Release Notes for Cisco 7000 Series Routers for Cisco IOS Release 12.2 SZ

April 21, 2004

Cisco IOS Release 12.2(14)SZ6

OL-4268-07

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(14)SZ6. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(14)SZ6, see the "Caveats for Cisco IOS Release 12.2 SZ" section on page 18.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:
http://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback .

Contents

These release notes describe the following topics:

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(14)SZ6 and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ6

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	128 MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ5

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7301-is-mz	64 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	64 MB	128 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	64 MB	128 MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ4

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM
Cisco 7301 Series	IP Standard Feature Set	IP	c7300-is-mz	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ3

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ2

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7300-p-mz	64 MB	256 MB	RAM
	IP Standard Feature Set	IP	c7301-is-mz	128 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7301-js-mz	128 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	c7301-p-mz	128 MB	256 MB	RAM

Table 6 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ1

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	7300-p-mz	64 MB	256 MB	RAM

Table 7 Images and Memory Recommendations for Cisco IOS Release 12.2(14)SZ

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	64 MB	256 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7300-js-mz	64 MB	256 MB	RAM
	Service Provider Standard Feature Set	Service Provider	7300-p-mz	64 MB	256 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(14)SZ6 supports the following Cisco 7000 family platforms:

- Cisco 7301 router
- Cisco 7304 router

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 8.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7304 Software (c7300-is-mz), Version 12.2(14)SZ6, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to S*oftware Installation and Upgrade Procedures* located at the following URL:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

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 12.2 SZ supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2 SZ can include new features supported by the Cisco 7000 family.

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.

Table 8 lists the features and feature sets supported by the Cisco 7000 family in Cisco IOS Release 12.2(14)SZ6 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, (14)SZ means a feature was introduced in 12.2(14)SZ. If a cell in this column is empty, the feature was included in the initial base release.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com.

Table 8 Feature List by Feature Set for the Cisco 7304

Features	In	Software Images by Feature Sets			
		IP	Enterprise	Service Provider	
Ethernet over MPLS	(14)SZ	Yes	Yes	Yes	
MPLS Traffic Engineering	(14)SZ3	Yes	Yes	Yes	
MPLS VPN—VRF Selection Based on Source IP Address	(14)SZ	Yes	Yes	Yes	
PXF Show Command Changes	(14)SZ	Yes	Yes	Yes	
Quality of Service for Virtual Private Networks in PXF	(14)SZ3	Yes	Yes	Yes	
VRF Aware GRE Tunnels in PXF	(14)SZ3	Yes	Yes	Yes	

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.2 SZ.

New Hardware Features in Cisco IOS Release 12.2(14)SZ6

There are no new hardware features supported in Cisco IOS Release 12.2(14)SZ6.

New Software Features in Cisco IOS Release 12.2(14)SZ6

There are no new software features supported in Cisco IOS Release 12.2(14)SZ6.

New Hardware Features in Cisco IOS Release 12.2(14)SZ5

There are no new hardware features supported in Cisco IOS Release 12.2(14)SZ5.

New Software Features in Cisco IOS Release 12.2(14)SZ5

There are no new software features supported in Cisco IOS Release 12.2(14)SZ5.

New Hardware Features in Cisco IOS Release 12.2(14)SZ4

There are no new hardware features supported in Cisco IOS Release 12.2(14)SZ4.

New Software Features in Cisco IOS Release 12.2(14)SZ4

There are no new software features supported in Cisco IOS Release 12.2(14)SZ4.

New Hardware Features in Cisco IOS Release 12.2(14)SZ3

There are no new hardware features supported in Cisco IOS Release 12.2(14)SZ3.

New Software Features in Cisco IOS Release 12.2(14)SZ3

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(14)SZ3:

MPLS Traffic Engineering

Platform: Cisco 7304 router

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient, so that they can withstand link or node failures.

MPLS traffic engineering provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

MPLS traffic engineering routes traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.

MPLS traffic engineering employs "constraint-based routing," in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS traffic engineering, the flow has bandwidth requirements, media requirements, a priority over other flows, and so on.

- MPLS traffic engineering gracefully recovers to link or node failures that change the topology of the backbone by adapting to the new set of constraints.
- In Cisco IOS Release 12.2(14)SZ3, the following MPLS Traffic Engineering features are introduced. This list also notes the features that were introduced in the PXF switching path:
- MPLS Traffic Engineering—basic PXF switching and accounting (PXF)
- Basic PXF switching and accounting of MPLS Traffic Engineering traffic.
- MPLS Traffic Engineering—Load Balancing (PXF)

  Allows a router to balance Traffic Engineering traffic over multiple Traffic Engineering tunnels.
- MPLS Traffic Engineering—Automatic Bandwidth Adjustment (PXF)

  Automatically resizes a tunnel based on the tunnel's utilization. Automatic Bandwidth Adjustment decides whether to resize a tunnel at a specified collection frequency. The frequency is the number of seconds between samples of the tunnel output rate.
- MPLS Traffic Engineering—1-hop MPLS-Traffic Engineering tunnel support (PXF)

  An MPLS Traffic Engineering tunnel where the tunnel-head and the tunnel-tail routers are connected back to back is referred to as a 1-hop tunnel. In the 1-hop tunnel, the Label Switched Path terminates at the next hop. 1-hop MPLS Traffic Engineering tunnels are supported in PXF.
- MPLS Traffic Engineering over Frame Relay, 802.1q, and ATM subinterfaces (PXF)

  MPLS Traffic Engineering is supported over Frame Relay, 802.1q, and ATM subinterfaces in PXF.
- MPLS Traffic Engineering—Auto Route Calculation

  The MPLS Traffic Engineering Auto Route Calculation is used to instruct the Interior Gateway Protocol to use a tunnel in it's Shortest Path First (SPF)/next-hop calculation if the tunnel is up.

- MPLS Traffic Engineering—IP Explicit Address Exclusion Support

  The ability to include and exclude given explicit IP addresses during Label Switched Path (LSP) setup.

- MPLS Traffic Engineering—Link Coloring

  The affinity bits are an MPLS label distribution tunnel's requirements on the attributes of the links the tunnel will cross. The tunnel's affinity bits and affinity mask must match up with the attributes of the various links carrying the tunnel.

For sample MPLS Traffic Engineering configurations, see the Cisco 7304 Troubleshooting and Configuration Notes document.

Quality of Service for Virtual Private Networks in PXF

Platform: Cisco 7304 router

The Quality of Service for Virtual Private Networks feature, which pre-classifies packets for QoS purposes in a VPN, is now available in PXF.

When packets are encapsulated by tunnel or encryption headers, Quality of Service (QoS) features are unable to examine the original packet headers and correctly classify the packets. Packets traveling across the same tunnel have the same tunnel headers, so the packets are treated identically if the physical interface is congested.

With the growing popularity of Virtual Private Networks (VPNs), the need to classify traffic within a traffic tunnel is gaining importance. QoS features have historically been unable to classify traffic within a tunnel. With the introduction of the Quality of Service for Virtual Private Networks (QoS for VPNs) feature, packets can now be classified before tunneling and encryption occur. The process of classifying packets before tunneling and encryption allows routers to configure QoS features and tunneling and cypto maps on the same interface.

The QoS for VPNs feature is designed for tunnel interfaces. When the new feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be adjusted in congested environments. The end result is more effective packet tunneling.

The QoS for VPNs feature pre-classifies a packet for QoS purposes in a VPN and is enabled using the **qos pre-classify** command. This feature is restricted to tunnel and virtual template interfaces.

VRF Aware GRE Tunnels in PXF

Platform: Cisco 7304 router

VRF Aware GRE tunnels are now available in PXF.

This feature allows you to configure the source and destination of a tunnel to belong to any Virtual Private Network (VPN) routing/forwarding (VRFs) tables. A VRF table stores routing data for each VPN. The VRF table defines the VPN membership of a customer site attached to the network access server (NAS). Each VRF table comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

For a sample VRF Aware GRE tunnel in PXF, see the Cisco 7304 Troubleshooting and Configuration Notes document.

New Hardware Features in Cisco IOS Release 12.2(14)SZ2

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(14)SZ2:

NSE-100 Hardware MAC Addresses Filtering

Platform: Cisco 7304 router

Each native Gigabit Ethernet port on the NSE-100 can support up to 16 hardware MAC addresses. Each ports MAC addressees are stored in a hardware MAC address filtering table. With two NSE-100s installed, the chassis can support up to four native Gigabit Ethernet ports.

Phase 2 PA Support

Platform: Cisco 7301 router and Cisco 7304 router

The following Port Adaptors are now supported on the 7304 Carrier Card for 7200 Series Port Adapters:

- PA-POS-2OC3
- PA-A3-8E1IMA
- PA-A3-8T1IMA

The following Port Adaptor is now supported on the 7301:

- PA-POS-2OC3

New Software Features in Cisco IOS Release 12.2(14)SZ2

There are no new software features supported in Cisco IOS Release 12.2(14)SZ2.

New Hardware Features in Cisco IOS Release 12.2(14)SZ1

There are no new hardware features supported in Cisco IOS Release 12.2(14)SZ1.

New Software Features in Cisco IOS Release 12.2(14)SZ1

There are no new software features supported in Cisco IOS Release 12.2(14)SZ1.

New Hardware Features in Cisco IOS Release 12.2(14)SZ

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(14)SZ:

NPE-G100

Platform: Cisco 7304 router

The NPE-G100 contains the route processor that maintains and executes the system management functions, as well as the forwarding path and forwarding packet functions, and also holds the system memory and environmental monitoring functions for the Cisco 7304 router.

The NPE-G100 consists of the following components:

- BCM 1250 processor system:
  - Microprocessor operates at an internal clock speed of 800 Mhz.
  - Hardware logic to interconnect the processor, dual double data rate synchronous dynamic random-access memory (DDR-SDRAM), hypertransport (HT) interface, the generic PCI bus, and the two midplanes.
  - Cache memory—The NPE-G100 has two levels of cache: primary and secondary cache that are internal to the BCM 1250 processor system with secondary unified cache for data and instruction.
- DDR-SDRAM fro providing code, data, and packet storage.
- Three environmental sensors for monitoring the cooling air as it enters, moves across the system board, and leaves the chassis.
- Three Gigabit Ethernet interfaces (six connectors; three Gigabit Ethernet SFP [optical] and three 10/100/1000 RJ-45s [copper]). For each interface, either the Gigabit Ethernet SFP or the RJ-45 port is available. The ports are linked directly to the BCM 1250 processor system.
- CompactFlash Disk: Stores sufficient code for booting the Cisco IOS boot loader image (bootdisk).
- NVRAM for storing the system configuration and environmental monitoring logs. NVRAM uses a lithium battery to maintain its contents when disconnected from power.
- Upgradeable boot ROM for storing the ROMmon image and upgrading the system to newer versions of the ROMmon image. there are two upgradeable BootROM fro storing the ROMmon image.
- Non-upgradeable boot ROM provides a “golden copy” of the default ROMmon image.
- Auxiliary port with full data terminal equipment (DTE) functionality.
- Console port with full data communications equipment (DCE) functionality.
- ECC (error correction code) system memory and internal L2 cache support.

Phase 2 PA Support

Platform: Cisco 7304 router

The following Port Adaptors are now supported on the 7304 Carrier Card for 7200 Series Port Adapters:

- PA-4E=
- PA-8E=
- PA-4E1G-75=
- PA-4E1G-120=
- PA-4T+=
- PA-8T-232=
- PA-8T-V35=
- PA-8T-X21=
- PA-A3-E3=
- PA-A3-OC3-MM=
- PA-A3-OC3-SMI=
- PA-A3-OC3-SML=
- PA-A3-T3=
- PA-E3=
- PA-2E3=
- PA-FE-FX=
- PA-FE-TX=
- PA-2FE-FX=
- PA-2FE-TX=
- PA-GE=
- PA-H=
- PA-2H=
- PA-MC-2E1/120=
- PA-MC-8E1/120=
- PA-MC-2T1=
- PA-MC-4T1=
- PA-MC-8T1=
- PA-MC-8DSX1
- PA-MC-8TE1+=
- PA-MC-E3=
- PA-MC-STM-1MM=
- PA-MC-STM-1SMI=
- PA-MC-T3=
- PA-MC-2T3+=

- PA-POS-OC3-MM
- PA-POS-OC3-SMI
- PA-POS-OC3-SML
- PA-T3=
- PA-2T3=
- PA-T3+
- PA-2T3+

New Software Features in Cisco IOS Release 12.2(14)SZ

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(14)SZ:

Ethernet over MPLS

Platform: Cisco 7304 router

Ethernet over MPLS is now available on Cisco 7304 routers.

Ethernet over MPLS allows you to connect two VLAN networks that are in different locations, without using expensive bridges, routers, or switches at the VLAN locations. You can enable the MPLS backbone network to accept Layer 2 VLAN traffic by configuring the label edge routers (LERs) at both ends of the MPLS backbone. Adding a point-to-point virtual circuit (VC) requires you to configure the two VC endpoints at the two PE routers. Only the two PE routers at the ingress/egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 VLAN traffic. All other routers do not have table entries for those VCs.

MPLS VPN—VRF Selection Based on Source IP Address

Platform: Cisco 7304 router

The VRF Selection feature allows packets arriving on an interface to be switched into the appropriate VRF table based upon the source IP address of the packets. Once the packets have been "selected" into the correct VRF routing table, they are processed normally based upon the destination address and forwarded through the rest of the Multiprotocol Label Switching (MPLS) VPN.

In most cases, the VRF Selection feature is a "one way" feature; it works on packets coming from the end users to the PE router.

PXF Show Command Changes

Platform: Cisco 7304 router

In Cisco IOS Release 12.2(14)SZ, the **show c7300 pxf** command was changed to **show pxf**. The **c7300** keyword, which had previously been a requirement for entering the command for all IOS Releases that supported the Cisco 7304 (all 12.1EX releases and Release 12.2(11)YZ), is no longer required for entering the command.

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

AGENT-CAPABILITIES for the corresponding MIBs can also be obtained from the above location.

The GPRS specific capability files are

- CISCO-GTP-CAPABILITY.my
- CISCO-GGSN-CAPABILITY.my
- CISCO-GPRS-ACC-PT-CAPABILITY.my
- CISCO-GPRS-CHARGING-CAPABILITY.my
- CISCO-GGSN-QOS-CAPABILITY.my

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 9.

Table 9 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

Table 9 Deprecated and Replacement MIBs (continued)

Deprecated MIB	Replacement
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 12.2 SZ that can apply to the Cisco 7301 router and the Cisco 7304 router.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ6

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.2(14)SZ6. All Cisco IOS Release 12.2(14)SZ6 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.2(14)SZ5.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ5

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.2(14)SZ5. All Cisco IOS Release 12.2(14)SZ5 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.2(14)SZ4.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ4

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.2(14)SZ4. All Cisco IOS Release 12.2(14)SZ4 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.2(14)SZ3.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ3

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.2(14)SZ3. All Cisco IOS Release 12.2(14)SZ3 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.2(14)SZ2.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ2

All Cisco IOS Release 12.2(14)SZ2 software images support the bundled field-programmable gate arrays (FPGA) listed in Table 11.

Table 11 lists the FPGA versions that are bundled in Cisco IOS Release 12.2(14)SZ2 and only applies to the Cisco 7304 router.

Table 10 Bundled FPGA Versions for Cisco IOS Release 12.2(14)SZ2

FPGA Image	FPGA Version Bundled
6T3 Linecard FPGA	0.15
NPE-G100	2.02
OC12 POS Linecard FPGA	0.16
OC3 ATM Linecard FPGA	0.18
OC3 POS Linecard FPGA	0.18
OC48 POS Linecard FPGA	0.15
NSE-100 Daughterboard FPGA	1.04
NSE-100 Motherboard FPGA	1.07
PACC Linecard FPGA	1.10

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 12.2(14)SZ1

There are no new field-programmable gate arrays (FPGA) images for Cisco IOS Release 12.2(14)SZ1. All Cisco IOS Release 12.2(14)SZ1 software images support the bundled field-programmable gate arrays (FPGA) released in Cisco IOS 12.2(14)SZ.

Bundled FPGAs for Cisco IOS Release 12.2(14)SZ

All Cisco IOS Release 12.2(14)SZ software images support the bundled field-programmable gate arrays (FPGA) listed in Table 11.

Table 11 lists the FPGA versions that are bundled in Cisco IOS Release 12.2(14)SZ and only applies to the Cisco 7304 router.

Table 11 Bundled FPGA Versions for Cisco IOS Release 12.2(14)SZ

FPGA Image	FPGA Version Bundled
Clear Channel T3 Linecard FPGA	0.14
NPE-G100	2.02
OC12 POS Linecard FPGA	0.16
OC3 ATM Linecard FPGA	0.17

Table 11 Bundled FPGA Versions for Cisco IOS Release 12.2(14)SZ

FPGA Image	FPGA Version Bundled
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.

Caveats for Cisco IOS Release 12.2 SZ

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 12.2 and Cisco IOS Release 12.2 S are also in Cisco IOS Release 12.2(14)SZ6.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, **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/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 12 Caveats Reference for Cisco IOS Release 12.2 SZ

DDTS Number	Open in Release	Resolved in Release
CSCdu53656		12.2(14)SZ2
CSCdx95364		12.2(14)SZ2
CSCdy61350		12.2(14)SZ2
CSCdy87741		12.2(14)SZ3
CSCdz63182		12.2(14)SZ
CSCdz63669		12.2(14)SZ
CSCdz64878		12.2(14)SZ
CSCdz65342	12.2(14)SZ	
CSCdz65389		12.2(14)SZ
CSCdz68002	12.2(14)SZ	
CSCdz69173	12.2(14)SZ	12.2(14)SZ3

Table 12 Caveats Reference for Cisco IOS Release 12.2 SZ (continued)

CSCdz70316		12.2(14)SZ3
CSCdz71127		12.2(14)SZ2
CSCdz72530		12.2(14)SZ
CSCdz76672		12.2(14)SZ
CSCdz78601		12.2(14)SZ
CSCdz79023		12.2(14)SZ3
CSCdz80757		12.2(14)SZ
CSCdz82441		12.2(14)SZ
CSCdz85439		12.2(14)SZ
CSCdz85927		12.2(14)SZ2
CSCdz87536		12.2(14)SZ
CSCdz87607		12.2(14)SZ
CSCdz87613		12.2(14)SZ
CSCea02012	12.2(14)SZ	
CSCea02355		12.2(14)SZ2
CSCea15744		12.2(14)SZ
CSCea26993		12.2(14)SZ3
CSCea28131		12.2(14)SZ2
CSCea29514		12.2(14)SZ2
CSCea32513		12.2(14)SZ
CSCea33447	12.2(14)SZ	
CSCea35763		12.2(14)SZ
CSCea36962		12.2(14)SZ
CSCea44185	12.2(14)SZ	
CSCea44928	12.2(14)SZ	12.2(14)SZ2
CSCea46135		12.2(14)SZ
CSCea47603		12.2(14)SZ
CSCea50565	12.2(14)SZ	
CSCea51753	12.2(14)SZ	
CSCea52106		12.2(14)SZ2
CSCea55174	12.2(14)SZ	
CSCea55963	12.2(14)SZ	12.2(14)SZ2
CSCea58795		12.2(14)SZ3
CSCea62901	12.2(14)SZ	
CSCea62933	12.2(14)SZ	
CSCea63068	12.2(14)SZ	
CSCea65807	12.2(14)SZ	

Table 12 Caveats Reference for Cisco IOS Release 12.2 SZ (continued)

CSCea66777	12.2(14)SZ	
CSCea68333	12.2(14)SZ	
CSCea69676		12.2(14)SZ2
CSCea72349		12.2(14)SZ
CSCea72684		12.2(14)SZ3
CSCea73517		12.2(14)SZ3
CSCea76179	12.2(14)SZ	12.2(14)SZ1
CSCea78255		12.2(14)SZ2
CSCea80009		12.2(14)SZ3
CSCea82081	12.2(14)SZ	
CSCea83212		12.2(14)SZ2
CSCea83322		12.2(14)SZ2
CSCea83584		12.2(14)SZ2
CSCea83735	12.2(14)SZ	12.2(14)SZ1
CSCea85841		12.2(14)SZ2
CSCea86011		12.2(14)SZ2
CSCea87210		12.2(14)SZ1
CSCea87242		12.2(14)SZ3
CSCea91831		12.2(14)SZ2
CSCeb01067		12.2(14)SZ2
CSCeb01253		12.2(14)SZ2
CSCeb05029		12.2(14)SZ2
CSCeb07170		12.2(14)SZ5
CSCeb08858		12.2(14)SZ2
CSCeb09322		12.2(14)SZ2
CSCeb01188	12.2(14)SZ2	
CSCeb01192	12.2(14)SZ2	
CSCeb11344	12.2(14)SZ2	12.2(14)SZ3
CSCeb19110	12.2(14)SZ2	
CSCeb20619		12.2(14)SZ3
CSCeb21792		12.2(14)SZ2
CSCeb22302	12.2(14)SZ2	
CSCeb26429		12.2(14)SZ2
CSCeb29760		12.2(14)SZ3
CSCeb34069		12.2(14)SZ3
CSCeb39237	12.2(14)SZ2	
CSCeb43106		12.2(14)SZ3

Table 12 Caveats Reference for Cisco IOS Release 12.2 SZ (continued)

CSCeb44478		12.2(14)SZ3
CSCeb51226		12.2(14)SZ3
CSCeb54391	12.2(14)SZ4	
CSCeb56568		12.2(14)SZ3
CSCeb58048		12.2(14)SZ3
CSCeb59610		12.2(14)SZ3
CSCeb66639		12.2(14)SZ4
CSCeb72681	12.2(14)SZ3	
CSCeb82658	12.2(14)SZ4	
CSCeb82722	12.2(14)SZ4	
CSCec02503		12.2(14)SZ4
CSCec11736		12.2(14)SZ4
CSCec14245		12.2(14)SZ4
CSCec14424		12.2(14)SZ4
CSCec14882		12.2(14)SZ6
CSCec15517		12.2(14)SZ4
CSCec21525		12.2(14)SZ4
CSCec22970		12.2(14)SZ4
CSCec28094		12.2(14)SZ4
CSCec28416	12.2(14)SZ4	
CSCec32091		12.2(14)SZ4
CSCec34830		12.2(14)SZ4
CSCec39258		12.2(14)SZ4
CSCec39281	12.2(14)SZ4	
CSCec40097	12.2(14)SZ4	
CSCec40175		12.2(14)SZ6
CSCec42467		12.2(14)SZ4
CSCec43129		12.2(14)SZ4
CSCec43308		12.2(14)SZ4
CSCec43621		12.2(14)SZ4
CSCec43772		12.2(14)SZ4
CSCec45767		12.2(14)SZ4
CSCec49575		12.2(14)SZ4
CSCec50743	12.2(14)SZ4	
CSCec52267		12.2(14)SZ4
CSCec52747		12.2(14)SZ4
CSCec56992		12.2(14)SZ6

Table 12 Caveats Reference for Cisco IOS Release 12.2 SZ (continued)

CSCec61844		12.2(14)SZ4
CSCec62366	12.2(14)SZ4	
CSCec64603		12.2(14)SZ5
CSCec69068		12.2(14)SZ5
CSCec74504		12.2(14)SZ6
CSCec75000		12.2(14)SZ5
CSCec77695		12.2(14)SZ5
CSCec78738		12.2(14)SZ6
CSCec79129		12.2(14)SZ5
CSCec83116		12.2(14)SZ5
CSCed00323		12.2(14)SZ6
CSCed05394		12.2(14)SZ6
CSCed10406		12.2(14)SZ6
CSCed11124		12.2(14)SZ6
CSCed26141		12.2(14)SZ6
CSCed27956		12.2(14)SZ6
CSCed38527		12.2(14)SZ6
CSCin22321	12.2(14)SZ4	
CSCin24908		12.2(14)SZ2
CSCin38900	12.2(14)SZ3	
CSCin40963	12.2(14)SZ	
CSCin42139		12.2(14)SZ2
CSCin42149	12.2(14)SZ	
CSCin42252		12.2(14)SZ2
CSCin42622		12.2(14)SZ2
CSCin43420		12.2(14)SZ2
CSCin43504		12.2(14)SZ2
CSCin44157		12.2(14)SZ2
CSCin44279	12.2(14)SZ2	
CSCin44998		12.2(14)SZ2
CSCin45661		12.2(14)SZ2
CSCin45721		12.2(14)SZ2
CSCin45747		12.2(14)SZ3
CSCin53739	12.2(14)SZ4	
CSCin45756	12.2(14)SZ2	
CSCin45957		12.2(14)SZ2

Open Caveats—Cisco IOS Release 12.2(14)SZ6

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(14)SZ6.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ6

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec14882

  When a PA-A3-XXX port adaptor is used in a c7304 PA-CC and RBE is configured on the interface, the source MAC address sent to the peer is 0000.0000.0000.

  Workaround: Configure a manual MAC address using the **mac address** interface command.

- CSCec40175

  Router unexpectedly reloads at bootup when more than 2000 VCs are configured on a PA-A3-8T1IMA/PA-A3-8E1IMA. A running router may also crash when more than 2000 VCs are created in quick succession.

  This problem is observed on a Cisco 7304 that runs Cisco IOS Release 12.2S and is configured with a Network Processing Engine G-100 (NPE-G100), a 7300-CC-PA carrier card, and a PA-A3-8T1IMA/PA-A3-8E1IMA.

  There are no known workarounds.

- CSCec56992

  The Parallel Express Forwarding (PXF) processor of a Network Service Engine (NSE100) on a Cisco 7304 may display corrupted error message.

  This problem is observed during HA switchover.

  There are no known workarounds.

- CSCec74504

  PA-A3-8T1IMA/PA-A3-8E1IMA interfaces do not come up at bootup.

  This problem is observed on a Cisco 7304 that runs Cisco IOS Release 12.2S and is configured with a Network Processing Engine G-100 (NPE-G100), a 7300-CC-PA carrier card, and a PA-A3-8T1IMA/PA-A3-8E1IMA. It is only seen when startup-config's section for IMA PA is more than 20 lines.

  Workaround: hw-module slot slot# stop|start is required to bring the interface up.

- CSCec78738

  The show int atm 5/0 packet statistics update very slowly.

  This problem occurs on an ATM PA card installed in Globemaster.

  There are no known workarounds.

- CSCec83116

  This caveat consists of three symptoms and contains a workaround for each symptom:

  Symptom 1: A Cisco 7304 may reload unexpectedly when you remove and re-add one or more service policies.

  This symptom is observed when you apply quality of service (QoS) policies to both physical interfaces and subinterfaces on the same port by entering the **service-policy** interface configuration command, you reload the router, and you remove and re-add one or more service policies.

  Workaround: Boot up the router without the service policies applied to the physical interface. Then, apply the service policies to the physical interface. Note that the symptom does not occur when you apply service policies to subinterfaces only, you reload the router, and you remove and re-add one or more service policies.

  Symptom 2: A Cisco 7304 may reload unexpectedly when you apply a service policy to a permanent virtual circuit (PVC).

  This symptom is observed when you first apply the service policy to an ATM subinterface, remove the service policy from the ATM subinterface, and then apply the service policy to a PVC.

  Workaround: Do not apply the service policy to the ATM subinterface: this configuration is not supported. You may apply the service policy to the PVC.

  Symptom 3: A Cisco 7304 may reload unexpectedly when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an ATM interface.

  This symptom is observed when you first attach a service policy to a subinterface of the ATM main interface and then enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration on the main interface.

  Workaround: Do not apply the service policy to the ATM subinterface: this configuration is not supported.

- CSCed00323

  When input traffic are process switched through BVI or Tunnel interface, BVI/Tunnel interface input queue may become wedged.

  This problem occurs on NSE-100 forwarding engine only.

  There are no known workarounds.

- CSCed05394

  A Cisco7304 router may display incorrect input rate and input packet counters.

  This problem is observed an a Cisco7304 router that is running Cisco IOS release 12.2(14)SZ4. The incorrect counters were observed on the NSE GigEthernet Ports.

  There are no known workarounds.

- CSCed10406

  When input features such as iACL is configured on an inteface, incoming packet that are switched through a tunnel interface are not properly encapsulated and transmitted.

  There are no known workarounds.

- CSCed11124

  A low-bandwidth class may be allocated more than its share of bandwidth, at the expense of a high-bandwidth class.

  This problem is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100) when the ratio of the configured bandwidths between two data classes is rather high (8:1 or higher) and when there is a priority class that receives traffic at least 20 percent of the line rate. The traffic that is received by the data classes should be in the ratio of the configured bandwidths.

  There are no known workarounds.

- CSCed13668

  A Cisco 7304 input policing may get in-accurate policing rate and the byte count of “show pol int” input policy may be off.

  If the packet is coming from Link side (LCs), the ingress link header (8 bytes) and real packet length will be counted in the input policing.

  There are no known workarounds.

- CSCed26141

  The service provider “p” image of the Cisco 7304 router does have the support for Cisco-Syslog-MIB.

  This problem occurs with regular usage of the service provider “p” image.

  Workaround: Please use the enterprise “js” image if the support for Cisco-Syslog-MIB is required.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

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

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

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

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Open Caveats—Cisco IOS Release 12.2(14)SZ5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(14)SZ5.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb07170

  BGP prefixes whose table id is more than 255 would not be resolved and installed into the mpls forwarding table.

  The VRF table number of the BGP prefix should be more than 255 in order to see this problem.

  There are no known workarounds.

- CSCec64603

  You will not be able to receive multicast packets on any ethernet port adaptor after issues a “hw-module slot x stop” and “hw-module slot x start”. Similar behavior is also noticed if the carrier card (7300-CC-PA) is OIR.

  This problem is observed on a Cisco 7304 that runs IOS Release 12.2S or 12.3T and that is configured with a NPE-G100 and 7300-PA-CC carrier card.

  Workaround: Reload the router if an OIR is require.

- CSCec69068

  After reload, the following commands are lost from the POS configuration:

  ```
  crc 32
  pos scramble-atm
  ```

  Machine affected: c7300-NSE

  There are no known workarounds.

- CSCec75000

  On the NPE-G100 the native GE-GE (GE ports on the engine) no drop packet switching performance is lower than expected. The linecard to linecard switching performance is not affected.

  There are no known workarounds.

- CSCec77695

  On Cisco Internet router c7300 employing NSE100 forwarding engine, IOBUS timeouts detected by the system controller do not get logged as such explicitly. One can determine that software forced crash was due to an IOBUS timeout by decoding the System Controller register dump.

  There are no known workarounds.

- CSCec79129

  The QoS function of interface on Cisco 7304 may not work after OIR the line card.

  This problem occurs when Configuring the QoS features on the interface and OIR the line card.

  Workaround: re-apply the QoS service policy.

Open Caveats—Cisco IOS Release 12.2(14)SZ4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb54391

  A Network Service Engine 100 (NSE-100) that is installed in a Cisco 7304 may reload unexpectedly.

  This problem is occurs when attempting to apply a quality of service (QoS) service policy to an unspecified bit rate (UBR) ATM virtual circuit (VC) by using modular QoS CLI (MQC). The following is an example of such an attempt:

  ```
  class-map match-any prec2
    match ip precedence 2
  class-map match-any prec3
    match ip precedence 3
  policy-map cc
    class prec2
     bandwidth 5000
    class prec3
     bandwidth 2000
  !
  interface ATM5/0
   no ip address
   pvc 0/200
    service-policy output cc
  ```

  This problem does not occur in Cisco IOS Release 12.2(20)S.

  There are no known workarounds.

Note The fix for this caveat prevents the router from reloading unexpectedly but still does not allow a QoS service policy to be applied to an UBR ATM VC by using MQC because the VC does not have any implied bandwidth.

- CSCeb82658

  The Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may reload unexpectedly.

  This problem is observed on a Cisco 7304 when a Reverse Path Forwarding (RPF) configuration is applied to an interface.

  Workaround: First shut down the interface and then apply the RPF configuration.

- CSCeb82722

  With arp'able interface, if the source route ARP is not resolved, PXF will drop the packet as RPF drops.

  Workaround. Triggering the ARP for source route either by ping or data packets will fix this problem.

- CSCec28416

  Under some conditions, an NSE-100 provides traffic streams with more equal bandwidths than are configured. The low bandwidth class is permitted more than its configured bandwidth, at the expense of the high bandwidth class.

  Several classes are configured, including at least one **priority** class and at least two **bandwidth** classes with substantially different bandwidth values. There is traffic on the priority class, the low bandwidth class offers more than its configured bandwidth, and the high bandwidth class offers most of or more than its configured bandwidth. In total, the interface is congested.

  There are no known workarounds.

- CSCec50743

  A Cisco 7304 may reload unexpectedly after a high availability (HA) switchover has occurred.

  This problem is occurs when the router is configured with 255 point-to-multipoint permanent virtual circuits (PVCs).

  There are no known workarounds.

- CSCec62366

  When the router is left at the --MORE-- prompt during a **show policy interface** on a 7304-NSE100 router, one or more of the following problems may occur:

  - Failure in SNMP pols
  - BGP sessions going down
  - Failure in telnet sessions

  This problem only occurs with the **show policy interface** command and only when left at the ---MORE--- prompt.

  Workaround: Set term length to 0.

- CSCin22321

  If the netConfigSet and hostConfigSet variables of the OLD-CISCO-SYS-MIB MIB are set, the corresponding commands may not be executed, and the following error messages and tracebacks may be generated:

```
%SYS-4-SNMP_NETCONFIGSET: SNMP netConfigSet request.
Loading configuration from 10.10.10.10

%SYS-3-TIMERNEG: Cannot start timer (0x545E1928) with negative offset (-1).
-Process= "SNMP ENGINE", ipl= 6, pid= 143
-Traceback= 502308BC 5022E3F8 50233358 501B0A24 501B298C 501C3618 501C3800
50259C00 50255290 5024F444 502574BC 502576FC 5017C4F4 508EBE04 508EBBBC
508D4D8C

%PARSER-4-BADCFG: Unexpected end of configuration file.
```

  This problem is platform independent.

  There are no known workarounds.

- CSCin53739

  When you enter the **show ip cache verbose flow** EXEC command on a Cisco 7304, the output of the command does not display the source interface, and the router may reload unexpectedly.

  This problem is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(18)S and that is configured with a Network Service Engine 100 (NSE-100) when NetFlow accounting is enabled on the Parallel Express Forwarding (PXF) processor of the NSE-100.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb66639

  The Gigabit Ethernet ports on a Network Processing Engine G-100 (NPE- G100) may not respond.

  This problem is observed intermittently on a Cisco 7304 when the Gigabit Interface Converter (GBIC) media type is selected.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ports.

- CSCec02503

  A spurious PPLM alarm is raised on POS OC12 and POS OC48 linecard of a Cisco 7304 router.

  When there is an outage in the SDH or SONET network, the PAIS and PPLM alarms are raised. However, when the outage has been restored, the PAIS alarm is correctly cleared but the linecard continues to report PPLM alarm.

  Workaround: Use interface configuration command **pos flag c2** to set the correct c2 value again to clear the PPLM alarm.

- CSCec11736

  When using **shape** on an NSE-100, the shaping may allow up to 10% too much traffic on the class.

  There are no known workarounds.

- CSCec14245

  The number of packets input, and the number of bytes input on the C7300 NSE-100 GE interface may occasionally decrement.

  When doing subsequent show interface commands on the NSE-100 native GE ports, the number of input packets and/or bytes could be less on the second invocation than they were on the first (i.e., input packets/bytes counters appear to decrement with time).

  This problem is most likely to be noticed with light traffic conditions and the reception of packets that are dropped due to MAC filtering.

  There are no known workarounds.

- CSCec14424

  High CPU utilization may occur on the Route Processor (RP) of a Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100).

  This problem is observed on a Cisco 7304 that is configured for tag switching when any of the following protocols or features are also configured:

  - Tag Distribution Protocol (TDP)
  - Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)
  - VPN Routing/Forwarding Lite (VRF Lite)
  - MPLS-traffic engineering (MPLS-TE)

  There are no known workarounds.

- CSCec15517

  A router may reload when the **show policy-map interface** EXEC command is issued.

  It is unclear at this time what conditions must exist to trigger this problem. A preliminary review indicates that the problem may exist in the **show policy-map interface** code when a Frame Relay (FR) permanent virtual circuit (PVC) policy is shown.

  There are no known workarounds.

- CSCec21525

  A PXF reload may occur with the c7304 router and the NSE-100 processing engine. The reload occurs with Ethernet interfaces (of any speed) configured with 802.1q VLANS.

  This problem does not occur with the native Gigabit Ethernet ports on the NSE-100 processing engine.

  Workaround: Use the native Gigabit Ethernet ports for the VLAN configuration.

- CSCec22970

  When the **negotiation auto** command is enabled, the Gigabit Ethernet port link is up and down between the Cisco 7301 router and the network processing engine-G1 (NPE-G1).

  This problem is observed on a Cisco 7301 router but is platform independent.

  Workaround: Enter the **no negotiation auto** command on the interface of each router.

- CSCec28094

  A Cisco 7304 that is configured to reboot automatically may not do so.

  This problem is observed on a Cisco 7304 that is configured with a Network Processing Engine G-100 (NPE-G100) and occurs when the router goes down after a fatal exception.

  Workaround: Power-cycle the router.

  Alternate Workaround: Send a break signal via the console connection to the NPE-G100 while the NPE-G100 is in the process of rebooting automatically. Then, from ROM monitor (ROMmon) mode, reset the router.

- CSCec32091

  Classed based WRED under hierarchal policy-map quits working each time the router is reloaded. Most of the traffic being dropped under the class.

  This problem is observed on a 7300 with a NSE100 running 12.2(18)s.

  Workaround: Remove and re-configure the service-policy under the interface.

- CSCec34830

  The Parallel Express Forwarding (PXF) processor of a Cisco 7304 may pause indefinitely or reload unexpectedly.

  This problem is observed when a Multiprotocol Label Switching (MPLS) packet is received on a generic routing encapsulation (GRE) tunnel that is configured on the Cisco 7304.

  There are no known workarounds.

- CSCec39258

  After executing “hw-module stop” and “hw-module start”, E1/T1 IMA PA will not pass traffic.

  This problem occurs in the following:

  - E1/T1 IMA PA
  - PA-CC, NPE-G100
  - c7304 12.3T images
  - c7304 12.2S images.

  Workaround: Reload the router.

- CSCec39281

  Queueing stats is zero.

  This problem occurs when shaping is configured in a class.

  There are no known workarounds.

- CSCec40097

  Sometimes PXF tail drop counter increased slowly during full duplex 64-byte GigE traffic

  This problem occurs during full duplex wire speed traffic.

  There are no known workarounds.

- CSCec42467

  The following message appears after no shut and cannot be ping:

  ```
  "
  %LINK-3-UPDOWN: Interface xxxxxx, changed state to down,
  "
  ```

  This problem occurs when OIR (physical, or logical with “hw-module slot <x> start” is follow by shut/no shut on interface.

  Workaround: If the interface is not shut in the running config, a repeat of the OIR (physical or logical) will bring the interface back up.

- CSCec43129

  A Cisco 7304 may pause indefinitely or reload unexpectedly while processing statistics packets from the Parallel Express Forwarding (PXF) processor. When the PXF processor processes quality of service (QoS) traffic, the PXF processor sends these statistics packets to the Route Processor (RP).

  Even if the Cisco 7304 does not pause indefinitely or reload unexpectedly, the QoS statistics from different interfaces or classes, or from both, may become mixed up in such a way that there are no QoS statistics for a class, or traffic from one class on an interface is reported as coming from a different class.

  The output of the **show policy-map interface** EXEC command displays the QoS statistics, which are also accessible through the CISCO-CLASS-BASED-QOS-MIB MIB.

  This problem is observed when you boot up the Cisco 7304 or when you make any QoS configuration changes while there are service policies attached to interfaces, subinterfaces, or ATM virtual circuits (VCs). The following commands change the QoS configuration:

  - class-map

  - match

  - policy-map

  - class

  - set

  - police

  - bandwidth

  - priority

  - random-detect

  - shape

  - queue-limit

  - access-list

Note The **access-list** global configuration command is relevant only if the access control list (ACL) that is stated in the command is referred to by at least one **match access-group** class-map configuration command.

Workaround: Reload the Cisco 7304 without any service policy applied to any interface, subinterface, or ATM VC. When the Cisco 7304 has booted up, manually apply the service policies to the interfaces, subinterfaces, or ATM VCs.

Before you change any QoS configuration (as described in the conditions), detach all service policies from the interfaces, subinterfaces, or ATM VCs. Then, make the necessary changes and reattach the service policies.

- CSCec43308

  The **ip default-network** global configuration command may be ignored by the Parallel Express Forwarding (PXF) processor, causing packets that do not have a route specified to be dropped instead of being forwarded to the default network.

  This problem is observed on a Cisco 7304 that is configured with a Network Service Engine 100 (NSE-100).

  Workaround: Disable the PXF processor by entering the **no ip pxf** global configuration command.

- CSCec43621

  Very long boot up time (hours).

  This problem occurs when a system with many interfaces is configured with MQC.

  There are no known workarounds.

- CSCec43772

  When a large number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets is received, the input-queue counters of an interface may slowly increase, eventually causing the interface to become wedged.

  This problem is observed on a Cisco router that runs Cisco IOS Release 12.2(14)SZ3 or Release 12.2(18).

  Workaround: Reload the router.

- CSCec45767

  On a Cisco IOS router running BGP and PIM with multicast routing enabled and MBGP configured on BGP, some of the default rpf lookups and sh ip rpf <prefix> command fails for MBGP routes.

  There are no known workarounds.

- CSCec49575

  After congestion occurs, ATM per VC queue may stay congested for a while.

  This problem only occurs on an NPE-G100 forwarding engine.

  There are no known workarounds.

- CSCec52267

  The Parallel Express Forwarding (PXF) processor of a Network Service Engine 100 (NSE-100) may crash when switching the forwarding from IP to MPLS path.

  This condition is observed when traffic is being forwarded and BGP or any other routing protocol peer goes down forcing the path to change from IP to MPLS. There must be two paths for forwarding to destination, one IP and second MPLS.

  Workaround: Make sure primary and backup path are either IP or MPLS.

- CSCec52747

  Bursts of traffic set to an egress LLQ may have four or more data packets interleaved on the link. The condition will arise only when total egress traffic on the link approaches line rate. The issue does not affect the NSE-100's local GE interfaces.

  There are no known workarounds.

- CSCec61844

  A Cisco 7304 may reload unexpectedly when you perform an online insertion and removal (OIR) of an ATM line card or ATM port adapter.

  This problem is observed on a Cisco 7304 that is configured with a Network Processing Engine G-100 (NPE-G100) when the router processes traffic.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(14)SZ3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb72681

  On an NSE-100, when a burst of data at a high packet rate is presented for policing on a class, much more than the correct burst size might be allowed through before drops occur.

  For example, if the police rate is 500Mbps, the burst size is defaulted (0.25 seconds of data), and 10% overload is offered, all data should be allowed through for 2.5 seconds. But more than 3 seconds were observed.

  There are no known workarounds.

- CSCin38900

  On an NSE-100, a CE1 egress interface may be under utilized when shaping is configured in the policy.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy87741

  Transition of group mode from Sparse to Bidir and Bidir to Sparse does not change the existing mroute entries on a router even though it gets the new auto-rp mappings. This is 100% reproducible.

  This defect is platform independent.

  Workaround: Use the **clear ip mroute *** command.

- CSCdz69173

  When you use the command **show diag *slot*** on a c7300 router with a 7300-CC-PA Port Adapter Carrier Card in the specified slot, the port adapter status shows “Port adapter is analyzed” instead of “Port adapter is active”.

  The associated SNMP cardOperStatus has a value of “down” instead of “up”.

  There are no known workarounds.

- CSCdz70316

  When “show mpls l2transport vc summary” is performed on PE, AToM VC fails to come up.

  This problem occurs when re-enable mpls ip/mpls label protocol ldp on MPLS core interfaces on Cisco 7200 with 12.2(13.7)T2 -p-mz or -js-mz images.

  Workaround: Disable-re-enable “mpls ip” on MPLS core router configuration mode.

- CSCdz79023

  An ATM subinterface that is configured with switched virtual circuits (SVCs) may pause indefinitely and does not recover.

  This symptom is observed when the last dynamic virtual circuit (VC) is deleted from the interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCea26993

  Multicast traffic may get dropped by a Cisco router that is running in dense mode. (Note that all routers have the multicast group in a pruned state even though interested receivers are present.)

  This problem is observed when a T-flag is incorrectly set on an (S,G) entry.

  A process that is used by dense mode and that is called an Assert process (referred to as Assert) is triggered, causing a designated forwarder (referred to as an Assert winner) to be elected. The Assert winner forwards multicast traffic onto a multiaccess segment when there is more than one router on the segment. If the router that becomes the Assert winner has the T-flag incorrectly set because traffic arrives on its outgoing interface (OIF) rather than on its incoming interface (IIF), multicast traffic is dropped as a result of Reverse Path Forwarding (RPF).

  The Assert winner is based on the lowest administrative distance that is required to reach the source. When administrative distances are equal, the Interior Gateway Protocol (IGP) metric is used to determine how to reach the source. When both the administrative distance and the IGP metric are equal, the router with the highest IP address is used as a tiebreaker.

  Workaround: Disable Protocol Independent Multicast (PIM) on the interface of the Assert winner that has incorrectly set the T-flag on its (S,G) entry as a result of receiving traffic on its OIF rather than on its IIF.

  First Possible Alternate Workaround: Enter the **ip mroute** *source-address rpf-address distance* global configuration command with a value of 255 for the distance argument on the Assert winner.

  Second Possible Alternate Workaround: Configure the **ip pim sparse- mode** interface configuration command on the interface of the Assert winner to prevent the interface from operating

- CSCea58795

  BGP VPN tags not released to free available pool of tags in the router when such a prefix that had local label assigned has now been withdrawn. When this happens with huge number of prefixes, router could eventually run out of available labels on the box.

  On a PE router that has VRF’s configured & BGP vpn allocated and freed local labels. Found with router using 122-16.9.S release.

  Workaround: Increase/configure larger label range.

- CSCea72684

  On a Cisco7300 “show memory summary” shows that NAT holds memory even though its not configured on the box.One would see the following snip when performing “show memory summary”:

```
 Address      Bytes     Prev     Next Ref   Alloc Proc     Alloc PC  What
436CDE94 0000131072 436BDE68 436EDEC0 001  *Init*          400734FC  PXF NAT local
hash tbl
436EDEC0 0000131072 436CDE94 4370DEEC 001  *Init*          40073510  PXF NAT global
hash tbl
4372DF18 0002359296 4370DEEC 4396DF44 001  *Init*          40073544  PXF NAT entries
table
4396DF44 0001835120 4372DF18 43B2DFE0 001  *Init*          400735B8  PXF NAT hash
entries chunks
43B2DFE0 0007471188 4396DF44 4424E060 001  *Init*          400735DC  PXF NAT fib
chunks
4424E060 0000065536 43B2DFE0 4425E08C 001  *Init*          40073604  PXF NAT API
chunks
***
```

  There are no known workarounds.

- CSCea73517

  When the software OIR sequence is invoked by issuing the command sequence **hw-module slot *x* stop**, **hw-module slot *x* start**, the Port Adapter Carrier Card with a PA-MC-8T1 Port Adapter may not come up if traffic is running.

  This problem occurs if there are packets being transmitted or received on the interface during this operation.

  Workaround: Disable traffic to the interface before performing the operation.

- CSCea80009

  When a router receives a Register message for a dense group it decapsulates the packets and sends it out on its Olist and does not send a Register stop.This cause the DR to be stuck in Registering state and to keep sending Registers.

  There are no known workarounds.

- CSCea87242

  This is one case of CSCea26993 which has not been fixed.

  The T flag is set on the s, g on routers directly connected to source, even for non-RPF traffic. This might lead to blackholing of traffic for the case mentioned in CSCea26993

  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 min. for 100K prefixes.

  The above 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.

- CSCeb20619

  Ping fails after applying dynamic tunnel.

  The problem is observed when dynamic tunnel is configured.

  There are no known workarounds.

- 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.

- CSCeb34069

  Under load, some packets to a congested link may be dropped even though the class they belong to is within CIR.

  There are no known workarounds.

- CSCeb43106

  On an NSE-100 with a queueing policy configured on a native Gigabit Ethernet port, no allowance is made by the queueing logic for the 20 byte framing overheads (12B minimum gap + 8B preamble).

  This can result in arbitrary drops and high latency for both priority and non-priority traffic.

  Workaround: Configure hierarchical shaping on the interface, with a shape rate of 900Mbps. That assumes an average packet size of 200 bytes. This workaround should be removed when an a corrected image is loaded, otherwise the link will be under utilized.

- CSCeb44478

  When a Port Adapter Carrier Card (PACC) contains a channelized PA, and the PACC is OIR'd, the controllers are not removed. They still appear in the running-config.

  This only afflicts Channelized Port Adapters.

  Workaround: Power down the router and remove the PA.

- CSCeb51226

  PXF forwarding fails with channelized Port Adapter interfaces. This can be observed with the **show pxf interface**, where all of the packets are punted to the RP.

  This only affects the NSE-100 processor card.

  There are no known workarounds.

- CSCeb56568

  If MTU is changed on GE interface of NSE100 installed in Cisco 7300, router stops to receive multicast packets. There is no problem with unicats and broadcasts.

  Routing protocols which use multicast packets to maintain adjacency (OSPF, ISIS) lost their neighbors over this GE interface, even if the configured MTU is a right one.

  Workaround: Use the **shutdown / no shutdown** command on the gigabit Ethernet interface.

- CSCeb58048

  After a hw-module stop/start command sequence, the channelized interfaces will punt traffic to the RP.

  This only affects systems with the NSE100 processor card.

  Workaround: Configure ip route-cache cef on the interfaces.

- CSCeb59610

  Ingress label accounting per interface missing in PXF path.

  There are no known workarounds.

- CSCin45747

  Traceback occurs at process_enqueue in 7304 router while configuring the command **ip pim sparse-dense-mode** in the interface configure mode.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(14)SZ2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu53656

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

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

- CSCdz71127

  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

- 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

- CSCea28131

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

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

- CSCeb01188

  When a policy-map have NBAR classification is applied to the Fast Ethernet interface of a PA contained in the Port Adapter Carrier Card, the NBAR classification may fail.

  This problem occurs when the c7300 switching engine is the NPE-G100.

  There are no known workaround.

- CSCeb01192

  When there is a broad range of class bandwidths in a queueing policy, and the high bandwidth class is underloaded, the link utilization can be poor.

  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 min. for 100K prefixes.

  The above 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.

- CSCeb19110

  On an NSE-100, when LLQ is enabled on an ATM PVC, and priority + non-priority traffic is sent, all priority packets get through, but more non-priority traffic than necessary get dropped. Hence the traffic never reaches line rate.

  There are no known workarounds.

- CSCeb22302

  When using hierarchical policy-maps, **police** is NOT supported on the parent policy-map. Currently, such configuration is erroneously accepted.

  This problem occurs on the c7304 NSE-100 board, 12.2S releases.

  Workaround: Use the **shape** command on the parent policy-map.

- CSCeb39237

  On a c7304 system with an NSE-100 service engine running 12.2(14)SZ2 version of the IOS software, command **show ip cache [verbose] flow** does not show source interface, command **show ip cache verbose flow** does not show correct mask/AS/nexthop information. A trace back is also seen when the **show ip cache [verbose] flow** is entered.

  This problem is observed when netflow accounting is enabled in the PXF processor on the NSE-100.

There are no known workarounds.

- CSCin44279

  Had PA-MC-2T3+ configured back to back. Configured a few T1 controllers and the corresponding serial interfaces. Back to back pings were successful. Later, removed the configurations and configured the card as unchannelized i.e. “no channelized” initially and configured to “channelized” again. On configuring the channelized serial interfaces again, found that the back to back pings were unsuccessful.

  There are no known workarounds.

- CSCin45756

  When using a Switched Virtual Circuits (SVC) configuration with the ATM Port Adapter in the Port Adapter Carrier Card, the SVC may not come up after it times out. The ATM subinterface goes down.

  Pinging the SVC will not bring the SVC up, since the subinterface is down.

  Workaround: Issue a **no shut** command on the ATM subinterface.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx95364

  When a NPE-G1 GigabitEthernet interface is configured for “no negotiation auto” and the link partner is in the shutdown (or not connected) state the interface will flap repeatedly with the following message

  ```
  01:19:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed
  state to up
  01:19:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed
  state to down
  ```

  Workaround: Configure the GigabitEthernet interface on the NPE-G1 to use “negotiation auto” mode.

- 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, i.e., 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.

- CSCdz85927

  A Cisco 7300 series router running IOS 12.1.EX may experience assertion failures and a link flap when a subinterface is added to the gigabit ethernet port. The log will show something like this:

  ```
  %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
  up Assertion failure in ../toaster/ws-rp/ws_rp_mpls.c (954)
  ```

  The link will go down temporarily and then come back after a few moments.

  There are no known workarounds.

- CSCea29514

  Router's console log can be shown on PC through Aux port on NPE-G1. If configuration is changed, Aux port doesn't work. If the same procedure is done on I/O board, AUX port works normally.

  This occurs under the following:

  ```
  PC -- [ rollover cable for console ] -> AUX:NPE-G1
  ```

  The following configuration changes:

  ```
  Router(config)#line aux 0
  Router(config-line)#no stopbit 1
  Router(config-line)#stopbits 1
  ```

  There are no known workarounds.

- CSCea44928

  The standby NSE-100 will fail to become active due to a PXF exception when a switch-over is in progress and the standby is trying to become the primary NSE. The two NSE-100's will recover and the original primary NSE will become active again, without the switch-over having taken effect.

  The above symptom may be observed on a c7304 system with two NSE-100 services engines when a switchover is attempted with moderate to high traffic flowing through the system at the time of switch-over. This caveat is observed only in the c7304 releases based off 12.2S.

  There are no known workarounds.

- CSCea52106

  When Ethernet over MPLS is configured on the gigaethernet port of Cisco 7304 NPE-G100 board, it initially displays “Failed to set promiscuous mode” message and the connectivity is not there. It takes a while for the promiscuous mode to be set and the connectivity to be established.

  There are no known workarounds.

- CSCea55963

  An interface may flap when a service policy is attached to the interface.

  This problem has been observed on a c7304 with an NSE-100 services engine when a service policy is attached to an interface. Currently, this has only been observed on ethernet interfaces - the GigE interfaces on the NSE as well as the PA-2FE.

  There are no known workarounds.

- CSCea69676

  When a virtual template interface is applied to an ATM VC on a c7300 platform with a NPE-G100 service engine, and if this virtual template has PPP multilink configured, ingress packets for this ATM VC may be dropped. The reason for this problem is that ATM interface driver code for c7300 does not have the proper support for multilink-PPP.

  There are no known workarounds.

- CSCea78255

  When the line protocol flaps on any 7300 ATM interface (PA-A3, PA-A3-IMA, native ATM-OC3 line card) a message will be displayed indicating that a bad rewrite string was encountered.

  The message does not interfere with the normal operation of the interface.

  There are no known workarounds.

- CSCea83212

  When the Port Adapter Carrier Card is OIR with a PA-E3 inserted the PA-E3 does not boot up and remains disabled.

  Workaround: Issue the command sequence **hw-module slot** <*x*> **stop**, **hw-module slot** <*x*> **start**.

- CSCea83322

  After an online insertion (OIR) of the small-form-pluggable (SFP) GBIC in giga ethernet on the NPE-G100 board of the Cisco 7304 router, the first read to the GBIC’s EEPROM may fail causing the system to have incorrect information.

  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 a situation where you have to upgrade to an IOS image with new fpga firmware in a dual cpu card system, do 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

- CSCea86011

  When the remote link goes down the PA-GE transmit will lock up.

  Workaround: A shut/no shut of the interface is required.

- CSCea91831

  A crash may occur when reloading a c7300 platform with a NPE-G100 service engine that has a corrupted FPGA image.

  There are no known workarounds.

- CSCeb01067

  When a c7200 with later revisions of an NPE-G1 processor boots the user may see the following message:

  ```
  00:00:07: GigabitEthernet0/1: Unknown PHY revision (0xCC1)
  ```

  Workaround: The message is benign and the router will continue to function without problems. However there is no workaround to prevent this message from being printed.

- CSCeb01253

  Hierarchical policy does not work on NPE-G100 when parent policy is configured with traffic shaping while child policies have different bandwidths. Although the aggregated traffic is shaped correctly at the parent level, the child policies always get equal bandwidth; Weighted fair queueing does not apply. Also all drop rates and drop counters under “show policy interface” are zeros and drops are displayed under “show interface” output drops.

  There are no known workarounds.

- CSCeb05029

  On an NSE-100, if more than 8000 interfaces (including VCs) exist then packets may be sent to the wrong egress interface.

  There are no known workarounds.

- CSCeb08858

  Currently, CLI doesn't allow the class-based **shape average** target bit rate parameter to be higher than 154400000 bps.

  This happens on both NSE-100 and NPE-G100 boards.

  There are no known workarounds.

- CSCeb09322

  On an NSE-100, under load, using CBWFQ, on rare occasions an old packet is sent (again) instead of the correct one.

  There are no known workarounds.

- CSCeb21792

  When executing show c7300 command on a c7300 platform, it may display that all the line card FPGA images need to be updated although the FPGA versions on the line card boards are the same as the FPGA versions bundled with IOS image.

  There are no known workarounds.

- CSCeb26429

  At random times, PXF VTMS stops passing packets to an interface for half a second. Under load, this happens on average every 200 seconds.

  There are no known workarounds.

- CSCin24908

  The message RSP-3-RESTART is seen almost continuously for a channelized interface. (Note: no cbus-complex is seen).

  When trying to send large packet sizes at greater than line rate through a channelized interface continuously for a long period of time. (Note: This will not normally be seen on customer network).

  There are no known workarounds.

- CSCin42139

  After a large amount of traffic has been received on the PA-MC-CE3 interface, issuing of the **clear counters** command may cause a large number in input errors to appear on the interface.

  There are no known workarounds.

- CSCin42252

  When the **frame-relay map ip** command is configured on a Channelized Port Adapter interface, packets cannot be transmitted out of the virtual circuit.

  There are no known workarounds.

- CSCin42622

  On configuring the PA-MC-STM1 in the 7300-CC-PA, LINK-2-LINEST tracebacks from the “CEF Process” are seen at 15 second intervals. The PA continues to switch packets as expected.

  There are no known workarounds.

- CSCin43420

  Spurious access is seen every time a PVC is configured under a PA-A3-OC3 (sub) interface.

  There are no known workarounds.

- CSCin43504

  For all channelized PAs, packets get forwarded over the first serial interface only (first channel).

  Even packets that need to be forwarded over other serial interfaces, eventually get forwarded over the first serial interface.

  There are no known workarounds.

- CSCin44157

  Uni-directional traffic was generated by Ixia which was forwarded over all the 8 ports of the 8TE1+ link between “WstarReg” and “Router”. This traffic was then forwarded over the POS link between “Router” and “Central”. Traffic was generated be Ixia at 50000 pps with packet length being 64 bytes. The router “Router” crashed while the PA-MC-T3 was being replaced with PA-MC-2T3+.

  There are no known workarounds.

- CSCin44998

  Had PA-MC-2T3+ connected back to back. Channelized interfaces were configured on the first port (28 serial interfaces on port 0). Unchannelized interface was configured on port 1.

  On performing back to back ping for the unchannelized interface, it was observed that the far end received ping requests and sent ping replies over the first interface of port 0. The pings at the remote end infact, should have been received and sent on port 1.

  There are no known workarounds.

- CSCin45661

  When channelized Port-Adaptor on a 7500 platform is stressed with high traffic and high packet size the message “RSP-3-RESTART: <interface> not transmitting”.

  Workaround: This will only be seen on highly stressed links and should not be seen on production routers. A few drops may be dropped but otherwise normal operation should not be affected.

- CSCin45721

  The PACC with PA-A3-OC3 crashes when traffic above the line rate is passed.

  There are no known workarounds.

- CSCin45957

  A Router with NSE-100 crashes on removing the STM configurations.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(14)SZ1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(14)SZ1.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea76179

  The priority command does not accept kbps parameter.

  There are no known workarounds.

- CSCea83735

  When the GE on the NPE-G100 is configured with mtu greater than 1518, it is observed that, under heavy traffic conditions, the GE stops receiving packets. A shut/no shut on the GE port resumes packet reception.

  There are no known workarounds.

- CSCea87210

  There was a bug in the NPE-G100 software that skips the traffic shaping functionality.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(14)SZ

This section documents possible unexpected behavior by Cisco IOS Release 12.2(14)SZ and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz65342

  Traffic destined out an ATM interface or VC may not be classified as per the classification criteria in the attached output service policy.

  The above behavior may be observed on a c7304 system with an NSE-100 services engine if a service policy attached to an ATM interface or VC is repeatedly and quickly modified multiple times. Traffic does not appear to be dropped. This caveat only applies to the c7304 releases based off 12.2S.

  This problem is not easily reproducible. It could not be recreated on a Frame Relay VC.

  There are no known workarounds.

- CSCdz68002

  Packets sourced or switched out by the Route Processor are double accounted in the policy-map counters displayed via the **show policy interface <interface-type>** command.

  The above symptom is seen on a c7304 system with an NSE-100 services engine. On the NSE-100, all traffic goes through the PXF where all egress QoS features are applied. For RP sourced traffic, these packets are accounted a second time in PXF, resulting in the double accounting.

  There are no known workarounds. This is an accounting issue and there is no impact to any traffic processed/switched by the system.

- CSCdz69173

  When you use the command **show diag** ***slot*** on a c7300 router with a 7300-CC-PA Port Adapter Carrier Card in the specified slot, the port adapter status shows “Port adapter is analyzed” instead of “Port adapter is active”.

  The associated SNMP cardOperStatus has a value of “down” instead of “up”.

  There are no known workarounds.

- CSCea02012

  The **show atm vc** *vcd* command does not show the number of packets with CLP bit set.

  The above symptom is seen on a c7304 system configured with the OC3 ATM linecard. If a service policy with a **set atm clp** action is applied on the OC3 ATM LineCard interface, the packets that have the CLP bit set will not be accounted for in the **show atm vc** *vcd* command output. This caveat does not exist when using an ATM Port Adapter such as the PA-A3-E3, PA-A3-T3, PA-A3-OC3.

  Workaround: One way to see the number of packets that are marked with CLP is to use the **show policy interface** *int* command.

- CSCea33447

  Priority queue packets may be dropped when the offered traffic load to the link with the priority queue is above link bandwidth.

  The above behavior may be seen on a c7304 with an NSE-100 services engine configured with an output service policy that has an absolute priority queue plus multiple other classes and the offered load on the output link is excessive.

  There are no known workarounds.

- CSCea44185

  The bandwidth and shape commands in an output service policy may not be effective. Excess, unused bandwidth may not be distributed the way it should be.

  The above symptoms may be observed on a 7304 with an NSE-100 services engine when an output service policy is detached from and reattached to a port when that port is congested with egress traffic. Multiple detach and reattach operations may be required to trigger the symptom. This caveat is relevant only to the 12.2S based releases for the c7304, such as 12.2(11)YZ1 and 12.2(14)SZ.

  Workaround: The only known workarounds to recover from such a problem are to either physically remove and reinsert (OIR) the line card affected, or perform a software OIR via the **hardware module {stop|start}** commands. To avoid the problem, ensure that the port is not congested with egress traffic when reattaching the output service policy, or shutdown the port while making the configuration change.

- CSCea44928

  The standby NSE-100 will fail to become active due to a PXF exception when a switch-over is in progress and the standby is trying to become the primary NSE. The two NSE-100's will recover and the original primary NSE will become active again, without the switch-over having taken effect.

  The above symptom may be observed on a c7304 system with two NSE-100 services engines when a switchover is attempted with moderate to high traffic flowing through the system at the time of switch-over. This caveat is observed only in the c7304 releases based off 12.2S.

  There are no known workarounds.

- CSCea50565

  The packet accounting data shown in the **show mpls forwarding-table** command output may be lagging by several minutes.

  The above behavior may be seen on a c7304 system with an NSE-100 services engine configured for MPLS forwarding by the PXF processor.

  There are no known workarounds. This is a cosmetic display issue with retrieving accounting data from the PXF processor.

- CSCea51753

  Unused bandwidth may be wasted and not available for class queues that could use them. This could manifest itself as lower utilization of a link.

  The above symptom may be seen on a c7304 with an NSE-100 services engine configured for class based QoS on any link. Under certain configuration scenarios where a class queue being shaped gets a committed information rate equal to the shaped rated, the class queue may also automatically get default EIR that is never utilized due to the shaping. The unused EIR is wasted and not available to the other class queues.

  An example configuration is as follows:

```
policy-map test
  class class1
   bandwidth percent 30
  class class2
   shape average 30000000
```

  The 70% CIR not explicitly assigned is divided between Class2 and Class-Default, with class2 getting a CIR of 30Mb equal to its MIR. However, class2 also gets EIR by default in proportion to it's CIR.

  Workaround: Explicitly configure the allocation of EIR via the **bandwidth remaining percent** class command.

- CSCea55174

  Non-priority queues on a port or VC may see excessive packet queue tail drops.

  The above behavior may be observed on a c7304 system with an NSE-100 services engine when a port or VC is configured with an absolute or strict priority queue. This caveat applies only to the c7304 releases based off 12.2S.

  When an absolute priority queue is configured, it continues to get most of the EIR. As a result, the non-priority queues do not get their proper share of any unused bandwidth and end up overflowing, dropping packets.

  Workaround: One known workaround is to configure a **police** command on the priority queue to no longer make it a strict priority queue. If the priority queue has to be guaranteed all link bandwidth, then the police rate may be as high as 95% of link bandwidth.

- CSCea55963

  An interface may flap when a service policy is attached to the interface.

  The above symptom has been observed on a c7304 with an NSE-100 services engine when a service policy is attached to an interface. Currently, this has only been observed on ethernet interfaces - the GigE interfaces on the NSE as well as the PA-2FE.

  There are no known workarounds.

- CSCea62901

  RPF will not work on VRF-Select enabled interface of a c7304 with an NSE-100 services engine.

  There are no known workarounds.

- CSCea62933

  Enabling VRF-Select on a netflow enabled interface of a c7304 with an NSE-100 services engine will result in incomplete netflow accounting data. The source and destination AS (autonomous system) will not be available in this case. This is because the lookups to obtain the AS will fail due to use of an incorrect VRF index.

  There are no known workarounds.

- CSCea63068

  The message **ATOM_TRANS: VC id is already in used** may be seen when configuring a VC ID on a 802.1Q VLAN subinterface through the **mpls l2transport route** subinterface configuration command.

  The above symptom is seen on a c7200 or c7304 system when an ethernet type PA (PA-GE, PA-2FE, etc) configured for mpls l2transport is OIRed and replaced by a different ethernet type PA. The **mpls l2transport** command should be reconfigured on the new PA with the same VC ID configured earlier on the removed PA, without explicitly deconfiguring that PA before its removal.

  Removal of a PA is not automatically releasing the VC IDs configured on that PA via the **mpls l2transport** subinterface configuration commands.

  Workaround: Before removing the Port Adaptor, deconfigure all l2transport VCs configured on it.

- CSCea65807

  ICMP pings through an MPLS cloud to the loopback address of a Provider Edge router configured with **mpls ldp explicit-null** will fail. ICMP pings through the PE router are not affected.

  The above behavior may be observed on a c7304 with an NSE-100 services engine configured as an MPLS PE router. Through traffic is not affected. ICMP pings initiated from this PE router configured for explicit-null are not affected either.

  There are no known workarounds.

- CSCea66777

  Changes to the shape rate for any class queue in an output service policy may not take effect immediately while there is a sufficiently high rate of egress traffic on the link with that service policy.

  The above behavior may be observed on a c7304 with an NSE-100 services engine.

  Changes to the shape rate do not take effect until the class queue has drained out and has had a chance to get deactivated.

  There are no known workarounds. The new shape rate will ultimately take effect when the egress traffic rate goes below some level that's sufficient to cause the class queue to drain out and become empty for a short interval.

- CSCea68333

  No accounting information may be shown in the **show policy interface** command output.

  The above symptom may be observed on a c7304 with an NSE-100 services engine when a service policy that has no class actions is configured. The following is an example of such a policy:

```
policy-map capture
  class prec0
  class prec1
  class prec2
  class prec3
  class prec4
  class prec5
  class prec6
  class prec7
```

  This is purely an accounting issue. Traffic will still get classified as per the match criteria for each class. A QoS action in any class is required to trigger the accounting.

  Workaround: Configure at least one action in any of the classes.

- CSCea76179

  The priority command does not accept kbps parameter.

  There are no known workarounds.

- CSCea82081

  An LDP session may not be reestablished after disabling and enabling MPLS. This may result in the VC for transporting an 802.1Q VLAN over MPLS not coming up.

  The above behavior may be seen when ethernet 802.1Q VLAN over MPLS is configured via the **mpls l2transport** subinterface configuration command and MPLS is disabled and then enabled again.

  Workaround: Remove and reconfigure the **mpls l2transport** subinterface configuration command after MPLS has been re-enabled.

- CSCea83735

  When the GE on the NPE-G100 is configured with mtu greater than 1518, it is observed that, under heavy traffic conditions, the GE stops receiving packets. A shut/no shut on the GE port resumes packet reception.

  There are no known workarounds.

- CSCin40963

  On a few occasion, the following traceback messages were received while passing traffic or when the interface goes down:

  ```
  Cannot get buffer to copy received IPC packet
  ```

  This is not easily reproducible.

  There are no known workarounds.

- CSCin42149

  Removing the LDP configuration before the EoMPLS configuration may cause the c7300 router to crash. The crash may be seen on entering the **no mpls l2transport route** command.

  This problem occurs when the router is configured for EoMPLS.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(14)SZ

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(14)SZ. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

  The above symptom may be observed on a c7300 with an NSE-100 services engine.

  There are no known workarounds.

- CSCdz63669

  DMA error message and loss of certain packets. The DMA error is reported by an on-board ASIC called VAN ALLEN.

  The above symptoms may be seen on a c7300 system with an NSE-100 services engine if there are ingress packets on any of the GigE ports with frame size greater than 1485 bytes. This is true even if the port MTU is increased beyond the default of 1500 bytes.

  For GigE ingress packets greater than 1485 bytes, the hardware sets a specific bit in the packet context fed to the PXF processor. This bit is reused to designate an output feature, and so should have been cleared prior to start of output feature processing. The bit was however not being cleared, causing the PXF ucode to mistakenly process a feature when it shouldn't have. The result is an attempt to transmit out a malformed packet, which the DMA ASIC is detecting.

  There are no known workarounds.

- CSCdz64878

  Only one Fan module is shown in the entity MIB. The Fan Module entity physical class and the container lass values are incorrect.

  This occurs when the entity MIB information about the Fan modules is queried in a Cisco 7300 router running images prior to the Cisco IOS Release 12.1(13)EX.

  There are no known workarounds.

- CSCdz65389

  Aging of flows, and thereby, export of aged out flows, may stall. When there are a large number of flows, this may result in failure to get new flow IDs. The flow data shown in **show ip cache flow** may be incorrect or incomplete or repeated multiple times.

  The above symptoms may be observed on a c7300 with an NSE-100 services engine enabled for netflow accounting when the **show ip cache flow** display is held at a --More-- prompt or if the show command is executed simultaneously from multiple vty sessions.

  In order to retrieve the detailed flow information from the PXF, the flow ager within the PXF is temporarily frozen so that a snapshot of the flow data can be taken. The freeze time is between the start and end of the show command display. If the display is held at a --More-- prompt, the ager remains frozen for that duration. Also, the ager freezing is not protected from multiple simultaneous sessions of the **show ip cache flow** command. This can result in the ager being re-enabled when one display terminates while another display is still active.

  Workaround: Do not execute the **show ip cache flow** command simultaneously from more than one session. Do not hold the output display at the --More-- prompt.

- CSCdz72530

  7304 routers with the NSE-100 services engine might stop forwarding with PXF when netflow v5 enabled in PXF.

  Workaround: Disable netflow v5 accounting.

- CSCdz76672

  The communication between the route processor (RP) and the port adapter carrier card (PA-CC) is based on interprocessor communications (IPC) on Cisco 7300 routers. Periodic IPC packets are used for keepalive heartbeats for the PA-CC. If the heartbeat packets are lost, the PA-CC will go to reset for recovery. This may happen only on the NPE-G100 board as the RP. The problem has been fixed by putting all IPC packets in the high priority path that is separate from the normal data path in the router.

  There are no known workarounds.

- CSCdz78601

  Link utilization may be low in certain cases when configured for class based weighted fair queueing via the **bandwidth** class command.

  The above behavior may be seen on a c7304 system with an NSE-100 services engine when an output service policy has a class with a high CIR but low offered rate and a class with a low CIR but high offered rate.

  In certain cases depending on the traffic flow, allocation of excess or unused bandwidth to the low CIR queue, when that queue goes active, may not be optimal due to the presence of the other high CIR queue.

  There are no known workarounds. This behavior is dependent on traffic pattern, packet size, and traffic rate per class queue.

- CSCdz80757

  MPLS MIBs is not accessible.

  The above symptom may be observed on a c7304 system with an NSE-100 services engine configured for MPLS.

  There are no known workarounds as the MIB support was excluded from the images.

- CSCdz82441

  A traceback message may be seen when configuring dynamic NAT.

  The above mentioned traceback may be seen on a c7304 with an NSE-100 services engine.

  This traceback seems to be due to an interaction between Access lists and NAT, possibly due to a race condition between the two whereby NAT checks an ACL data structure prior to its setup.

  There are no known workarounds. The message has been seen just once and is difficult to reproduce. There was no known misbehavior after the traceback was seen.

- CSCdz85439

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

  This happens only for ICMP echo replies when:

  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 configure ACL with unsupported ACEs.

- CSCdz87536

  Packets that should have got switched by the PXF processor get punted to the Route Processor due to MPLS Null Rewrite. This may manifest itself as high RP CPU utilization and lower throughput.

  The above behavior may be seen on a c7304 with an NSE-100 services engine when an interface is deconfigured for MPLS switching.

  The **show pxf accounting punt** command output will display a non-zero count against the entry for MPLS Null Rewrite Punt.

  There are no known workarounds. Packets punted to the RP will still be forwarded by the RP.

- CSCdz87607

  On a c7300 system with an NSE-100 services engine configured for netflow accounting, exported flow records show start and end timestamps very close to system up time.

  This caveat is observed when netflow accounting is enabled in the PXF processor on the NSE-100.

  Workaround: Run RP netflow by configuring ‘no ip pxf’.

- CSCdz87613

  On a c7300 system with an NSE-100 services engine configured for netflow accounting, sometimes large packet count or byte account is observed.

  This caveat is observed when netflow accounting is enabled in the PXF processor on the NSE-100.

  Workaround: Disable pxf netflow by using the **no ip pxf** command.

- CSCea15744

  On a c7300 system with an NSE-100 services engine configured for netflow accounting, netflow stats have included L2 length from each data packet.

  This caveat is observed when netflow accounting is enabled in the PXF processor on the NSE-100.

  Workaround: Select RP netflow using “no ip pxf” when traffic is light enough to be handled by RP alone.

- CSCea32513

  The following error message, followed by a traceback message from the OIR Handler process, may be seen:

  ```
  %SYS-2-INTSCHED: 'suspend' at level 5
  ```

  The above messages may be seen on a c7304 system with an NSE-100 services engine after online removal of a line card.

  There are no known workarounds. There is no known negative effect from these messages either.

- CSCea35763

  Forwarding of input traffic from an interface stops if a service policy with a shape command is applied as an input service policy. Incoming packets on that interface are dropped in the PXF processor.

  The above behavior may be seen on a c7304 with an NSE-100 services engine when an input service policy with shaping or any queueing commands is applied as an input policy.

  Workaround: Deconfigure and reconfigure the service policy as an output policy.

- CSCea36962

  Packets with source address destined to NULL interface may not be dropped when loose mode unicast RPF is configured.

  The above behavior may be observed on a c7304 with an NSE-100 services engine configured for uRPF in the PXF processor. Routes to the NULL interface must exist in the system.

  There are no known workarounds. Note that packets are dropped correctly if the system has no routes for the source addresses.

- CSCea46135

  WRED drops may not be as expected.

  The above behavior may be seen on a c7304 with an NSE-100 services engine configured for the following:

  - IP precedence based WRED and non-default thresholds
  - IP DSCP based WRED and non-default thresholds but default mark probability

  For the cases mentioned above, the default threshold values are being downloaded to the PXF processor instead of the configured thresholds.

  There are no known workarounds. WRED will still function, but with the default threshold values, not those configured.

- CSCea47603

  On Cisco 7304 routers, getting access to the Flash MIB ciscoFlashFileTable may cause router crash. It is due to uninitialized buffer for holding Flash MIB that gives wrong database. The problem has been fixed.

  There are no known workarounds.

- CSCea72349

  System may hang after configuring a police command on a priority queue.

  The above symptom may be seen on a c7304 system with an NSE-100 services engine. Exact conditions under which the system hangs are not known, but it depends on the values configured in the police command, as well as possibly the bandwidth allocation to other class queues within the service policy.

  There are no known workarounds. This caveat does not happen in all cases and may be difficult to reproduce.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family. 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 these documents:

- Release-Specific Documents, page 55
- Platform-Specific Documents, page 56
- Feature Modules, page 56
- Cisco IOS Software Documentation Set, page 57

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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 12.2*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 SZ" in these release notes, see *Caveats for Cisco IOS Release 12.2* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, 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/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Core/High-End Routers**

  On the Documentation CD-ROM at:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(14)SZ6 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 Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

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: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set Contents

Table 13 lists the contents of the Cisco IOS Release 12.2 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.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 13 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide: Dial Access* • *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications* • *Cisco IOS Dial Technologies Command Reference, Volume 1 of 2* • *Cisco IOS Dial Technologies Command Reference, Volume 2 of 2*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 13 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 13 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 S* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through 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

- 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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 55.