IOS Release 12.1(13)EX

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.1(13)EX. All Cisco IOS Release 12.1(13)EX software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.1(12c)EX1.

### Bundled FPGAs for Cisco IOS Release 12.1(12c)EX1

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.1(12c)EX1. All Cisco IOS Release 12.1(12c)EX1 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.1(12c)EX.

## Bundled FPGAs for Cisco IOS Release 12.1(12c)EX

All Cisco IOS Release 12.1(12c)EX software images support the bundled field-programmable gate arrays (FPGA) listed in [Table 16](#).

[Table 16](#) lists the FPGA versions that are bundled in Cisco IOS Release 12.1(12c)EX

**Table 16** Bundled FPGA Versions for Cisco IOS Release 12.1(12c)EX

FPGA Image	FPGA Version Bundled
Clear Channel T3 Linecard FPGA	0.14
OC12 POS Linecard FPGA	0.16
OC3 ATM Linecard FPGA	0.17
OC3 POS Linecard FPGA	0.18
OC48 POS Linecard FPGA	0.14
NSE-100 Daughterboard FPGA	1.04
NSE-100 Motherboard FPGA	1.04

If the version of FPGA running on your hardware does not match the version that is bundled in the IOS, it is recommended that you update your FPGA image. For more details, please refer to *Cisco 7300 Series FPGA Bundling and Update* feature module.

## Bundled FPGAs for Cisco IOS Release 12.1(10)EX1

All Cisco IOS Release 12.1(10)EX1 software images support the bundled field-programmable gate arrays (FPGA) listed in [Table 16](#).

[Table 17](#) lists the FPGA versions that are bundled in Cisco IOS Release 12.1(10)EX1

**Table 17** Bundled FPGA Versions for Cisco IOS Release 12.1(10)EX1

FPGA Image	FPGA Version Bundled
Clear Channel T3 Linecard FPGA	0.13
OC12 POS Linecard FPGA	0.16
OC3 ATM Linecard FPGA	0.17
OC3 POS Linecard FPGA	0.18
OC48 POS Linecard FPGA	0.14
NSE-100 Daughterboard FPGA	0.10
NSE-100 Motherboard FPGA	0.12

If the version of FPGA running on your hardware does not match the version that is bundled in the IOS, it is recommended that you update your FPGA image. For more details, please refer to *Cisco 7300 Series FPGA Bundling and Update* feature module.

## Bundled FPGAs for Cisco IOS Release 12.1(10)EX

Cisco IOS Release 12.1(10)EX contains software images with bundled field-programmable gate arrays (FPGA).

Table 18 lists the FPGA versions that are bundled in Cisco IOS Release 12.1(10)EX.

**Table 18** Bundled FPGA Versions for Cisco IOS Release 12.1(10)EX

FPGA Image	FPGA Version Bundled
Clear Channel T3 Linecard FPGA	0.12
OC12 POS Linecard FPGA	0.16
OC3 POS Linecard FPGA	0.18
OC48 POS Linecard FPGA	0.13
NSE-100 Daughterboard FPGA	0.10
NSE-100 Motherboard FPGA	0.12

If the version of FPGA running on your hardware does not match the version that is bundled in the IOS, it is recommended that you update your FPGA image. For more details, please refer to *Cisco 7300 Series FPGA Bundling and Update* feature module.

## Image Deferral, Cisco IOS Release 12.1(12c)EX1

All Cisco 7300 series crypto images in Cisco IOS Release 12.1(12c)EX have been deferred to Cisco IOS Release 12.1(12c)EX1 due to the following caveats:

- CSCdy28182—Corrupt/invalid NSE100 FPGA handling (minimum boot) is broken
- CSCdy35865—Need to reduce the RP memory usage for XCM management
- CSCdy29934—POS interface do not properly detect line protocol state
- CSCdy37094—WS:Fatal parity and ECC errors should reset the NSE-100 board
- CSCdy29222—7300:PXN Netflow source AS and netmask is corrupted
- CSCdy28595—can not ping when testing IP switching



### Note

Disclaimer: In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images. PLEASE BE AWARE THAT FAILURE TO UPGRADE THE AFFECTED IOS IMAGES MAY RESULT IN NETWORK DOWNTIME. The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

## Image Deferral, Cisco IOS Release 12.1(9)EX2

All Cisco 7300 series crypto images in Cisco IOS Release 12.1(9)EX1 have been deferred to Cisco IOS Release 12.1(9)EX2 due to the following caveat:

- CSCdv67149—c7300 crypto images: standard testing not yet completed

**Note**

---

Disclaimer: In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images. **PLEASE BE AWARE THAT FAILURE TO UPGRADE THE AFFECTED IOS IMAGES MAY RESULT IN NETWORK DOWNTIME.** The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

---

## Image Deferral, Cisco IOS Release 12.1(9)EX1

Cisco 7300 series images c7300-is-mz and c7300-js-mz in Cisco IOS Release 12.1(9)EX have been deferred to Cisco IOS Release 12.1(9)EX1 due to the following caveat:

- CSCdv70275—Default to Rev2 NSE if NSE Revision is greater than two

**Note**

---

Disclaimer: In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images. **PLEASE BE AWARE THAT FAILURE TO UPGRADE THE AFFECTED IOS IMAGES MAY RESULT IN NETWORK DOWNTIME.** The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

---

# Caveats for Cisco IOS Release 12.1 EX

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

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

All caveats in Cisco IOS Release 12.1 are also in Cisco IOS Release 12.1(13)EX3.

For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.



## Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Because Cisco IOS Release 12.1(9)EX1 is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

**Table 19** Caveats Reference for Cisco IOS Release 12.1 EX

DDTS Number	Open in Release	Resolved in Release
CSCdu41610	12.1(9)EX, 12.1(9)EX1	12.1(9)EX2
CSCdv10449	12.1(9)EX, 12.1(9)EX1, 12.1(9)EX2	12.1(13)EX
CSCdv29682	12.1(9)EX, 12.1(9)EX1, 12.1(9)EX2	
CSCdv55966	12.1(9)EX, 12.1(9)EX1	12.1(9)EX2
CSCdv72888	12.1(9)EX2	
CSCdv73310	12.1(9)EX2	12.1(13)EX
CSCdv76107		12.1(10)EX1
CSCdv82103		12.1(10)EX
CSCdw08796		12.1(10)EX2
CSCdw15420		12.1(9)EX2, 12.1(10)EX
CSCdw29879		12.1(10)EX
CSCdw31309		12.1(10)EX
CSCdw32990		12.1(10)EX2
CSCdw35614		12.1(10)EX1
CSCdw46504		12.1(10)EX1
CSCdw56354		12.1(10)EX
CSCdw61239		12.1(10)EX1
CSCdw61263		12.1(10)EX1

**Table 19** Caveats Reference for Cisco IOS Release 12.1 EX (continued)

CSCdw65903		12.1(9)EX3
CSCdw73511	12.1(10)EX1	12.1(10)EX2
CSCdw93271	12.1(10)EX1	12.1(13)EX
CSCdw94400	12.1(10)EX1	12.1(10)EX2
CSCdw95046	12.1(10)EX1	12.1(13)EX2
CSCdx00377	12.1(10)EX1	12.1(10)EX2
CSCdx07907	12.1(10)EX1	12.1(13)EX
CSCdx08542		12.1(10)EX2
CSCdx12712	12.1(10)EX2	12.1(12c)EX
CSCdx14359	12.1(10)EX2	12.1(12c)EX
CSCdx18960	12.1(10)EX2	12.1(12c)EX
CSCdx23186	12.1(10)EX2	12.1(12c)EX
CSCdx27566	12.1(10)EX2	12.1(12c)EX
CSCdx27982	12.1(10)EX2	12.1(13)EX
CSCdx29732	12.1(10)EX2	12.1(12c)EX
CSCdx29868		12.1(10)EX2
CSCdx36545		12.1(12c)EX
CSCdx37159		12.1(12c)EX
CSCdx38526		12.1(12c)EX
CSCdx44140		12.1(12c)EX
CSCdx44699		12.1(12c)EX
CSCdx44706		12.1(12c)EX
CSCdx46041		12.1(12c)EX
CSCdx46535		12.1(12c)EX
CSCdx52072	12.1(12c)EX	12.1(12c)EX1
CSCdx52095		12.1(12c)EX
CSCdx52772	12.1(12c)EX	12.1(13)EX
CSCdx54485	12.1(12c)EX	
CSCdx59721	12.1(12c)EX	12.1(12c)EX1
CSCdx60576		12.1(12c)EX
CSCdx61081		12.1(12c)EX
CSCdx61687		12.1(12c)EX
CSCdx62102	12.1(12c)EX	
CSCdx63389	12.1(12c)EX	
CSCdx63894		12.1(12c)EX
CSCdx71070		12.1(12c)EX
CSCdx87286		12.1(12c)EX

**Table 19** Caveats Reference for Cisco IOS Release 12.1 EX (continued)

CSCdx89185	12.1(12c)EX	
CSCdx93151	12.1(12c)EX	12.1(13)EX
CSCdx95161		12.1(12c)EX
CSCdy01180	12.1(12c)EX	12.1(12c)EX1
CSCdy05945	12.1(12c)EX	
CSCdy06022	12.1(12c)EX	
CSCdy06637	12.1(12c)EX	12.1(13)EX
CSCdy06958	12.1(12c)EX	12.1(13)EX
CSCdy10381		12.1(12c)EX
CSCdy12530	12.1(12c)EX	
CSCdy14458	12.1(12c)EX	12.1(12c)EX1
CSCdy17263	12.1(12c)EX	
CSCdy17908	12.1(12c)EX	12.1(13)EX
CSCdy19425	12.1(12c)EX	12.1(12c)EX1
CSCdy23870		12.1(12c)EX1
CSCdy24424	12.1(12c)EX1	
CSCdy26973	12.1(12c)EX1	
CSCdy28182		12.1(12c)EX1
CSCdy28595		12.1(12c)EX1
CSCdy29222		12.1(12c)EX1
CSCdy29412		12.1(12c)EX1
CSCdy29934		12.1(12c)EX1
CSCdy29978		12.1(12c)EX1
CSCdy33680	12.1(12c)EX1	
CSCdy33698	12.1(12c)EX1	12.1(13)EX
CSCdy34154		12.1(12c)EX1
CSCdy35865		12.1(12c)EX1
CSCdy37094		12.1(12c)EX1
CSCdy37376	12.1(12c)EX1	12.1(13)EX
CSCdy42731		12.1(12c)EX1
CSCdy43027	12.1(12c)EX1	12.1(13)EX
CSCdy43366		12.1(12c)EX1
CSCdy44444	12.1(12c)EX1	
CSCdy44546	12.1(12c)EX1	
CSCdy46959	12.1(12c)EX1	
CSCdy47732	12.1(12c)EX1	12.1(13)EX
CSCdy48126		12.1(12c)EX1

**Table 19** Caveats Reference for Cisco IOS Release 12.1 EX (continued)

CSCdy53410	12.1(12c)EX1	
CSCdy56643	12.1(13)EX	
CSCdy57637		12.1(13)EX
CSCdy57676		12.1(13)EX
CSCdy59224		12.1(13)EX
CSCdy59350		12.1(13)EX
CSCdy59713	12.1(13)EX	
CSCdy60065	12.1(13)EX	
CSCdy61350	12.1(13)EX	
CSCdy63335		12.1(13)EX
CSCdy66701	12.1(13)EX2	
CSCdy68623	12.1(13)EX	12.1(13)EX3
CSCdy76811	12.1(13)EX	12.1(13)EX1
CSCdy78608	12.1(13)EX	
CSCdy83719	12.1(13)EX	
CSCdy86138		12.1(13)EX1
CSCdy89131		12.1(13)EX
CSCdz00391		12.1(13)EX
CSCdz02486		12.1(13)EX2
CSCdz02641		12.1(13)EX
CSCdz04603	12.1(13)EX	
CSCdz05576	12.1(13)EX	
CSCdz09869	12.1(13)EX3	
CSCdz13228		12.1(13)EX1
CSCdz13599		12.1(13)EX1
CSCdz15336		12.1(13)EX1
CSCdz21214		12.1(13)EX1
CSCdz46569		12.1(13)EX1
CSCdz46772		12.1(13)EX1
CSCdz47930		12.1(13)EX1
CSCdz51168		12.1(13)EX1
CSCdz63182		12.1(13)EX2
CSCdz76979	12.1(13)EX2	
CSCdz85439		12.1(13)EX2
CSCdz88728	12.1(13)EX2	
CSCea02355		12.1(13)EX2
CSCea06731	12.1(13)EX2	

**Table 19** Caveats Reference for Cisco IOS Release 12.1 EX (continued)

CSCea54593		12.1(13)EX3
CSCea77047		12.1(13)EX3
CSCea83584		12.1(13)EX3
CSCea85841		12.1(13)EX3
CSCeb09322		12.1(13)EX3
CSCeb11344		12.1(13)EX3
CSCeb15564		12.1(13)EX3
CSCeb22731		12.1(13)EX3
CSCeb29760		12.1(13)EX3
CSCeb56764		12.1(13)EX3

## Open Caveats—Cisco IOS Release 12.1(13)EX3

This section documents possible unexpected behavior by Cisco IOS Release 12.1(13)EX3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz09869

This fix addresses incompatibility between 12.2S and 12.1E images in a redundant RP 7300 system. Prior to this fix when we boot primary RP with 12.2S image and redundant RP with 12.1E image in a 7300 system, after the switchover, the new master loses the start up configuration.

With this fix, after a switchover secondary should come up with all the primary RP config that a 12.1E release software can support. This fix is not available in releases prior to 12.1(13)EX.

There are no known workarounds.

## Resolved Caveats—Cisco IOS Release 12.1(13)EX3

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(13)EX3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy68623

Cannot attach a service policy with the **set mpls exp** action to a ATM VC in the Cisco 7300 router.

There are no known workarounds.

- CSCea54593

First compact disk read results in failure after hot insertion (OIR).

Workaround: Re-issue the command.

- CSCea77047

PXF may crash after the FIB is updated with new prefixes. This only applies if outbound ACL's and traffic are destined to the new prefixes. There is a small window when this may occur.

There are no known workarounds.

- CSCea83584
 

After an hw-module start/stop of POS card provisioned with sdh framing the path trace buffer information is not sent anymore. However the card still shows remote site path trace information.

Workaround: Avoid hw-module stop/start of the POS card.
- CSCea85841
 

In a Cisco 7300 system with dual cpu cards (NSE-100 or NPE-G100), when the IOS image needs to be upgraded on both cpu cards to an image that also has ne firmware for the fpgas, then it is possible for both the active and standbt cpu cards to get stuck in a partially initialized state which required a power-cycle to recover from.

Workaround: To avoid getting into this situation when upgrading to an IOS image with new fpga firmware in a dual cpu card system, perform the upgrade in the following sequence:

  - copy new IOS image on active and standby flash
  - modify config to boot new IOS and save config
  - reset standby from active (using **hw-module standby reset**)
  - reload active
  - when active comes up and prompts for fpga upgrade, decline upgrade
  - let active boot up completely
  - let standby boot up completely as standby
  - use upgrade **fpga all** command on active to upgrade fpga
  - reload active
  - when standby becomes active and prompts for fpga upgrade, decline upgrade
  - let new standby (old active) boot up completely as standby
  - now issue **upgrade fpga all** command on new active
  - reload new active
  - let standby now become active - since it has the new fpga code it won't prompt for upgrade.
  - let the other NSE boot up as standby
  - at this point, both fpgas and IOS is upgraded on both NSEs
- CSCeb09322
 

An NSE-100 which is under load and using CBWFQ may, on rare occasions, send an old packet (again) instead of the correct one.

There are no known workarounds.
- CSCeb11344
 

c7300 might experience High CPU load due to interrupts during full internet routing table download. Also, the time to download the bgp table is significantly high, 20 minutes for 100K prefixes.

This problem only occurs if there are redundant paths to reach the BGP next-hop.

Workaround: Use only one path.

Alternative workaround: Try to configure scheduler allocate 3000 1000 to give more time to process switching tasks.

- CSCeb15564  
PXF QoS on 7304 NSE-100 may repeatedly allocate some RP memory without freeing it. This will cause the RP memory leak.  
There are no known workarounds.
- CSCeb22731  
In Cisco 7304 router with the configuration of two NSE-100 processor boards in a system. When the NSE-100 board in slot 0 is the active, if the gigabit ethernet port on the standby processor board in slot 2 is configured with both keepalive and auto-negotiation disabled, then the interface does not automatically switch from line down state to line up state when the line protocol comes up. When the line protocol goes down, it automatically switch to line down state. However, when the line protocol is back up, it does not switch the line state back.  
Work around: Reset the gigaethernet port on the standby processor in slot 2 by using the **shutdown** command, followed by **no shutdown** command.
- CSCeb29760  
Super frame (SF), single domain (SD), and threshold crossing alarms B1, B2, and B3 (TCA\_B1, TCA\_B2, and TCA\_B3) defects may not clear on a Packet- over-SONET (POS) line card. This situation may cause the interface of the POS line card to pause permanently.  
These problems are observed on a POS line card that is installed in a Cisco 7300 series when SF, SD, TCA\_B1, TCA\_B2, and TCA\_B3 defects are asserted and deasserted very quickly.  
There are no known workarounds.
- CSCeb56764  
The number of classification classes that the turboACL compiler generates depends on the complexity of the entire ACL set, as well as the traffic pattern of a particular router. On certain combination of a complex ACL set with a very diverse traffic pattern, the number of classification classes produced by the turboACL compiler may be too large to fit into the PXF ACL memory. When this happens, the entire PXF ACL classification is no longer valid.  
However, at this time, the RP ACL classification is not affected. So if the download to PXF ACL memory failed, then we punt all packets that require ACL processing to the RP.  
This happens only with certain combination of a complex ACL set with a very diverse traffic pattern. When it happens, it will not impact the features that does not depend on PXF turboACL.  
There are no known workarounds.

## Open Caveats—Cisco IOS Release 12.1(13)EX2

This section documents possible unexpected behavior by Cisco IOS Release 12.1(13)EX2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy66701

Ping packet to local interface will not trigger ARP for multipoint interface.

Workaround: Any thru packet will trigger an ARP update.

- CSCdz76979

Currently, ATM interfaces on c7300 platform do not support sonetVTIntervalTable MIB. If trying to gather sonetVTIntervalTable message from a c7300 system which has an ATM line card installed, the SNMP getmany may keep in a loop.

Workaround: If there is an ATM line card presented in a c7300 system, do not run getmany for sonetVTIntervalTable.

- CSCdz88728

On a c7300 system with an NSE-100 services engine configured for netflow accounting, the **show c7300 pxf netflow cache [verbose]** command sometimes shows NULL as the destination interface for a flow with valid destination interface.

This caveat is observed so far only in the lab testing environment when

- 1) netflow accounting is enabled in the PXF processor on the NSE-100,
- 2) flows are being aged around the same time.

Workaround: Command **show c7300 pxf netflow cache** is a command hidden from end users. There is currently no workaround on this when this command is run.

- CSCea06731

On a c7300 system with an NSE-100 services engine configured for netflow accounting, the **show c7300 pxf netflow cache [verbose]** command sometimes shows a locally destined flow and the data is incorrect.

This caveat is observed when netflow accounting is enabled on an interface to which data packets destined to this c7300 system are being sent.

Workaround: Command **show c7300 pxf netflow cache** is a command hidden from end users. There is currently no workaround on this when this command is run.

## Resolved Caveats—Cisco IOS Release 12.1(13)EX2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(13)EX2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw95046

On a c7300 system, ICMP replies for ACL denies generated by the PXF processor are not rate-limited.

There are no known workarounds.

- CSCdz02486

The prefix/mask/AS info for certain packets may be wrong when netflow accounting is enabled. Also, ICMP replies generated will not be subject to the right egress QoS, especially if they need to be marked. This is because the ICMP messages are not being reclassified but rather use the classification done on the original ingress packet.

These caveats are observed on a c7300 system with an NSE-100 services engine when ICMP handling is enabled in PXF (which is by default). The first symptom is applicable when netflow accounting is also enabled. The second symptom is for all ICMP messages generated by the PXF processor.

Workaround: Disable ICMP processing in the PXF processor via the **debug ip icmp** exec command.

- CSCdz63182

Ingress traffic accepted on a shutdown subinterface. The most common case for this would be multicasts and broadcasts on a GigE 802.1Q sub-interface.

This problem occurs on a c7300 with an NSE-100 services engine.

There are no known workarounds.

- CSCdz85439

ICMP Echo reply might not be generated correctly in some cases.

This happens only for ICMP echo replies when the following occurs:

1) The outgoing interface of the ICMP reply has ACL configured

AND

2) The ACL has ACEs that are not supported in PXF.eg. log-input, timed

AND

3) The ICMP reply matches this unsupported ACE.

Workaround: Do not to configure ACL with unsupported ACEs.

- 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

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

## Open Caveats—Cisco IOS Release 12.1(13)EX1

This section documents possible unexpected behavior by Cisco IOS Release 12.1(13)EX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

## Resolved Caveats—Cisco IOS Release 12.1(13)EX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(13)EX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy76811

On a c7300 system configured with an NSE-100 services engine and configured for Netflow accounting, packets sent up to the RP for processing may be accounted twice by Netflow, resulting in duplication of exported data. Normally, most packets should be processed by the PXF processor, so the amount of such duplication should be minimal.

- CSCdy86138

This fix is require to fix the HSRP instability problem on the native NSE-GE ports.

There are no known workarounds.

- CSCdz13228

If a router running 12.1(13)EX code is reloaded, the router will not respond to arp request for static nat address defined.

Workaround: Remove the static nat statement and put it back in.

- CSCdz13599

A c7300 with an NSE100 services engine may experience I/O memory redzone corruption and thereby, a software forced reload, when netflow export is enabled.

This situation occurs when part of the traffic is being netflow switched by the Route Processor, resulting in the simultaneous export of netflow data collected by both the PXF processor and the RP.

Workaround: Disable netflow export.

- CSCdz15336

A router with PXF processor such as the C7300 NSE100, may crash with Fatal Error interrupt in situations where PXF processes traffic over more than 2 equal cost parallel routes.

Although show version indicates “System returned to ROM by power-on”, the real reload reason shown is “Last reset from watchdog nmi”.

Workaround: Remove one or more equal cost path from the configuration, to bring down the number of parallel routes to two.

- CSCdz21214

When an ATM-OC3 interface is shut down on a c7300 with an NSE-100 services engine, the remote-end ATM interface does not detect an alarm and stays in the UP state. The reason for this behavior is that the ATM-OC3 interface shutdown does not send the correct framer alarm signal to the remote-end ATM interface.

There are no known workarounds.

- CSCdz46569

On a c7300 system with an NSE-100 services engine configured for netflow v5 accounting, the exported v5 records do not have the correct SNMP interface index values set for input and output interface fields. The values set are internal interface numbers local to the system.

There are no known workarounds.

- CSCdz46772

A c7300 system with an NSE-100 services engine configured for GRE but having no access-list configured may experience a system reload due to a PXF exception triggered by traffic.

Workaround: Configure an access list, even a dummy one that permits all traffic, and assign it to an interface.

- CSCdz47930

The following messages may be seen on a c7300 with an NSE-100 services engine.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x412CE040 reading 0x1
%ALIGN-3-TRACE: -Traceback= 412CE040 40473CA4 00000000 00000000 00000000
```

These messages may appear during boot up or when one of the disks, bootdisk: or disk0:, is accessed.

There are no known workarounds, but the messages are cosmetic.

- CSCdz51168

IOS reload due to an exception when executing the **show ipcache flow** command.

The above behavior may be experienced on a c7300 system with an NSE-100 services engine configured for PXF netflow accounting when the show command is executed just after deletion of sub-interfaces or VCs that had traffic flows active. The show command should have been executed prior to aging out of the traffic flows from PXF. The time for aging out would be as per default values (see product documentation) or configuration.

Workaround: Try and avoid issuing the show command right after deletion of a sub-interface or VC that had active traffic. If that is not possible, try and shut down sub-interface or VC for a period of time before removing it. Simply shutting down the sub-interface or VC should not trigger this caveat.

## Open Caveats—Cisco IOS Release 12.1(13)EX

This section documents possible unexpected behavior by Cisco IOS Release 12.1(13)EX and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy56643

The c7300 PXF MPLS support may punt one-label non-IP MPLS packet to the Router Processor by mistake. This can be seen using **show c7300 pxf acc punt**.

This will stop non-IP transport over MPLS, such as ATOM.

```
Router#show c7300 pxf acc punt
PXF Punt Reasons:
  LC Encap High Punt      : 6018
  IPv4 Options Punt      : 22
```

There are no known workarounds.

- CSCdy59713

Router running 12.1(12c)EX crashed when config change is made on named ACL. Router reload with the following message:

```
System returned to ROM by error - a Software forced crash, PC 0x403AF354 at
```

There are no known workarounds.

- CSCdy60065

On a c7300 system with an NSE-100 services engine configured for MPLS switching, the **show c7300 pxf mpls acc <label-id>** command output will not show any label entries when a specific label-id is specified in the show command.

This caveat is observed when MPLS load-balancing is enabled and a specific label ID is specified. The display is OK when load-balancing is not enabled.

This caveat is a cosmetic issue and has no impact on correct operation of the system.

Workaround: Use the **show c7300 pxf mpls acc all** or the **show tag forward <dest-ip> <dest-mask>** commands.

- CSCdy61350

On a c7300 system with an NSE-100 services engine configured as an MPLS P or PE router, MPLS packets that are within 4 bytes less than the configured MTU may be erroneously sent up (punted) to the Route Processor (RP) by the PXF processor for fragmentation. The RP will correctly switch these packets without fragmenting. However, in cases where the amount of such punting is high, ie., a lot of packets are within a 4 byte range of the MTU, it may reflect as reduced system performance.

The **show c7300 pxf mpls tag** command will show an MPLS MTU value that is 4 bytes less than the configured value.

Workaround: Configure an MPLS MTU value that is 4 bytes more than the desired value.

- CSCdy68623

Cannot attach a service policy with the **set mpls exp** action to a ATM VC in the Cisco 7300 router.

There are no known workarounds.

- CSCdy76811
 

On a c7300 system configured with an NSE-100 services engine and configured for Netflow accounting, packets sent up to the RP for processing may be accounted twice by Netflow, resulting in duplication of exported data. Normally, most packets should be processed by the PXF processor, so the amount of such duplication should be minimal.

There are no known workarounds.
- CSCdy78608
 

Configuring 2k point-to-point VCs at one ATM port and consecutively executing shut/no shut interface and hardware-module stop/start for more than 60 times, may cause memory exhausting and receive warning message “Failed to allocate HW leaf”

Workaround: Do not do more than 60 times shut/no shut and hardware-module stop/start for ATM-OC3 line card. This problem will be fixed in the next release.
- CSCdy83719
 

In some situations, a few NAT entries are not timing out.

Most entries in this condition were found to be for the following UDP traffic:

```
Port  Service
-----
137 - Netbios Name Service
138 - Netbios Datagram Service
53  - DNS
```

Workaround: Use the **clear ip nat translation \*** command to clear non timed-out entries.
- CSCdz04603
 

In the load balancing configuration, sometimes the PXF shadow information is not updated correctly if one of paths is flapped. This could result the issue in this ddt.

Workaround: Retry the “shut/noshut” on that interface.
- CSCdz05576
 

Doing hw-module stop <x> stop will generate traceback message

There are no known workarounds.

## Resolved Caveats—Cisco IOS Release 12.1(13)EX

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(13)EX. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv10449
 

If the system is reloaded while there is incoming traffic to one of the ports on the 4xOC3 POS line card, sometimes, after reload, the system is unable to forward traffic. In this case, another reload is required.

Workaround: Shut down all OC3 POS interfaces and save the running configuration to nonvolatile memory before reloading the system.

Alternative workaround: Configure **pos ais-shut** on the OC3 POS interface.

- CSCdv73310
 

On a Cisco c7300 system, classification of packets for PXF accelerated QoS features has to be done via access list statements supported by TurboACL.

The **match ip precedence value** or **match ip dscp value** match statements under a class-map are not supported in PXF. In order to match on IP precedence or DSCP values, appropriate access-list entries need to be defined and then used via **match access-group list**.

There are no known workarounds.
- CSCdw93271
 

Japan SDH requires that all Z0 bytes have the value 10 (AA). Capella has the first 16 Z0 bytes set to something different in SDH mode.

There are no known workarounds.
- CSCdx07907
 

The PXF LLQ implementation on a c7300 system assigns a fixed weightage of 90% to an interface's priority queue, with the balance 10% going to the other non-priority queues, so that the priority queue does not starve the other queues. This will be modified to make the priority queue weightage configurable so that users can chose anywhere up to 100% weightage (for strict priority) if they so desire.

There are no known workarounds.
- CSCdx27982
 

On a c7300 system with an NSE-100, configuring **ip verify unicast reverse-path** may cause inconsistent behavior when replying to ICMP echo requests (pings) over a POS interface.

If you configure Reverse Path Forwarding on a POS interface, valid ping packets might be dropped. This behavior is observed very rarely and is not easily reproducible.

There are no known workarounds.
- CSCdx52772
 

If we ungracefully remove the primary NSE while it is active, it might cause line cards unstable after the system switches over to the standby NSE. In fact, this is not a valid operation as it could cause the line card to be deactivated. However, line card could be brought up manually with the command **hw-module slot slot\_number start**
- CSCdx93151
 

A Cisco 7300 router running 12.1(10)EX1 may suffer bus errors due to accessing an invalid address. The tracebacks from the crash shows the error occurred within the `mips_ipfib_flow_switch` function.

There is currently no workaround.
- CSCdy06637
 

VRF scalability with the PXF processor on an NSE-100 in a c7300 may be limited to around 500. The exact limit depends on the type and number of IP prefixes. All attempts will be made to improve the VRF scalability to handle around 1000 VRFs in a subsequent release.
- CSCdy06958
 

**encapsulation aal5mux** is not supported on a c7300 system for MPLS labeled packets even though this encapsulation can be configured.

aal5mux encapsulation is supported for IP packets and the caveat only applies to MPLS packets. There is no workaround other than to try and use the aal5snap encapsulation.

- CSCdy17908

A 7300 may experience a hang or crash with a MISTRAL error similar to:

```
MISTRAL-3-ERROR: Error condition detected: SYSAD_TIMEOUT_DPATH
```

There are no known workarounds.

- CSCdy33698

The following messages may be seen on a c7300 system configured with an NSE-100 services engine:

```
00:00:40: ws_tt_index_to_addr: out of range
00:00:40: ws_direct_read: address/offset is invalid: src 0 , dst 42508FD8
```

The value for dst is an example and will be different in the actual messages. MPLS packets are still switched correctly in PXF and no abnormal behavior has been observed.

The messages are seen on a system reload if the **mpls label range <min> <max>** command is configured with a <min> value of 200000 or higher.

Workaround: Configure a <min> value less than 200000 or leave the label range at the default.

- CSCdy37376

The FE Management port of the NSE-100 card in the Cisco 7304 router only supports settings that either both the duplex and the speed settings are in auto configuration or both are in fixed configuration. Although currently there's no warning message when the user tries to configure one fixed and the other one auto, however the port may not function correctly under these settings.

Workaround: Set both the speed and the duplex settings to auto configuration

Alternative workaround: Set both the speed and duplex settings to the fixed configuration.

- CSCdy43027

The following error messages may be intermittently observed on a c7300 system with an NSE-100 services engine:

```
"%SYS-2-GETBUF: Bad getbuffer" and
"%WSIPC-3-GETBUF: Cannot get a buffer to copy rcvd ipc packet".
```

Traceroutes through the c7300 system have been seen to cause the above messages. Other conditions are not known.

There are no known workarounds.

- CSCdy47732

When doing a traceroute between two CE routers connected via an MPLS cloud, the P routers will not be seen, ie., they will not be shown as hops along the path.

For this caveat to be seen, the c7300 system with an NSE-100 services engine needs to be the PE router closest to the traceroute originating CE router and should not have been configured with the **mpls ip propagate-ttl** after boot up.

Workaround: Reconfigure the **mpls ip propagate-ttl** command. This will enable TTL propagation in PXF on the PE router when switching packets from the IP side to the MPLS side. This caveat is due to the fact that the system comes up with TTL propagation disabled by default in PXF on a reload.

- CSCdy57637  
This DDTS is used to bundle OC3-ATM line card FPGA image version 17 to IOS image. This OC3-ATM line card FPGA image has the features to support NSE switch over.  
There are no known workarounds.
- CSCdy57676  
On a c7300 system with an NSE-100 services engine configured as an MPLS P or PE router, packets that are equal to the configured MTU size are either fragmented or dropped depending on the DF bit set.  
This caveat is true for packets that exactly match the MTU.  
There are no known workarounds.
- CSCdy59224  
A c7300 system with an NSE-100 services engine configured as an MPLS PE or P router may reload due to an exception caused by an illegal access to a low memory address.  
This caveat is triggered by disabling and re-enabling CEF via the **no ip cef** and **ip cef** configuration commands and the system is configured for MPLS switching.  
Workaround: Do not disable and re-enable CEF.
- CSCdy59350  
On a c7300 system with an NSE-100 services engine, deletion of an ACL configured on a sub-interface, or deletion of an ACL from the main interface that has ACLs configured on sub-interfaces under that interface, may result in no change after the deletion of the ACL. The deleted ACL remains sticky and effective until all ACLs on the interface and sub-interface(s) have been deleted.  
This caveat applies to interfaces that have one or more sub-interfaces configured under them, with security ACLs on the main interface as well as one or more sub-interfaces, or, just on the sub-interface(s). The caveat is triggered if one of those ACLs is de-configured/deleted.  
Workaround: First deconfigure all ACLs from the sub-interfaces, then de-configure the ACL from the main interface (if present), and then repeat the de-configuration on all sub-interfaces. The **show c7300 pxf interface** command can be used to confirm if all the ACLs have been removed or not. Once all ACLs have been removed, reconfigure back any of the required ACLs.
- CSCdy63335  
On a c7300 system with an NSE-100 services engine configured for netflow accounting, the **show ip cache flow** command may not show or may show incorrect protocol aggregation data.  
This caveat is observed when netflow accounting is enabled in the PXF processor on the NSE-100.  
There are no known workarounds.
- CSCdy89131  
Configuring VC OAM management together with PXF enabled, data packets switched by PXF may be corrupted. Data packets may be sent out as OAM packets which will be dropped at far end.  
This problem is fixed in 12.1(13)EX release.  
Workaround: Do not enable OAM management together with PXF.

- CSCdz02641  
On Cisco 7300 router systems with total memory in excess of 256 MB, configuring power-on diagnostics can cause the system to crash in the memory test when the power-on diagnostics are executing at boot-up.  
Workaround: Disable power-on diagnostics by issuing the **no diagnostic level power-on** and saving the config to startup-config.
- CSCdz00391  
Configuring VC OAM loopback, the PTI value in OAM packet header may be modified from PTI=4 to PTI=5 for F5 OAM packets.  
This problem is fixed in release 12.1(13)EX.  
There are no known workarounds.

## Open Caveats—Cisco IOS Release 12.1(12c)EX1

This section documents possible unexpected behavior by Cisco IOS Release 12.1(12c)EX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy24424  
On a c7300 system configured with an NSE-100 services engine, switching performance for 1518 byte packets between GigE and OC48-POS is slightly (2%) less than expected.  
The above caveat is only applicable when CEF switching at the RP. It does not apply to PXF based switching.  
Workaround: To get decent performance for GigE <-> OC48-POS switching, it is expected that packet switching will be PXF based, not RP based.
- CSCdy26973  
On a c7300 system configured with an NSE-100 services engine, enabling netflow aggregation in PXF also automatically results in IOS trying to export the aggregated data in v8 format. This is an issue only if export of aggregated data is not desired even though aggregation is being done.  
There are no known workarounds.
- CSCdy33680  
Packets may be dropped due to CRC errors on a system connected to a GigE port of an NSE-100 services engine for the c7300.  
The CRC errors may happen when a VRF is configured on the GigE port while it is under stress with near line rate traffic.  
There is no workaround other than to not configure the VRF while the port is under stress. The problem is temporary and the CRC errors should go away within a short time.

- CSCdy33698

The following messages may be seen on a c7300 system configured with an NSE-100 services engine:

```
00:00:40: ws_tt_index_to_addr: out of range
00:00:40: ws_direct_read: address/offset is invalid: src 0 , dst 42508FD8
```

The value for dst is an example and will be different in the actual messages. MPLS packets are still switched correctly in PXF and no abnormal behavior has been observed.

The messages are seen on a system reload if the **mpls label range <min> <max>** command is configured with a <min> value of 200000 or higher.

Workaround: Configure a <min> value less than 200000 or leave the label range at the default.

- CSCdy37376

The FE Management port of the NSE-100 card in the Cisco 7304 router only supports settings that either both the duplex and the speed settings are in auto configuration or both are in fixed configuration. Although currently there's no warning message when the user tries to configure one fixed and the other one auto, however the port may not function correctly under these settings.

Workaround: Set both the speed and the duplex settings to auto configuration

Alternative workaround: Set both the speed and duplex settings to the fixed configuration.

- CSCdy43027

The following error messages may be intermittently observed on a c7300 system with an NSE-100 services engine:

```
"%SYS-2-GETBUF: Bad getbuffer" and
"%WSIPC-3-GETBUF: Cannot get a buffer to copy rcvd ipc packet".
```

Traceroutes through the c7300 system have been seen to cause the above messages. Other conditions are not known.

There are no known workarounds.

- CSCdy44444

On a c7300 system configured for VRFs, routes received beyond the limit configured in the **maximum routes** command are not dropped. Instead, they are entered in the VRF table and can be seen via the **sh ip bgp vpnv4 vrf <name of vrf>** or **sh ip route vrf <name of vrf> exec** commands.

Packet forwarding does not seem to be affected.

There are no known workarounds.

- CSCdy44546

The **show interface accounting** command output on a c7300 configured with an NSE-100 services engine does not display any MPLS/Tag accounting information for PXF switched MPLS traffic on MPLS enabled interfaces.

There are no known workarounds.

- CSCdy46959

Loadbalancing IP to MPLS traffic when configured for MPLS VPN is not effective on a c7300 system configured with an NSE-100. All traffic will take one of the MPLS paths.

There are no known workarounds.

- CSCdy47732

When doing a traceroute between two CE routers connected via an MPLS cloud, the P routers will not be seen, ie., they will not be shown as hops along the path.

For this caveat to be seen, the c7300 system with an NSE-100 services engine needs to be the PE router closest to the traceroute originating CE router and should not have been configured with the **mpls ip propagate-ttl** after boot up.

Workaround: Reconfigure the **mpls ip propagate-ttl** command. This will enable TTL propagation in PXF on the PE router when switching packets from the IP side to the MPLS side. This caveat is due to the fact that the system comes up with TTL propagation disabled by default in PXF on a reload.

- CSCdy53410

Loadbalancing MPLS to IP traffic when configured for MPLS VPN is not effective on a c7300 system configured with an NSE-100. All traffic will take one of the IP paths.

This behavior is seen whether the traffic is being switched by PXF or the RP.

There are no known workarounds.

## Resolved Caveats—Cisco IOS Release 12.1(12c)EX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(12c)EX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx52072

MPLS load balancing is currently not operational on a c7300 configured with an NSE-100. This applies to both PE (IP to MPLS) and P (MPLS to MPLS) router environments.

There are no known workarounds.

- CSCdx59721

**encapsulation aal5nlpid** is not supported on a c7300 system for MPLS labeled packets even though this encapsulation can be configured. This is true with or without PXF enabled on the NSE-100.

aal5nlpid encapsulation is supported for IP packets and the caveat only applies to MPLS packets. There is no known workaround other than to try and use the aal5snap encapsulation.

- CSCdy01180

This caveat applies to PXF switched MPLS traffic with an NSE-100 on a c7300 used as a PE router. When switching MPLS packets to an IP non-VPN destination (label disposition case), none of the supported egress QoS features will be effective on the IP packet.

This caveat does not apply to packets switched to an IP VPN (deaggregation case).

There are no known workarounds.

- CSCdy14458

When a sub-interface is in shutdown state, configuring svc under the sub-interface will trigger this sub-interface to up state. Similarly, a shutdown-state sub-interface will be triggered to up-state after C7300 reload if this sub-interface has svc configured.

Workaround: Shutdown the sub-interface after configuring svc.

- CSCdy19425
 

On a c7300 system configured with an NSE-100, spurious accesses for reads from a very low memory address may be reported together with a traceback. NAT translations do not seem to be affected.

In some cases, the system may stop responding to user input after an extended period, even though it may be switching traffic.

This caveat seems to be triggered when doing inside to outside static NAT with overload.

Workaround: Try and use dynamic NAT and avoid using static NAT.
- CSCdy23870
 

On a c7300 system configured with an NSE-100 services engine, the **sh ip cache flow** command does not display the GigE subinterface for flows with a source or destination interface as a 802.1Q subinterface.

There are no known workarounds.
- CSCdy28182
 

When the NSE100 MotherBoard (MB) FPGA is corrupted, the system will crash instead of entering the minimum boot mode. This DDTS fixes the problem. Now the system will enter the minimum boot mode, if the NSE100 FPGA is corrupted, and the FPGAs can be updated using the **upgrade fpga all** command.

There are no known workarounds.
- CSCdy28595
 

A subinterface behavior may not match the features configured on that subinterface, leading to a failure in switching IP packets.

Deconfiguration of port level features after subinterface is setup may trigger this caveat on a c7300 system configured with an NSE-100 services engine.

A subinterface was inheriting default configuration from its parent port. With certain configuration/deconfiguration command sequences, the subinterface may end up with an inconsistent config between the PXF processor and the RP, resulting in this caveat.

There is no workaround.
- CSCdy29222
 

On a c7300 system configured with an NSE-100 services engine and netflow v8 aggregation configured in PXF, the source AS or source prefix netmask may be wrongly set for randomly selected flows. As a result, some of the aggregated data may be wrong. The **sh ip cache flow aggregation {source-prefix | as}** commands may show spurious AS and netmask values.

There are no known workarounds.
- CSCdy29412
 

In traceroutes through a c7300 system, the IP address of the c7300 is not shown (it is reported as 0.0.0.0).

This caveat occurs when the c7300 is configured with an NSE-100 services engine, PXF is enabled, and the traceroute path comes into the c7300 over an ATM interface.

There are no known workarounds.
- CSCdy29934
 

Occasionally, POS interface is not properly detecting the line protocol state.

Workaround: Clear the interface alarms with the **clear int pos** command.

- CSCdy29978  
This DDTS is opened to bundle the latest SAR firmware (version 1.6.3 General Availability [GA]) with IOS image. The GA SAR firmware does not have new feature.
- CSCdy34154  
On a c7300 system configured with an NSE-100 services engine, class based QoS features do not work on MPLS packets. Coloring of MPLS packets via the Exp bits also does not take effect.  
This caveat is observed when the **match mpls exp** command is applied to a class-map. It is also observed when the **set mpls exp <val>** command is applied to a class or as part of a police command.  
There are no known workarounds.
- CSCdy35865  
Currently for systems configured with 128M of memory, users may see memory allocation failures or system instability issues. It's recommended to upgrade the system image to 12.1(12c)EX1.
- CSCdy37094  
Currently in Cisco 7300 router, it does not reset the NSE board nor write a crashinfo file on bootdisk: when a fatal parity or uncorrectable ECC error happens. These errors can threaten the integrity of the data in the system memory and therefore are severe enough to trigger a NSE board reset.  
Presently, the system only displays an error message and the screen dump of certain registers values for diagnostic purpose. The correct behavior is to reset the NSE board to avoid future data integrity problem.  
There are no known workarounds.
- CSCdy42731  
A c7300 system with an NSE-100 services engine and configured for MPLS will reload due to a PXF exception when trying to switch IP packets exceeding the outgoing interface MTU but with the DF bit set in the IP header.  
For this caveat to be triggered, the c7300 system needs to be a PE router configured for MPLS VPN.  
The IP MTU check coupled with the DF bit caused the PXF processor to drop the packet and generate an ICMP reply. The FIB lookup for forwarding the ICMP reply was not done with the correct VRF, leading to the exception.  
There are no known workarounds. This caveat was introduced in the 12.1(12c)EX release and has been resolved in 12.1(12c)EX1.
- CSCdy43366  
A c7300 system with an NSE-100 services engine and configured for MPLS switching may run out of memory and reload from an exception due to illegal memory access.  
This caveat has been observed when MPLS is disabled and re-enabled one or more times. A command such as **clear tag counters** after MPLS is re-enabled can trigger the reload.  
Workaround: Avoid disabling and re-enabling MPLS.
- CSCdy48126  
A c7300 system configured with an NSE-100 services engine may reload with an exception on deleting a frame relay sub-interface. Multiple sub-interfaces may have to be deleted to trigger the exception.  
There are no known workarounds.

## Open Caveats—Cisco IOS Release 12.1(12c)EX

This section documents possible unexpected behavior by Cisco IOS Release 12.1(12c)EX and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx52072
 

MPLS load balancing is currently not operational on a c7300 configured with an NSE-100. This applies to both PE (IP to MPLS) and P (MPLS to MPLS) router environments.

There are no known workarounds.
- CSCdx52772
 

If we ungracefully remove the primary NSE while it is active, it might cause line cards unstable after the system switches over to the standby NSE. In fact, this is not a valid operation as it could cause the line card to be deactivated. However, line card could be brought up manually with the command **hw-module slot slot\_number start**
- CSCdx54485
 

PPPoATM and other features that require virtual access interfaces are currently not supported in PXF on the c7300 with an NSE-100 processor card. Support for virtual access interfaces in PXF will be provided in a future release.
- CSCdx59721
 

**encapsulation aal5nlpid** is not supported on a c7300 system for MPLS labeled packets even though this encapsulation can be configured. This is true with or without PXF enabled on the NSE-100.

aal5nlpid encapsulation is supported for IP packets and the caveat only applies to MPLS packets. There is no known workaround other than to try and use the aal5snap encapsulation.
- CSCdx62102
 

Current NSE-100 queue congestion control is based on the flow control message between Line Card (LC) and Toaster. If the LC egress FIFO above the high threshold, LC sends a XOFF to Toaster. After LC egress FIFO below the low threshold, LC sends a XON to Toaster. All the packets for same output class queue are queued in the class queue if the interface is at the XOFF state. The default class queue depth is 128 packets. If the class queue reaches the limit, the packet is tail drop.

Since each LC has different gap between high and low thresholds and the flow control message has some propagation delay, the class queue packet accumulate and drain rate is very fast. Hence this burst traffic situation will create some uncertain queue depth situation if each wred precedence min/max thresholds are closer and the mark probability is low (eg. 1/10). Believe the situation will be solved after the PXF traffic shaping is implemented. In the meantime before PXF shaping, we are looking for other improvement approach if it is possible.
- CSCdx63389
 

The C7300 system with an NSE-100 processor card does not support CEF per-packet load balancing in PXF. The PXF only supports per destination load balancing. However, the configuration command for per-packet load balancing was not disabled. This caveat has now been addressed and the per-packet load balancing command will no longer be available.
- CSCdx89185
 

There is an inconsistency when apply a service-policy to an UBR vc. If a service-policy is configured by using bandwidth percentage, this service-policy can be applied to an UBR vc. While if a service-policy is configured by using bandwidth value, this service-policy can not be applied to an UBR vc due to that the visible\_bandwidth of UBR vc is zero.

Workaround: Use VBR vc instead of UBR vc.

- CSCdx93151  
A Cisco 7300 router running 12.1(10)EX1 may suffer bus errors due to accessing an invalid address. The tracebacks from the crash shows the error occurred within the mips\_ipfib\_flow\_switch function.  
There is currently no workaround.
- CSCdy01180  
This caveat applies to PXF switched MPLS traffic with an NSE-100 on a c7300 used as a PE router. When switching MPLS packets to an IP non-VPN destination (label disposition case), none of the supported egress QoS features will be effective on the IP packet.  
This caveat does not apply to packets switched to an IP VPN (deaggregation case).  
There are no known workarounds.
- CSCdy05945  
The PXF support for RPF (Reverse Path Forwarding) on an NSE-100 in a c7300 is not yet VRF aware. RPF will be made VRF aware in a release after 12.1(12c)EX, the release where IP VRF support in PXF is being first introduced.
- CSCdy06022  
On a c7300, the NSE-100 PXF support for NAT does not include per-port timeouts. This support will be added in a subsequent release.
- CSCdy06637  
VRF scalability with the PXF processor on an NSE-100 in a c7300 may be limited to around 500. The exact limit depends on the type and number of IP prefixes. All attempts will be made to improve the VRF scalability to handle around 1000 VRFs in a subsequent release.
- CSCdy06958  
**encapsulation aal5mux** is not supported on a c7300 system for MPLS labeled packets even though this encapsulation can be configured.  
aal5mux encapsulation is supported for IP packets and the caveat only applies to MPLS packets. There is no workaround other than to try and use the aal5snap encapsulation.
- CSCdy12530  
On a c7300 system configured with an NSE-100, pings to a native VLAN sub-interface on a GigE port may fail. This happens whether ICMP echo reply handling is done in PXF or the RP. VLAN id's greater than 1 are not affected. Through traffic across the native vlan is not affected.  
There is no workaround.
- CSCdy14458  
When a sub-interface is in shutdown state, configuring svc under the sub-interface will trigger this sub-interface to up state. Similarly, a shutdown-state sub-interface will be triggered to up-state after C7300 reload if this sub-interface has svc configured.  
Workaround: Shutdown the sub-interface after configuring svc.
- CSCdy17263  
If configure more than 1000 VCs in one OC3-ATM port and each VC has WRED feature applied, some of the VCs may not work properly that they can not transfer traffic.  
Work around: Configure 1000 or less VCs in one OC3-ATM port if each VC has WRED feature configured.

- CSCdy17908

A 7300 may experience a hang or crash with a MISTRAL error similar to:

```
MISTRAL-3-ERROR: Error condition detected: SYSAD_TIMEOUT_DPATH
```

There are no known workarounds.

- CSCdy19425

On a c7300 system configured with an NSE-100, spurious accesses for reads from a very low memory address may be reported together with a traceback. NAT translations do not seem to be affected.

In some cases, the system may stop responding to user input after an extended period, even though it may be switching traffic.

This caveat seems to be triggered when doing inside to outside static NAT with overload.

Workaround is to try and use dynamic NAT and avoid using static NAT.

## Resolved Caveats—Cisco IOS Release 12.1(12c)EX

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(12c)EX. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx12712

On a c7300 system with an NSE-100, packets destined to some 802.1q vlan sub-interfaces are silently dropped.

The packet drops occur if you configure more than 236 sub-interfaces with 802.1q vlan encapsulation on a single Gigabit ethernet interface. The packets are punted to the Route Processor by the PXF processor, and the Route Processor silently drops them. This caveat currently limits the number of usable sub-interfaces with 802.1q vlan encapsulation on any GigE port to 236.

There are no known workarounds.

- CSCdx14359

After an ATM PVP is configured, the newly created VP is in INAC state and does not associate with its VCs. Need shutdown / no shutdown on the interface to change the VP state and activate the VCs. The problem is associated with VP initialization and activation.

There are no known workarounds.

- CSCdx18960

When a SVC is tore down on a C7300 OC3-ATM line card, input traffic for that SVC will be punt to RP. Packets may be dropped if input traffic is heavier then RP can handle. If ATM control traffic has the same priority level as data packets, ATM control packets may be dropped also.

The changes of this DDTS is to set ATM control packets with higher priority in both ingress (Toaster to RP) and egress (RP to Toaster) sides. This avoids loss of ATM control packets.

There are no known workarounds.

- CSCdx23186

On a c7300 system with NSE-100, the maximum throughput achieved when policing in PXF is slightly lower than expected by about 200Kpps.

There are no known workarounds.

- CSCdx27566  
On a c7300 system with an NSE-100, **show ip traffic** does not show any fragmentation statistics for IP packets fragmented in the RP fast switching path. There is no workaround and this is only an accounting issue.
- CSCdx29732  
On a c7300 system with an NSE-100, PXF processed packets that are dropped by Reverse Path Forwarding but permitted by a configured Access Control List are not accounted as suppressed drops.  
Example Interface Configuration:  
**ip verify unicast reverse-path 172** If packets are dropped by Reverse Path Forwarding but are permitted by a corresponding rule in the Access Control List (in this case 172), these packets are currently not accounted as suppressed drops. They are however accounted as pxf switched packets and in the corresponding counters of the appropriate rule of the Access Control List  
Workaround: These packets are accounted for in the output of **show ip access-list counters** under the corresponding rule in the Access Control List.
- CSCdx36545  
A c7300 with a large number of ethernet dot1q sub interfaces may take additional time to boot.
- CSCdx37159  
Executing hardware module stop/start with SVC configured may cause C7300 crash. The reason of this problem is that ATM signalling function calls teardown SVC after an interface is gone and does not check the status of the interface.
- CSCdx38526  
If the default WRED parameters (min-threshold, max-threshold, mark-probability, and exponential weight) are selected to be used, suggest to change the exponential weight from default value 9 to 4 by the following command since the threshold values are smaller: **(config-pmap-c)#random exponential 4**
- CSCdx44140  
This DDTS is used to enable RP level PPP over ATM feature for C7300 platform.
- CSCdx44699  
The problem is when set an OC3-ATM interface at loopback mode, the loopback led of that interface did not turn yellow which is required.
- CSCdx44706  
A C7300 system with an NSE-100 processor card may experience a catastrophic SYSAD\_TIMEOUT\_DPATH failure under certain stress conditions. Cause of this failure is not fully understood.
- CSCdx46041  
In c7300 images prior to 12.1(10)EX release, T3 linecard can cause a system crash when it is recovering from fatal errors. This is an extremely rare event.
- CSCdx46535  
When ATM OAM management is configured, OAM packets can not be received at peer router. This problem is due to a new feature check-in which broken the OAM egress path.

- CSCdx52095  
The problem was that new configured VC inherited all the QoS features for the last configured VC under the same sub-interface.
- CSCdx60576  
Configuring PPP authentication on an ATM VC with encapsulation type of AAL5MUX PPP caused a catastrophic failure due to **MISTRAL\_GLOBAL\_HW\_HAZARD: 29 0x0008**. This failure was caused by a caveat in handling very small 6 byte packets related to the PPP authentication protocol. There is no known workaround other than to avoid authentication.
- CSCdx61081  
The C7300 system with an NSE-100 processing engine does not support access-list based rate-limit. Rate-limiting is instead configured via the class based **police** command under the modular QoS commands framework.
- CSCdx61687  
On a C7300 system with an NSE-100 processor card, ethernet\_SNAP encapsulated IP packets get dropped by the RP when not processed by the PXF. PXF forwarding of such packets works fine.
- CSCdx63894  
This commit is require to fix the occasional in-accurate reporting of GE interface line protocol state when no negotiation auto is enable and the cable is plug/unplug.
- CSCdx71070  
This DDTS is used to bundle OC3-ATM line card FPGA image version 16 to IOS image. This OC3-ATM line card FPGA image fixed the problem that port loopback LED did not turn to yellow when that port was configured at loopback mode.  
  
This FPGA image also has the enhancement of transferring ATM control packets such as OAM packets, ATM signal packets through FPGA control buffer instead of per port data buffer.
- CSCdx87286  
There was a CLI command that did not allow user to configure VBR vc with PCR or SCR between half line-rate and line rate since 10EX1 IOS image release.
- CSCdx95161  
NSE DB and MB - No operational functional changes. Added diagnostic capabilities for failure analysis for manufacturing and engineering development.  
T3 - No operational functional changes. Optimized timing to improve manufacturing yield.
- CSCdy10381  
During the hardware configuration verification process, the system migrates from the bandwidth point terminology to communicate with the user in terms the total aggregate throughput for the line cards. The system still ensures the total aggregate line card throughput does not exceed the capacity of the single connector between the NSE-100 and all the line cards. The information is just presented in another way.  
  
No user action is required for this change.

## Open Caveats—Cisco IOS Release 12.1(10)EX2

This section documents possible unexpected behavior by Cisco IOS Release 12.1(10)EX2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx12712

On a c7300 system with an NSE-100, packets destined to some 802.1q vlan sub-interfaces are silently dropped.

The packet drops occur if you configure more than 236 sub-interfaces with 802.1q vlan encapsulation on a single Gigabit ethernet interface. The packets are punted to the Route Processor by the PXF processor, and the Route Processor silently drops them. This caveat currently limits the number of usable sub-interfaces with 802.1q vlan encapsulation on any GigE port to 236.

There are no known workarounds.

- CSCdx14359

After an ATM PVP is configured, the newly created VP is in INAC state and does not associate with its VCs. Need shutdown / no shutdown on the interface to change the VP state and activate the VCs. The problem is associated with VP initialization and activation.

There are no known workarounds.

- CSCdx18960

When a SVC is tore down on a C7300 OC3-ATM line card, input traffic for that SVC will be punt to RP. Packets may be dropped if input traffic is heavier then RP can handle. If ATM control traffic has the same priority level as data packets, ATM control packets may be dropped also.

The changes of this DDTS is to set ATM control packets with higher priority in both ingress (Toaster to RP) and egress (RP to Toaster) sides. This avoids loss of ATM control packets.

There are no known workarounds.

- CSCdx23186

On a c7300 system with NSE-100, the maximum throughput achieved when policing in PXF is slightly lower than expected by about 200Kpps.

There are no known workarounds.

- CSCdx27566

On a c7300 system with an NSE-100, **show ip traffic** does not show any fragmentation statistics for IP packets fragmented in the RP fast switching path. There is no workaround and this is only an accounting issue.

- CSCdx27982

On a c7300 system with an NSE-100, configuring **ip verify unicast reverse-path** may cause inconsistent behavior when replying to ICMP echo requests (pings) over a POS interface.

If you configure Reverse Path Forwarding on a POS interface, valid ping packets might be dropped. This behavior is observed very rarely and is not easily reproducible.

There are no known workarounds.

- CSCdx29732

On a c7300 system with an NSE-100, PXF processed packets that are dropped by Reverse Path Forwarding but permitted by a configured Access Control List are not accounted as suppressed drops.

Example Interface Configuration:

**ip verify unicast reverse-path 172** If packets are dropped by Reverse Path Forwarding but are permitted by a corresponding rule in the Access Control List (in this case 172), these packets are currently not accounted as suppressed drops. They are however accounted as pxf switched packets and in the corresponding counters of the appropriate rule of the Access Control List

Workaround: These packets are accounted for in the output of **show ip access-list counters** under the corresponding rule in the Access Control List.

## Resolved Caveats—Cisco IOS Release 12.1(10)EX2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(10)EX2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw08796

On a Cisco 7500 series router, the router may unexpectedly reload when a crypto map is applied to an interface.

There are no known workarounds.

- CSCdw32990

On a Cisco 7200 series router, removing the access-list entry when it is in use by a crypto map applied to interface(s) may crash the router.

There are no known workarounds.

- CSCdw73511

On a Cisco 7300 router, When ENTITY-MIB is queried, the entPhysicalDescr entry for the NSE board (CPU card) reports wrong hardware serial number and wrong hardware revision. The entPhysicalIsFRU entries for the field replaceable units are also mistakenly reported as false. The entPhysicalSerialNum entries are also blank.

There are no known workarounds.

- CSCdw94400

For system configured with large number of VCs and/or in conjunction with large number of sub-interfaces the system appears as no response for several minutes during bootup. This is a known issue and is a result of internal processing of the large number of VCs. Allow it the time to complete this process and the router will proceed to operate as normal.

This problem only occurs during bootup on system with large number of VCs configured or during the configuration of large number of VCs like copying configurations file with large number of VCs configured from nvram, flash, disk to the running-config. OIRing the atm linecard or issuing shut/no-shut does on the atm port will not cause this problem.

There are no known workarounds.

- CSCdx00377

The problem occurred when 100 VBR-nrt VCs are configured and each VC has SCR = 434 Kbps. It also occurred for 100 UBR VCs with PCR = 434 Kbps. The shaped VCs yield a rate of 50% of the configured rate. If each VBR-nrt VC is configured with SCR = 433 Kbps, or 435 Kbps, or other allowed rates, the problem does not happen. It is true for the PCR of UBR VCs. The problem can only be reproduced by a certain kind of test equipment currently. It is still under investigation whether it is an issue of the test equipment or it is a router system problem.

There are no known workarounds.

- CSCdx08542

On a Cisco 7300 series router, execution of the **show c7300 pxf cef** command on an NSE-100 may sometimes cause a display of the following messages:

```
00:23:07: ws_direct_read: address/offset is invalid: src 0 , dst 44481C00
00:23:07: ws_direct_read: out of boundary 0x0 0xFE800000 was attempting to
display
```

CEF load balancing may need to be configured to trigger these messages.

There are no known workarounds.

- CSCdx29868

On a Cisco 7300 series router, upgrading Windstar FPGA via VTY cause the system to reload. The problem occurs after issuing the “upgrade fpga all” commands from the remote VTY session.

Workaround: Upgrading fpga via direct console connection.

## Open Caveats—Cisco IOS Release 12.1(10)EX1

This section documents possible unexpected behavior by Cisco IOS Release 12.1(10)EX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw61239
 

On Cisco 7304 router running releases prior to 12.1(10)EX1, you may observe the following problem:

When a FPGA is being upgraded from the console, executing the **show c7300** command from a VTY connection, corrupts the FPGA and the FPGA upgrade process does not complete successfully.

There are no known workarounds.
- CSCdw61263
 

On the Cisco 7304 router running IOS releases prior to 12.1(10)EX1, you may observe the following problem:

When the system is in minimal boot mode, executing the **show c7300** command crashes the system.

There are no known workarounds.
- CSCdw73511
 

On a Cisco 7300 router, When ENTITY-MIB is queried, the entPhysicalDescr entry for the NSE board (CPU card) reports wrong hardware serial number and wrong hardware revision. The entPhysicalIsFRU entries for the field replaceable units are also mistakenly reported as false. The entPhysicalSerialNum entries are also blank.

There are no known workarounds.
- CSCdw93271
 

Japan SDH requires that all Z0 bytes have the value 10 (AA). Capella has the first 16 Z0 bytes set to something different in SDH mode.

There are no known workarounds.
- CSCdw94400
 

For system configured with large number of VCs and/or in conjunction with large number of sub-interfaces the system appears as no response for several minutes during bootup. This is a known issue and is a result of internal processing of the large number of VCs. Allow it the time to complete this process and the router will proceed to operate is normal.

This problem only occurs during bootup on system with large number of VCs configured or during the configuration of large number of VCs like copying configurations file with large number of VCs configured from nvram, flash, disk to the running-config. OIRing the atm linecard or issuing shut/no-shut does on the atm port will not cause this problem.

There are no known workarounds.
- CSCdw95046
 

On a c7300 system, ICMP replies for ACL denies generated by the PXF processor are not rate-limited.

There are no known workarounds.

- CSCdx00377

The problem occurred when 100 VBR-nrt VCs are configured and each VC has SCR = 434 Kbps. It also occurred for 100 UBR VCs with PCR = 434 Kbps. The shaped VCs yield a rate of 50% of the configured rate. If each VBR-nrt VC is configured with SCR = 433 Kbps, or 435 Kbps, or other allowed rates, the problem does not happen. It is true for the PCR of UBR VCs. The problem can only be reproduced by a certain kind of test equipment currently. It is still under investigation whether it is an issue of the test equipment or it is a router system problem.

There are no known workarounds.

- CSCdx07907

The PXF LLQ implementation on a c7300 system assigns a fixed weightage of 90% to an interface's priority queue, with the balance 10% going to the other non-priority queues, so that the priority queue does not starve the other queues. This will be modified to make the priority queue weightage configurable so that users can chose anywhere up to 100% weightage (for strict priority) if they so desire.

There are no known workarounds.

- CSCdx10720

A mismatch autonegotiation configuration between Windstar GE port and a remote GE port will cause the Windstar GE port to show line UP and protocol UP and will not pass traffic through. This is a known issue and will be fixed future releases.

A typical mismatch configuration is when user enable **Autonegotiation ON** on Windstar GE port and have **Autonegotiation OFF** on the connected remote GE port.

The workaround for this problem is to ensure both ends match, that is Windstar GE Port <----->  
Connected Remote GE Port

-----	-----
Autonegotiation ON	Autonegotiation ON
Autonegotiation OFF	Autonegotiation OFF

## Resolved Caveats—Cisco IOS Release 12.1(10)EX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(10)EX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv76107

Multicast packet handling does not work correctly on the FastEthernet management interface of the NSE100 card of the Cisco c7300 router platform.

There are no known workarounds.

- CSCdw35614

Under heavy traffic, changing service policy on OC3 POS interface while traffic is running could hang the console.

Workaround: Stop traffic on the port first.

- CSCdw46504

When sonet LOP (loss of path) alarm is cleared, PPLM alarm is falsely detected and it results sending RDI to far end.

There are no known workarounds.

## Open Caveats—Cisco IOS Release 12.1(10)EX

This section documents possible unexpected behavior by Cisco IOS Release 12.1(10)EX and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.1(10)EX.

## Resolved Caveats—Cisco IOS Release 12.1(10)EX

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(10)EX. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv82103
 

On a Cisco 7300 router, when either DLSw+ or Transparent Bridging are configured on either a Fast Ethernet interface or a Gigabit Ethernet interface, then IP connectivity to the router via that interface's IP address is lost. An outside entity will be unable to contact that IP address via Ping, Telnet, or other IP access methods.

Workaround: Remove the transparent bridging and/or DLSw+ configuration and IP connectivity will be restored.
- CSCdw15420
 

If a Cisco 7300 series router is configured as a DLSw+ peer, and transparent bridging is configured to bridge traffic from the Gigabit Ethernet interface into DLSw+, the router will reload upon any attempt to start a DLSw+ circuit using the Gigabit Ethernet interface as a LAN connection.

There are no known workarounds.
- CSCdw29879
 

On a Cisco c7300 system, when CEF load balancing is configured and one of the load balanced paths transitions from Up to DOWN to Up state, the following message may be displayed:

```
"<time>: ws_fib_tt_addr_to_index: out of range"
```

This is a cosmetic message caused by a race condition when re-updating the load balancing information after the path has come back to an operational state.

There are no known workarounds.
- CSCdw31309
 

A Cisco 7300 series router configured for Data-Link Switching (DLSw+) with Fast Sequenced Transport (FST) encapsulation experiences a large number of data alignment corrections, which significantly degrade performance especially in high DLSw+ traffic environments.

Workaround: Use TCP encapsulation to get the benefits of local DLC acknowledgement.

- CSCdw56354

A Cisco 7300 series router using a 12.1(9)EX2 or later boothelper image (c7300-boot-mz) to boot a 12.1(9)EX1 IOS system image (such as c7300-is-mz or c7300-js-mz) will cause the following error message to continuously appear on the console:

```
OIRINT: Long OIR interrupt, status 0x0400
```

This is due to the fact that the NSE100 Gigabit Ethernet interface GBIC Online Insertion and Removal (OIR) interrupt support was first introduced in 12.1(9)EX2. When using a 12.1(9)EX2 or later c7300-boot-mz image, the GBIC OIR interrupt is enabled. If this is used to boot a 12.1(9)EX1 system image that does not have the GBIC OIR interrupt support, this error message is generated.

Workaround: Use 12.1(9)EX2 and later c7300-boot-mz images only with 12.1(9)EX2 and later system images. If the 12.1(9)EX1 system image must be used, use the corresponding 12.1(9)EX1 c7300-boot-mz image to avoid enabling the OIR interrupt.

- CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

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

## Open Caveats—Cisco IOS Release 12.1(9)EX3

This section documents possible unexpected behavior by Cisco IOS Release 12.1(9)EX3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.1(9)EX3.

## Resolved Caveats—Cisco IOS Release 12.1(9)EX3

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(9)EX3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

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

## Open Caveats—Cisco IOS Release 12.1(9)EX2

This section documents possible unexpected behavior by Cisco IOS Release 12.1(9)EX2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv10449

If the system is reloaded while there is incoming traffic to one of the ports on the 4xOC3 POS line card, sometimes, after reload, the system is unable to forward traffic. In this case, another reload is required.

Workaround: Shut down all OC3 POS interfaces and save the running configuration to nonvolatile memory before reloading the system.

Alternative workaround: Configure **pos ais-shut** on the OC3 POS interface.

- CSCdv29682

On a Cisco 7300 series router, fast fragmentation of IP packets is done by the RP in the old cache-based fast switching path, not the CEF switching path. While there is no anomaly in this functionality, the fragmentation may not be obvious from any show or debug commands related to CEF.

There are no known workarounds.

- CSCdv72888

The kbps bandwidth value in the priority sub-command for a class under a policy-map is currently not supported on a c7300 system. Though the value is accepted, it is silently ignored. This caveat will be fixed in a future release so that the bandwidth limit on the priority queue has effect.

There are no known workarounds.

- CSCdv73310

On a Cisco c7300 system, classification of packets for PXF accelerated QoS features has to be done via access list statements supported by TurboACL.

The **match ip precedence value** or **match ip dscp value** match statements under a class-map are not supported in PXF. In order to match on IP precedence or DSCP values, appropriate access-list entries need to be defined and then used via **match access-group list**.

There are no known workarounds.

## Resolved Caveats—Cisco IOS Release 12.1(9)EX2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(9)EX2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu41610

On a Cisco 7300 series router, autonegotiation might not work on the Gigabit Ethernet Interfaces on the Network Services Engine-100 (NSE-100). The default configuration on the 7300 is **no negotiation auto**.

Workaround: Configure both sides of the Gigabit Ethernet connection to the **no negotiation auto** command in the interface subcommand.

- CSCdv55966

On a Cisco 7300 series router, IP packets requiring fragmentation are sent to the RP by the PXF for the fragmentation. Such packets have their TTL value decremented by 2.

There are no known workarounds.

- CSCdw15420

If a Cisco 7300 series router is configured as a DLSw+ peer, and transparent bridging is configured to bridge traffic from the Gigabit Ethernet interface into DLSw+, the router will reload upon any attempt to start a DLSw+ circuit using the Gigabit Ethernet interface as a LAN connection.

There are no known workarounds.

## Open Caveats—Cisco IOS Release 12.1(9)EX1

This section documents possible unexpected behavior by Cisco IOS Release 12.1(9)EX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu41610

Autonegotiation may not work on the Gigabit Ethernet Interfaces on the Network Services Engine-100 (NSE-100).

Workaround: Configure both sides of the Gigabit Ethernet connection to the **no negotiation auto** command in the interface subcommand.



**Note**

The Cisco 7304 router are set with a default of *no nego auto*. As long as this default has not been changed, only the other side of the Gigabit Ethernet connection needs to be configured.

- CSCdv10449

If the system is reloaded while there is incoming traffic to one of the ports on the 4xOC3 POS line card, sometimes, after reload, the system is unable to forward traffic. In this case, another reload is required.

Workaround: Shut down all OC3 POS interfaces and save the running configuration to nonvolatile memory before reloading the system.

Alternative workaround: Configure **pos ais-shut** on the OC3 POS interface.

- CSCdv29682  
On a Cisco 7300 series router, fast fragmentation of IP packets is done by the RP in the old cache-based fast switching path, not the CEF switching path. While there is no anomaly in this functionality, the fragmentation may not be obvious from any show or debug commands related to CEF.  
There are no known workarounds.
- CSCdv55966  
On a Cisco 7300 series router, IP packets requiring fragmentation are sent to the RP by the PXF for the fragmentation. Such packets have their TTL value decremented by 2.  
There are no known workarounds.

## Resolved Caveats—Cisco IOS Release 12.1(9)EX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(9)EX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no resolved caveats for Cisco IOS 12.1(9)EX1.

## Open Caveats—Cisco IOS Release 12.1(9)EX

This section documents possible unexpected behavior by Cisco IOS Release 12.1(9)EX and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu41610  
Autonegotiation may not work on the Gigabit Ethernet Interfaces on the Network Services Engine-100 (NSE-100).  
Workaround: Configure both sides of the Gigabit Ethernet connection to the **no negotiation auto** command in the interface subcommand.




---

**Note** The Cisco 7304 router are set with a default of *no nego auto*. As long as this default has not been changed, only the other side of the Gigabit Ethernet connection needs to be configured.

---

- CSCdv10449  
If the system is reloaded while there is incoming traffic to one of the ports on the 4xOC3 POS line card, sometimes, after reload, the system is unable to forward traffic. In this case, another reload is required.  
Workaround: Shut down all OC3 POS interfaces and save the running configuration to nonvolatile memory before reloading the system.  
Alternative workaround: Configure **pos ais-shut** on the OC3 POS interface.

- CSCdv29682  
On a Cisco 7300 series router, fast fragmentation of IP packets is done by the RP in the old cache-based fast switching path, not the CEF switching path. While there is no anomaly in this functionality, the fragmentation may not be obvious from any show or debug commands related to CEF.  
There are no known workarounds.
- CSCdv55966  
On a Cisco 7300 series router, IP packets requiring fragmentation are sent to the RP by the PXF for the fragmentation. Such packets have their TTL value decremented by 2.  
There are no known workarounds.

## Related Documentation

The following sections describe the documentation available for the Cisco 7304 router. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents, page 65](#)
- [Platform-Specific Documents, page 66](#)
- [Feature Modules, page 67](#)
- [Cisco IOS Software Documentation Set, page 67](#)

## Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.1 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

On Cisco.com at:

**Technical Documents: All Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes**

On the Documentation CD-ROM at:

**Cisco Product Documentation: All Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

**Technical Documents**

- *Caveats for Cisco IOS Release 12.1 EX*

As a supplement to the caveats listed in “[Important Notes](#)” in these release notes, see *Caveats for Cisco IOS Release 12.1* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.1.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: Release Notes: Caveats**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Caveats**



**Note**

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

## Platform-Specific Documents

These documents are available for the Cisco 7304 router on Cisco.com and the Documentation CD-ROM:

- Cisco 7300 Line Card Documentation
- Cisco 7300 Router Installation and Configuration Guide
- Cisco 7300 Series Platform-Specific Commands
- Cisco 7304 Online Troubleshooting
- Cisco 7304 Router Documentation Flyer
- Cisco 7304 Router Line Card Hardware Configuration Guidelines
- Cisco 7304 Router Quick Start Guide
- Cisco 7304 Router Troubleshooting and Configuration Notes
- Gigabit Interface Converter Installation Instructions
- Network Services Engine Installation and Configuration Guide
- Regulatory Compliance and Safety Information for Cisco 7304 Routers

On Cisco.com at:

**Technical Documents: All Product Documentation: Core/High-End Routers**

On the Documentation CD-ROM at:

**Cisco Product Documentation: All Product Documentation: Core/High-End Routers**

## Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1(13)EX3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: New Feature Documentation**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation**

## Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

## Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1: Configuration Guides and Command References**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References**

## Cisco IOS Release 12.1 Documentation Set Contents

Table 20 lists the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form if ordered.



**Note**

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.1**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1**

**Table 20 Cisco IOS Release 12.1 Documentation Set**

Books	Major Topics
<ul style="list-style-type: none"> <li><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li><i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Configuration Fundamentals Overview</li> <li>Cisco IOS User Interfaces</li> <li>Cisco IOS File Management</li> <li>Cisco IOS System Management</li> <li>Cisco IOS User Interfaces Commands</li> <li>Cisco IOS File Management Commands</li> <li>Cisco IOS System Management Commands</li> </ul>
<ul style="list-style-type: none"> <li><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i></li> </ul>	<ul style="list-style-type: none"> <li>Using Cisco IOS Software</li> <li>Overview of SNA Internetworking</li> <li>Bridging</li> <li>IBM Networking</li> </ul>

**Table 20 Cisco IOS Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions

**Table 20 Cisco IOS Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Security Overview</li> <li>Authentication, Authorization, and Accounting (AAA)</li> <li>Security Server Protocols</li> <li>Traffic Filtering and Firewalls</li> <li>IP Security and Encryption</li> <li>Other Security Features</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Cisco IOS Switching Services Overview</li> <li>Cisco IOS Switching Paths</li> <li>Cisco Express Forwarding</li> <li>NetFlow Switching</li> <li>Multiprotocol Label Switching</li> <li>Multilayer Switching</li> <li>Multicast Distributed Switching</li> <li>Virtual LANs</li> <li>LAN Emulation</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Wide-Area Networking Overview</li> <li>Configuring ATM</li> <li>Configuring Frame Relay</li> <li>Configuring Frame Relay-ATM Interworking</li> <li>Configuring SMDS</li> <li>Configuring X.25 and LAPB</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• New Features in 12.1-Based Limited Lifetime Releases</li> <li>• New Features in Release 12.1 T</li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> </ul>	

# Obtaining Documentation

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

## World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at [http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml).

## Documentation CD-ROM

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

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

# Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

## Cisco.com

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

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

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

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

<http://www.cisco.com>

## Technical Assistance Center

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

## Contacting TAC by Using the Cisco TAC Website

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

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

P3 and P4 level problems are defined as follows:

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

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

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

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

## Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 65.

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Copyright © 2001-2003  
Cisco Systems, Inc.  
All rights reserved.