Release Notes for Cisco 7000 Family and Cisco 12000 Series Routers for Cisco IOS Release 12.0 S

March 27, 2000

Cisco IOS Release 12.0(10)S

Text Part Number 78-7130-06

These release notes for Cisco 7000 family and Cisco 12000 series routers support Cisco IOS Release 12.0 S, up to and including Release 12.0(10)S. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents. Cisco IOS Release 12.0 S is based on Cisco IOS Release 12.0 and is tailored for service provider environments. Release 12.0 S is the follow on release to Release 11.1 CC, which was also targeted to the service provider environment. Additionally, many of the features in Release 12.0 S were first introduced for the Cisco 12000 series routers on Release 11.2 GS and for the Cisco 7000 family on Release 12.0 T.

Use these release notes in conjunction with the *Release Notes for Cisco IOS Release 12.0* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

In addition to the caveats listed in the "Caveats" section, the software caveats that apply to Release 12.0 also apply to Release 12.0 S. For information on other caveats that might apply to Cisco IOS Release 12.0 S, the caveats document for Release 12.0 is located on CCO and on the Documentation CD-ROM.

Contents

CISCO SYSTEMS

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

Introduction

Cisco IOS Release 12.0(5)S was the first public release of this software. Many of the features and hardware support in this software have previously been released to customers on other software releases. For information on new features and Cisco IOS commands supported by Release 12.0 S, see the "New and Changed Information" section on page 9 and "Related Documentation" section on page 53.

System Requirements

Memory Requirements

Tables 1, 2, and 3 list the memory requirements for the platforms supported in Cisco IOS Release 12.0 S.

Table 1 Memory Requirements for the Cisco 7200 Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	c7200-p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	c7200-k3p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	c7200-k4p-mz	16 MB	128 MB	RAM

Table 2 Memory Requirements for the Cisco 7500/RSP Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	rsp-pv-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	rsp-k3pv-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	rsp-k4pv-mz	16 MB	128 MB	RAM

Table 3 Memory Requirements for the Cisco 12000/GSR Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	gsr-p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	gsr-k3p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	gsr-k4p-mz	16 MB	128 MB	RAM

Hardware Supported

Cisco IOS Release 12.0 S supports the following platforms:

- Cisco 7200 series (including the Cisco 7202, Cisco 7204, Cisco 7204 VXR, Cisco 7206, and Cisco 7206 VXR)
- Cisco 7500 series (including the Cisco 7505, Cisco 7507, Cisco 7513, and Cisco 7576)
- Cisco 7000 series routers (including the Cisco 7000 and Cisco 7010) upgraded with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)
- Cisco 12000 series (including the Cisco 12008 and 12012)

Determining Your Software Release

To determine the version of Cisco IOS software currently running on Cisco routers, log in to the router and enter the **show version** EXEC command. The following is sample output from the **show version** command. The version number is indicated on the second line.

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-P-M), Version 12.0(5)S, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Microcode Software

Table 4 lists the current microcode versions for the Cisco 7500/RSP series. This series includes the Cisco 7000 equipped with the RSP7000 processor, the Cisco 7010 equipped with the RSP7000 processor, and the Cisco 7500 series routers. Note that microcode software images are bundled with the system software image, with the exception of the Channel Interface Processor (CIP) microcode (all system software images) and Versatile Interface Processor (VIP) microcode (certain system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. VIP and VIP2 microcode is bundled into all Cisco 7500 series feature sets listed in Table 4.

For further information about the CIP microcode, refer to the Cisco document *Channel Interface Processor Microcode Release Note and Microcode Upgrade Instructions*.

Note The Cisco 7000 series previously included the Cisco 7000 and 7010 routers. These products are not supported in Cisco IOS Release 12.0 S. The Cisco 7000 series now includes the Cisco 7000 equipped with the RSP7000 processor and the Cisco 7010 equipped with the RSP7000 processor.

Table 4 Cisco 7500/RSP Series Routers Microcode Versions

Processor or Module	Current Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	20.13
CIP/CIP2 (Channel Interface Processor)	26.12	26.2
EIP (Ethernet Interface Processor)	20.6	20.3
FEIP (Fast Ethernet Interface Processor)	20.8	20.7
FIP (FDDI Interface Processor)	20.4	20.4
FSIP (Fast Serial Interface Processor)	20.9	20.9
HIP (HSSI Interface Processor)	20.2	20.2
MIP (MultiChannel Interface Processor)	22.3	22.3
TRIP (Token Ring Interface Processor)	20.2	20.2
VIP2/VIP2C (Versatile Interface Processor)	22.20	22.20

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.

Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to U.S. government export controls and limited distribution. Images to be installed outside the U.S. require an export license. Customer orders may be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Tables 5, 6, and 7 list the newest features and feature sets supported by the Cisco 7200 series, the Cisco 7500/RSP series, and the Cisco 12000 series in Cisco IOS Release 12.0 S 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 12.0 S release in which the feature was introduced. Many of these features were initially available on other releases.

Note This feature set table only contains a selected list of features. This table is not cumulative— nor does it list all the features in each image.

Table 5 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ATM PVC Trap Support	(5)	Yes	Yes	Yes
Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Fast EtherChannel	(8)	Yes	Yes	Yes
Frame Relay Enhancements for K2 Scalability	(5)	Yes	Yes	Yes
Gigabit Ethernet (PA-GE Support)	(7)	Yes	Yes	Yes
ISL Support	(5)	Yes	Yes	Yes
MPLS over Frame Relay	(10)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Named Community Lists	(10)	Yes	Yes	Yes
NetFlow Policy Routing		No	No	No
New Revision of System Controller Chip for NPE-175/NPE-225	(9)	Yes	Yes	Yes
NPE-175/NPE-225	(6)	Yes	Yes	Yes
NPE-300	(5)	Yes	Yes	Yes
OC-12c Dynamic Packet Transport (DPT) Port Adapter	(6)	Yes	Yes	Yes
PA-MC-2T3+ Multichannel T3 Port Adapter	(6)	Yes	Yes	Yes
PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters	(5)	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter	(5)	Yes	Yes	Yes
PA-MC-T3 Multichannel T3 Port Adapter	(5)	Yes	Yes	Yes
Process MIB		No	No	No
Router-ports Group Management Protocol (RGMP)	(10)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters	(7)	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7500/RSP Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ATM PVC Trap Support	(5)	Yes	Yes	Yes
Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
Cisco 7576 Router	(5)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Distributed Multilink Point-to-Point Protocol	(9)	Yes	Yes	Yes
Distributed Traffic Shaping	(7)	Yes	Yes	Yes
Fast Etherchannel		Yes	Yes	Yes
Frame Relay Enhancements for K2 Scalability	(5)	Yes	Yes	Yes
Gigabit Ethernet Interface Processor	(5)	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7500/RSP Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ISL Support	(5)	Yes	Yes	Yes
Low Latency Queueing	(9)	Yes	Yes	Yes
Memory Scan	(6)	Yes	Yes	Yes
MPLS over Frame Relay	(10)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Named Community Lists	(10)	Yes	Yes	Yes
NetFlow Policy Routing	(6)	Yes	Yes	Yes
OC-12c Dynamic Packet Transport (DPT) Port Adapter	(6)	Yes	Yes	Yes
PA-MC-2T3+ Multichannel T3 Port Adapter	(6)	Yes	Yes	Yes
PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters	(5)	Yes	Yes	Yes
PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter	(5)	Yes	Yes	Yes
PA-MC-T3 Multichannel T3 Port Adapter	(5)	Yes	Yes	Yes
Process MIB		No	No	No
Route Switch Processor (RSP8)	(9)	Yes	Yes	Yes
Router-ports Group Management Protocol (RGMP)	(10)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7500/RSP Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters	(7)	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 12000 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
1OC-12/STM-4 SRP Line Card	(6)	Yes	Yes	Yes
2 x 32-Bit Counters	(10)	Yes	Yes	Yes
6DS3-SMB Line Card	(6)	Yes	Yes	Yes
8-Port Fast Ethernet Line Card	(6)	Yes	Yes	Yes
8xOC-3 POS or 16xOC-3 POS Line Card	(10)	Yes	Yes	Yes
Access List Performance Improvements for Cisco 12000 Gigabit Switch Routers	(10)	Yes	Yes	Yes
APS Reflector Mode	(8)	Yes	Yes	Yes
ATM PVC Trap Support	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
Cisco 12016 Gigabit Switch Router	(8)	Yes	Yes	Yes
Cisco Optical Regenerator	(10)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Enhanced OC-48c/STM-16c Layer 3 Packet-over-SONET Line Card	(7)	Yes	Yes	Yes
Enhanced Quad OC-12c/STM-4c Layer 3 Packet-over-SONET Line Card	(8)	Yes	Yes	Yes
Extended Ethernet Frame Size Support	(10)	Yes	Yes	Yes
Gigabit Ethernet Line Card	(5)	Yes	Yes	Yes
GRP Redundant Processor Support	(5)	Yes	Yes	Yes
ISL Support		No	No	No
MPLS Switching Support for Gigabit Ethernet	(7)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 12000 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Named Community Lists	(10)	Yes	Yes	Yes
NetFlow on GSR	(6)	Yes	Yes	Yes
NetFlow Policy Routing		No	No	No
NetFlow Support for Gigabit Ethernet	(7)	Yes	Yes	Yes
Per-VC Queueing	(7)	Yes	Yes	Yes
Process MIB	(6)	Yes	Yes	Yes
RFC 1483 Bridged PVC Encapsulation	(5)	Yes	Yes	Yes
Router-ports Group Management Protocol (RGMP)	(10)	Yes	Yes	Yes
Section Data Communications Channel (SDCC)[1]	(10)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Virtual Path Traffic Shaping	(8)	Yes	Yes	Yes
Weighted Random Early Detection (WRED)	(10)	Yes	Yes	Yes

1. SDCC is supported on GSR OC-48-based line cards.

New and Changed Information

- Important Notes, page 31

New Features in Release 12.0(10)S

Many of the new features in Cisco IOS Release 12.0 S were introduced on other Cisco IOS releases. For more complete information, refer to the original release.

2 x 32-Bit Counters

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports 2 x 32-bit counters. The 2 x 32-bit counters MIB will allow the 64-bit counters ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets, and ifHCOutUcastPkts to each be represented as two 32-bit objects. One object will represent the upper 32-bits and the other the lower 32-bits. The new objects are as follows:

- cHCCounterIfInOctetsUpper
- cHCCounterIfInOctetsLower
- cHCCounterIfInUcastPktsUpper
- cHCCounterIfInUcastPktsLower
- cHCCounterIfOutOctetsUpper
- cHCCounterIfOutOctetsLower
- cHCCounterIfOutUcastPktsUpper
- cHCCounterIfOutUcastPktsLower

8xOC-3 POS or 16xOC-3 POS Line Card

Platforms: Cisco 12000 series

The single-mode or multimode 8xOC-3 POS or 16xOC-3 POS line card allows Cisco 12000 series routers to aggregate large amounts of data on existing fiber networks. The 8xOC-3 POS or 16xOC-3 POS line card interfaces with the switch fabric in the Cisco 12000 series router and provides a support level of 64 ports per 8-port system and 256 ports per 16-port system. Support for quality of service (QoS) packet flow control processing provides an additional value-added routing feature for Internet service providers (ISPs).

The 8xOC-3 POS line card provides Cisco 12000 series routers with 8 OC-3/STM-1 ports per slot or up to 64 OC-3/STM-1 ports per system. The 16xOC-3 POS line card provides Cisco 12000 series routers with 16 OC-3/STM-1 ports per slot or up to 256 OC-3/STM-1 ports per system. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/41812oc3.htm

Access List Performance Improvements for Cisco 12000 Gigabit Switch Routers

Platforms: Cisco 12000 series

Access list (ACL) performance improvements are provided for two types of Cisco 12000 line cards:

- Line cards using engine 1 architecture
- Line cards using engine 2 architecture

The ACL performance improvement is implemented in a slightly different way depending on the line card type. Engine 1 line cards achieve ACLperformance improvement strictly through hardware, using an improved ASIC design. Engine 2 line cards use a microcode enhancement in the packet switch ASIC (PSA) for packet-over-SONET (POS) applications. See the following document for further information:

http://www.
cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s10/hw_acl.htm

Cisco Optical Regenerator

Platforms: Cisco 12000 series

The Cisco Optical Regenerator is a bidirectional OC-48/STM-16 regenerator that sends optical signals over the longest distance possible. It supports single-mode long reach optical-fiber transmission when connected to an OC-48 line card that is installed in a Cisco 12000 series Gigabit Switch Router (GSR). The SONET specification for fiber-optic transmission defines the standard for single-mode fiber. The regenerator provides an end-to-end IP transport for long distances by forwarding SONET/SDH traffic at OC-48 line rates.

The Cisco Optical Regenerator uses only single-mode fiber because signals can travel farthest through single-mode long reach fiber. The maximum distance for single-mode installations of the regenerator is determined by the amount of light loss in the fiber path andby the physical limitation of sending optical fiber to optical light over exceptionally long distances. High-quality single-mode fiber with minimal high-quality splices can carry a Cisco Optical Regenerator signal up to 50 miles (80 kilometers).

Extended Ethernet Frame Size Support

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports Extended Ethernet Frame Size in accordance with the Network Working Group Internet Draft titled “Extended Ethernet Frame Size Support,” draft-kaplan-isis-ext-eth-00.txt.

MPLS over Frame Relay

Platforms: Cisco 7200 series, Cisco 7500/RSP series

Transmission of Multiprotocol Label Switching (MPLS)-encapsulated packets across a point-to-point Frame Relay subinterface is now supported. Configuration of the feature is identical to configuration of MPLS on any other interface type:

```
(config)# interface Serial1/0.1 point-to-point
(config-if)# tag ip
```

or

```
(config-if)# mpls traffic-engineering tunnels
```

Note that some Frame Relay features (for example, FRF.12 fragmentation) are not supported for MPLS packets.

Named Community Lists

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

With numbered community lists, there are two types of community list numbers (standard and extended), and there can be up to 100 of each of the lists. Named community lists do not have an upper limit on the number of lists that can be defined. The command syntax is as follows:

ip community-list standard [**community-name** | **community-number**] [**permit**|**deny**] **community**

ip community-list extended [**community-name** | **community-number**] [**permit**|**deny**] **regular-expression**

All rules of numbered community lists apply.

Secure Shell Client Version 1

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. Two versions of SSH are available: SSH Version 1, and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

The SSH Client feature is an application that runs on a reliable TCP/IP transport layer, and provides strong authentication and encryption. The SSH Client in Cisco IOS software allows a user that is running an EXEC session on a Cisco router to log in to another remote Cisco router, and execute commands on the remote router. With authentication and encryption, SSH Client allows for a secure communication over an insecure network. SSH Client Version 1 supports DES and 3DES encryption and userid/password authentication.

Section Data Communications Channel

Platforms: Cisco 12000

On Cisco GSR OC-48 based line cards, Cisco IOS Release 12.0 S now supports the IP/Section Data Communications Channel (SDCC) interface that is available on the Cisco OC-48 Optical Regenerator. To enable this feature, enter the **sdcc enable** command in configuration mode. To disable this feature, enter the **no sdcc enable** command. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/optregen/opt_cfg/regen48.htm

SNMP Support for BGP Policy Accounting

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

BGP Policy Accounting accumulates incoming packet counts and octet counts per interface in the fibidb structure. These counters are now SNMP retrievable because of a new MIB called CISCO-BGP-POLICY-ACCOUNTING-MIB. Each row in the MIB table contains statistics for a particular traffic type on an interface. The table is indexed by ifindex from the IF-MIB and a traffic_index that identifies a particular traffic type. The traffic can be classified into one of eight types using the command-line interface (CLI).

Weighted Random Early Detection

Platforms: Cisco 12000 series

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of the TCP congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

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

WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than at the edge. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how it treats different types of traffic. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/wred_gs.htm

New Features in Release 12.0(9)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced on other Cisco IOS releases. For more complete information, refer to the original release.

BGP Policy Accounting

Platforms: Cisco 7200 series; Cisco 7500/RSP series, Cisco 12000 series

BGP Policy Accounting provides a means of charging customers according to the route that their traffic travels. Trans-Pacific, Trans-Atlantic, satellite, domestic, and other provider traffic can be identified and accounted for on a per-customer basis when customers are on a unique software interface. This feature also allows the accounting of traffic to known autonomous system numbers in order to better engineer and plan network circuit peering and transit agreements.

BGP Policy Accounting classifies IP traffic by autonomous system number or autonomous system community string and increments packet and byte counters per input interface. It performs this function using route-maps to classify the traffic into one of eight possible indexes, which represent a traffic classification.

Distributed Multilink Point-to-Point Protocol

Platforms: Cisco 7500/RSP series

The Distributed Multilink Point to Point Protocol (distributed MLP) feature allows T1/E1 lines to be combined in a Versatile Interface Processor (VIP) on a Cisco 7500 series router into a bundle that has the combined bandwidth of multiple T1/E1 lines by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle, which allows you to increase the bandwidth of your network links beyond that of a single T1/E1 line without the need to purchase a T3 line.

Nondistributed MLP can only perform limited links, with CPU utilization quickly reaching 90 percent with only a few T1/E1 lines running MLP. With distributed MLP, you can increase the total capacity of the router. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/multippp.htm

Low Latency Queueing

Platforms: Cisco 7500/RSP series

The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without Low Latency Queueing, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic, which is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queueing feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, Low Latency Queueing enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue.

In the event of congestion, when the bandwidth is exceeded, policing is used to drop packets. Voice traffic enqueued to the priority queue is User Datagram Protocol (UDP)-based and therefore not adaptive to the early packet drop characteristic of Weighted Random Early Detection (WRED).

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5c/llqvip.htm

New Revision of System Controller Chip for NPE-175/NPE-225

Platforms: Cisco 7200 series

This feature adds support for a new revision of a hardware component that fixes a previous error. For the benefit of users that have not upgraded to the new hardware, it will also exhibit the following warning error message that indicates the old hardware revision:

```
PLATFORM-4-RECALLED_NPE: Old version NPE-175/225 with Rev= 0xNN system controller.
Contact upgrades-info@cisco.com for replacement.
```

Cisco 7200 series routers with NPE-175 or NPE-225 network processing engines must upgrade to Cisco IOS releases that incorporate this change (for example, Cisco IOS Release 12.0(9) and later releases or Cisco IOS Release 12.0(9)S and later releases). Use of older Cisco IOS releases might result in unpredicted malfunctions. See the following document for further information:

http://www.cisco.com/warp/customer/770/fn8611.shtml

Route Switch Processor (RSP8)

Platforms: Cisco 7500/RSP series

The RSP8 is the newest main system processor module for Cisco 7500 series routers. In addition to running the system software from DRAM, the RSP8 sends and receives routing protocol updates, manages tables and caches, monitors interface and environmental status, and provides Simple Network Management Protocol (SNMP) management and the interface between the console and Telnet.

The high-speed switching section of the RSP8 communicates with and controls the interface processors on the high-speed CyBus. This switching section of the RSP8 decides the destination of a packet and switches it based on that decision. See the following document for further information:

www.cisco.com/cc/td/doc/product/core/cis7507/7507cfig/6586rsp8.htm

Router-ports Group Management Protocol (RGMP)

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Router-Port Group Management (RGMP) is a new protocol that restricts multicast traffic to router ports.

CGMP (Cisco Group Management Protocol) and IGMP (Internet Group Management Protocol) are two existing features that restrict multicast traffic to hosts that do not need to receive them, reducing the amount of processing the hosts have to do. CGMP and IGMP only restrict traffic on the ports of switches to which hosts are connected. CGMP and IGMP are designed for typical access networks where many hosts are connected but only one or two routers forward traffic to those hosts.

RGMP is designed for switched backbone networks or exchange points where predominantly routers are connected to each other. Large amounts of multicast traffic can be restricted, eliminating unnecessary congestion on the router ports. To effectively restrict multicast traffic to router ports, both the routers and the switches on the network must support RGMP.

New Features in Release 12.0(8)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced on other Cisco IOS releases. For more complete information, refer to the original release.

APS Reflector Mode

Platforms: Cisco 12000 series

APS reflector mode enhances the operation of automatic protection switching (APS) by decreasing the remote timeout that occurs when a remote router is informed of a switchover between the working router and protect router in an APS circuit.

Cisco 12016 Gigabit Switch Router

Platforms: Cisco 12000 series

The Cisco 12016 Gigabit Switch Router (GSR), is a 16-slot member of the Cisco 12000 series of Gigabit Switch Routers. The Cisco 12016 GSR delivers a raw transmission rate per slot of up to 10 Gbps, a switching capacity of up to 160 Gbps, and speeds of up to OC-48/STM-16 (2.44 Gbps). It uses the same Gigabit Route Processor (GRP) and line cards (OC-3, OC-12, and OC-48) as the other routers in the Cisco 12000 series of routers. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12016/hfricg/index.htm

Enhanced Quad OC-12c/STM-4c Layer 3 Packet-over-SONET Line Card

Platforms: Cisco 12000 series

The Quad OC-12c/STM-4c Packet-over-SONET (POS) line card provides Cisco 12000 series routers with four 622-Mbps POS interfaces on a single card. The card interfaces with the switch fabric in the Cisco 12000 series router and provides four OC-12c/STM-4c duplex SONET connections via Single-Mode OC-3c Cable (SC Connectors). Each connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/10187pos.htm

Fast EtherChannel Support on Cisco 7200 Platform

Platforms: Cisco 7200 series

Fast EtherChannel is now supported on Cisco 7200 series routers. The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. For more information on Fast EtherChannel, see the original feature guide written for the 11.1 CC Release, *Fast EtherChannel*, at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/ca111/fechan.htm

Or see page 31 of the *Cisco IOS Interface Configuration Guide* for Cisco IOS Release 12.0 at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/inter_c/iclanint.htm#3809

Multiprotocol Label Switching Traffic Engineering OSPF Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multiprotocol Label Switching (MPLS) traffic engineering software released in Cisco IOS Release 12.0(5)S has been enhanced to support OSPF routing. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s8/te_1208s.htm

Service Assurance Agent

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key service level agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

The SA Agent feature was introduced in Cisco IOS Release 12.0(5)T, and is now available in Cisco IOS Release 12.0(8)S.

The SA Agent provides new capabilities that enable you to monitor:

- Domain Name System (DNS) performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) echo response time, and TCP connection setup time, with different ToS settings in the IP header.
- Network one-way delay variance (jitter) and packet loss.
- Web server response time.

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/saaoper.htm

Virtual Path Traffic Shaping

Platforms: Cisco 12000 series

Virtual path (VP) traffic shaping allows multiple virtual circuits (VCs) to be bundled into one VP. This “bundling” is also called traffic shaping because all VCs bundled within the VP are shaped as one traffic rate. In addition, bundling the VCs improves the error detection for the bundled VCs.

New Features in Release 12.0(7)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced on other Cisco IOS releases. For more complete information, refer to the original release.

ATM CLP Setting

Platfforms: Cisco 7500/RSP series

The use of the Cell Loss Priority (CLP) bit in the ATM header of a cell provided a method of controlling the discarding of cells in a congested ATM environment. A CLP bit contains two settings: 0 or 1. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0. Before the introduction of the ATM CLP Setting feature, the CLP bit was automatically set to 0 when Cisco routers converted packets into ATM cells for ATM networks.

The ATM CLP Setting feature allows users to control the CLP bit setting on routers running the PA-A3 port adapter. CLP bits are set on each packet individually, and the default CLP bit setting is 0. The application of the ATM CLP feature changes the CLP bit setting to 1. Therefore, users have the option of leaving each packet with the default CLP bit setting of 0 or establishing a new CLP bit setting of 1. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s7/atmclp.htm

Distributed Traffic Shaping

Platforms: Cisco 7500/RSP series

Many enterprise and service provider customers need to shape traffic in their networks and sometimes need to shape IP traffic independently of the underlying interface. In other cases, the goal is to perform traffic shaping to ensure adherence to committed information rates on Frame Relay links.

The dTS feature is one element used to manage the bandwidth of an interface to avoid congestion, meet remote site requirements, and conform to a service rate that is provided on that interface.

The distributed Traffic Shaping (dTS) feature uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate, which ensures that traffic will behave in accordance with the configured descriptor, as defined by committed information rate (CIR) (mean rate), Bc (burst size), and Be (excess burst size). With the defined average bit rate and burst size that are acceptable on that shaped entity, you can derive a time interval value.

The excess burst size (Be) allows more than the burst size to be sent during a time interval under certain conditions. Therefore, dTS provides two types of **shape** commands: **average** and **peak**. When **shape average** is configured, the interface sends no more than the burst size for each interval, achieving an average rate no higher than the mean rate (CIR). When **shape peak** is configured, the interface sends Bc plus Be bits in each interval.

In a link layer network such as Frame Relay, the network sends messages with the forward explicit congestion notification (FECN) or backward explicit congestion notification (BECN) if there is congestion. With the dTS feature, the traffic shaping adaptive mode takes advantage of these signals and adjusts the traffic descriptors, which approximates the rate to the available bandwidth along the path.

Enhanced OC-48c/STM-16c Layer 3 Packet-over-SONET Line Card

Platforms: Cisco 12000 series

The OC-48c/STM-16c POS line card provides Cisco 12000 series routers with a single 2.5-Gbps POS interface on a single card. The card interfaces with the switch fabric in the Cisco 12000 series router and provides one OC-48c/STM-16c duplex SC or FC single-mode connection. This connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6792oc48.htm

Gigabit Ethernet (PA-GE Support)

Platforms: Cisco 7200 series

The PA-GE is a single-port port adapter that, when combined with the appropriate fiber-optic cable and a Gigabit Interface Converter (GBIC), provides one Gigabit Ethernet (GE) interface that is compliant with the IEEE 802.3z specification. The GE interface on a PA-GE operates in full-duplex mode. The PA-GE is supported by the Cisco 7200 VXR routers. Please note that this port adapter is not currently supported by the fourth-generation Versatile Interface Processor (VIP4). See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/72vxpa/7188page/index.htm

ISIS Over ISL

Platforms: Cisco 7200 series, Cisco 7500/RSP series

With release 12.0(7)S, Intermediate System-to-Intermediate System (ISIS), Connectionless Network Service (CLNS), and Interior Gateway Routing Protocol (IGRP) configuration commands are now recognized on an Inter-Switch Link (ISL) virtual LAN (VLAN) subinterface.

MPLS Switching Support for Gigabit Ethernet

Platforms: Cisco 12000 series

Basic tag/Multiprotocol Label Switching (MPLS) switching is now supported for Gigabit Ethernet (GE) line cards for the Cisco 12000 series Gigabit Switch Router (GSR).

NetFlow Support for Gigabit Ethernet

Platforms: Cisco 12000 series

The NetFlow feature is now a supported feature for Gigabit Ethernet (GE) line cards for the Cisco 12000 series Gigabit Switch Router (GSR).

Per-VC Queueing

Platforms: Cisco 12000 series

The per-virtual circuit (VC) queueing enhancements for the Quad OC-3c/STM-1c ATM line card provide additional control of traffic management on the line card. Within limits, you can adjust queuing priorities for each VC defined on a line card interface. This feature lessens traffic congestion and improves quality of service (QoS).

Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters

Platforms: Cisco 12000 series

Two-port versions of the Multichannel DS1/PRI and Multichannel E1/PRI port adapters are now available. See the following documents for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/4815ds1p/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/5083e1p/index.htm

New Features in Release 12.0(6)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced on other Cisco IOS releases. For more complete information, refer to the original release.

1OC-12/STM-4 SRP Line Card

Platforms: Cisco 12000 series

The 1OC-12/STM-4 spatial reuse protocol (SRP) line card equips the Cisco series 12000 Gigabit Switch Router with a total of two OC-12c, fiber-optic SC duplex ports. The line card provides two duplex SC connections for either the single-mode or multimode version. The Service Processing Element (SPE) payload is concatenated, which increases efficiency by eliminating the need to partition the bandwidth. The 1OC-12/STM-4 SRP line card is slot independent. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/5929srp.htm

6DS3-SMB Line Card

Platforms: Cisco 12000 series

The 6DS3-SMB line card consist of high-density DS3 service through six T3 interfaces.

The 6-port line card is a partially depopulated version of the 12-port line card. The 6-port line card consists of a total of 12 connectors. A single port consists of one coaxial connector for receiving (Rx) and one coaxial connector for sending (Tx). The ports on the 6-port line card are numbered 0 to 5.

The 6DS3-SMB line card supports serial encapsulation protocols, Gigabit Switch Router (GSR) standard line card packet switching, and DS3 support. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6587ds3.htm

8-Port Fast Ethernet Line Card

Platforms: Cisco 12000 series

The 8-Port Fast Ethernet line card provides eight Fast Ethernet (IEEE 802.3u) interfaces that operate at a full-duplex data rate of 100 Mbps each. This line card connects to the Gigabit Switch Router (GSR) switch fabric, which supports transfer rates of up to 40 Gbps within the GSR.

The 8-Port Fast Ethernet line card supports both copper and fiber-optic Fast Ethernet transceivers. The fiber-optic 100BaseFX interface supports multimode SC duplex connectors operating in half- or full-duplex mode. The copper interface supports both full- and half-duplex 100BaseTX standards that use an RJ-45 connector.

The Fast Ethernet connectivity gives the GSR platform the flexibility to be used as an edge router in high-bandwidth environments, such as an Internet service provider or a corporate backbone. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6224fe8.htm

Memory Scan

Platforms: Cisco 7500/RSP series

The Memory Scan feature for Cisco 7500 series router Route Switch Processor (RSP) modules adds a low-priority background process that searches all installed DRAM for possible parity errors. The process runs every 60 seconds and can be controlled and monitored with new command-line interface commands. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/tmemscn.htm

NetFlow Policy Routing

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

IP policy routing now works with Cisco Express Forwarding (CEF), distributed CEF (dCEF), NetFlow, and NetFlow with flow acceleration.

IP policy routing was formerly supported only in fast switching and process-switching. Furthermore, support in fast switching was limited because the routing table sometimes had to be consulted before packets could be policy-routed, which was too expensive or impossible in the fast-switching path.

NetFlow on GSR

Platforms: Cisco 12000 series

NetFlow routing is now supported on the Cisco 12000 series routers. Support for Netflow routing on the Gigabit Ethernet port adapter, PA-GE, is not yet available.

NPE-175/NPE-225

Platforms: Cisco 7200 series

The network processing engine is available in five versions: NPE-150, NPE-175, NPE-200, NPE-225, and NPE-300. The network processing engines have the same functionality; however, the performance differs because of the microprocessor type and the type of memory for packet data (SRAM and DRAM, or SDRAM) each network processing engine provides.

The latest network processing engines, the NPE-175 and NPE-225, consist of two modular boards: the processing engine and the network controller board. SRAM is not included in the NPE-175 or NPE-225.

OC-12c Dynamic Packet Transport Port Adapter

Platforms: Cisco 7200 series, Cisco 7500 series

The Dynamic Packet Transport (DPT) port adapter is a dual-width OC-12c port adapter that provides a shared IP over SONET capability in a Cisco 7200 series, Cisco 7200 VXR, or Cisco uBR7200 series router.

The DPT port adapter is designed to be deployed in SONET OC-12 DPT rings. DPT rings can also be connected to SONET add drop multiplexers (ADMs), thus allowing for the creation of small or very large DPT rings. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206cfig/6481oc12.htm

PA-MC-2T3+ Multichannel T3 Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections using BNC connectors. The interface can provide up to 28 T1 lines (a single T3 group). Each T1 line is presented to the system as a serial interface that can be configured as one or more serial interfaces.

The PA-MC-2T3+ is a channelized port adapter that sends and receives data bidirectionally at the T3 rate of 44.736 Mbps (digital signal carried on a T3 line, DS3). The T3 connection, provided by two female BNC connections for transmit (TX) and receive (RX), requires 734A coaxial cable that has an impedance of 75 ohms.

On the VIP2, PA-MC-2T3+ microcode is loaded into and operates from synchronous dynamic random-access memory (SDRAM) on the VIP2-50. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206cfig/64452t3/index.htm

Process MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by Sample Network Management Protocol (SNMP). The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation and deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for Versatile Interface Processor (VIP) cards and the master CPU occurs even if the SNMP subsystem is not initialized.

SNMPv3

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large-scale deployment of SNMP for configuration, accounting, and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the

SNMP entities that make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID, which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or an intranet. The SNMPv3 protocol consists of the specification for the User-based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- Modification of information, or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal
- Masquerade, or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- Message stream modification, or protection against messages getting maliciously reordered, delayed, or replayed in order to effect unauthorized management operations
- Disclosure, or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy:
  - Communication without authentication and privacy (NoAuthNoPriv)
  - Communication with authentication and without privacy (AuthNoPriv)
  - Communication with authentication and privacy (AuthPriv)

Turbo Access Control Lists

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The turbo access control lists feature enables Cisco 7200 and 7500 series routers, and Cisco 12000 series Gigabit Switch Routers (GSRs) to evaluate access control lists (ACLs) for more expedient packet classification and access checks.

New Features in Release 12.0(5)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced on other Cisco IOS releases. For more complete information, refer to the original release.

ATM PVC Trap Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The ATM PVC Trap Support feature provides Simple Network Management Protocol (SNMP) notification for permanent virtual circuit (PVC) failures, and it provides SNMP access to PVC status tables.

Normally, a management station is not notified when an ATM PVC goes down. The ATM PVC Trap Support feature enables an agent to send the required PVC traps for this notification. It also provides support for these PVC status tables: atmCurrentlyFailingPVclTable and atmInterfaceExtTable.

Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-A3 ATM port adapters (PA-A3-T3, PA-A3-E3, PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML) available on Cisco 7500 series routers now support the following new features:

- Available bit rate (ABR) — The ABR service category is specified in the ATM Forum Traffic Management Specification Version 4.0.
- Virtual Path Shaping — A virtual path (VP) is a logical association or bundle of virtual circuits (VCs).

The PA-A3 ATM port adapters support multiplexing of one or more VCs over a VP that is shaped at a constant bandwidth. To use this feature, you configure a permanent virtual path (PVP) with a specific virtual path identifier (VPI). Any VCs that are created subsequently with the same VPI are multiplexed onto this VP; the traffic parameters of individual VCs are ignored.

Cisco 7576 Router

Platforms: Cisco 7500/RSP series

The Cisco 7576 router is the newest member of the Cisco 7500 series of routers, which consists of the 5-slot Cisco 7505, 7-slot Cisco 7507, and the 13-slot Cisco 7513. The Cisco 7576 router supports multiprotocol and multimedia routing and bridging with a wide variety of protocols and any combination of available electrical interfaces and media.

The Cisco 7576 router consists of two independent routers configured on a single backplane. This system is housed within the chassis footprint of a Cisco 7513 router. The dual independent router design effectively doubles the system bandwidth that exists in the Cisco 7513 router.

Network interfaces reside on interface processors that provide a direct connection between the two independent dual CyBuses located on the backplane of the Cisco 7576 router and your external networks. The two independent dual CyBuses facilitate the configuration of two independent routers on a single backplane.

There are bays for up to two AC-input or DC-input power supplies. The Cisco 7576 router will operate with one power supply. Although a second power supply is not required, a second power supply allows load sharing and increased system availability. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7576/index.htm

Command Line Interface String Search

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The command line interface (CLI) string search feature allows you to search or filter the output of any **show** or **more** command, which is useful for sorting through large amounts of output, or if you want to exclude output that you do not need to see. CLI string search also allows for searching and filtering at --More-- paging prompts.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can specify a maximum of one filter per command to either include or exclude output lines that contain the specified regular expression.

A regular expression is any word, phrase, number, and the like that appears in **show** or **more** command output.

Frame Relay Enhancements for K2 Scalability

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The **logging event** command has been enhanced to enable or disable logging data-link connection identifier (DLCI) Change and subinterface UPDOWN console messages on Cisco 7200 and Cisco 7500 series routers. The **logging event dlci-status-change** and **logging event subif-link-status** commands are used to enable logging.

The display on the **show frame-relay pvc** command has been enhanced on Cisco 7200 and Cisco 7500 series routers to include a table showing the number of permanent virutal connections (PVCs) in their various states.

Gigabit Ethernet Interface Processor

Platforms: Cisco 7500/RSP series

The Gigabit Ethernet Interface Processor (GEIP) is a single-port fixed configuration interface processor that, when combined with the appropriate fiber optic cable, provides one 1000-Mbps Gigabit Ethernet interface that complies with IEEE 802.032 standards.

The Gigabit Ethernet interface operates in full-duplex mode at 1000 Mbps in each direction: transmit (TX) and receive (RX).

The GEIP is available on all Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

An increased maximum Ethernet packet size of 1500 takes advantage of increased bandwidth and the full-duplex point-to-point link.

An interface command MTU (maximum transmission unit) allows users to specify an MTU size up to 16K (maximum supported by FX1000). The minimum allowable MTU size is 1500 bytes.

If the interface is configured with a fall-back option, the other port will be reconfigured to support a large packet when a switchover occurs. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7000/7000cfig/5350geip.htm

Gigabit Ethernet Line Card

Platforms: Cisco 12000 series

The Gigabit Ethernet line card provides Cisco 12000 series routers with an optical Ethernet interface on a single card that operates faster than 1 Gbps. The card interfaces with the switch fabric in the Cisco 12000 series router and provides one Gigabit Ethernet SC single-mode or multimode connection. This connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/gigecr.htm

GRP Redundant Processor Support

Platforms: Cisco 12000 series

The Gigabit Route Processor (GRP) redundant processor feature allows for the installation of two GRPs in a Cisco 12000 series Gigabit Switch Router. One GRP functions as the primary processor. The primary GRP supports all normal GRP operation. The other GRP functions as the secondary processor. The secondary GRP monitors the primary and will take over normal GRP operations if it detects a failure in the primary GRP. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/gsr_rp.htm

ISL Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Inter-Switch Link (ISL) support maintains virtual LAN (VLAN) information as traffic flows between switches and routers. ISL support has been added to the following images for the Cisco 7000 family in Release 12.0(5)S: c7200-p-mz, c7200-k3p-mz, c7200-k4p-mz, rsp-pv-mz, rsp-k3pv-mz and rsp-k4pv-mz.

Multicast BGP

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multicast Border Gateway Protocol (MBGP) feature adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, MBGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) to build data distribution trees.

It is possible to configure BGP peers that exchange both unicast and multicast network-layer reachability information (NLRI).

MBGP is useful when you want a link dedicated to multicast traffic, perhaps to limit which resources are used for which traffic. Perhaps you want all multicast traffic exchanged at one network access point (NAP). MBGP allows you to have a unicast routing topology different from a multicast routing topology. Thus, you have more control over your network and resources.

Prior to MBGP, the only way to perform interdomain multicast routing was to use the BGP infrastructure that was in place for unicast routing. If those routers were not multicast capable, or you had differing policies where you wanted multicast traffic to flow, you could not support it. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/mbgp.htm

Multicast Distributed Switching

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Prior to multicast distributed switching (MDS), IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms. With Cisco IOS Release 11.2 GS and Release 11.1 CC, IP multicast traffic can be distributed switched on RSP-based platforms with Versatile Interface Processors (VIPs).

Furthermore, MDS is the only multicast switching method on the Cisco 12000 Gigabit Switch Router (GSR), starting with Cisco IOS Release 11.2(11)GS.

Switching multicast traffic at the RP has the following disadvantages:

- The load on the RP is increased. This increase affects important route updates and calculations (for BGP, among others) and can stall the router if the multicast load is significant.
- The net multicast performance is limited to what a single RP can switch.

MDS solves these problems by performing distributed switching of multicast packets received at the line cards (VIPs in the case of an RSP, and line cards in the case of a GSR). The line card is the interface card that houses the VIPs (in the case of RSP) and the GSR line card (in the case of a GSR). MDS is accomplished using a forwarding data structure called a Multicast Forwarding Information Base (MFIB), which is a subset of the routing table. A copy of MFIB runs on each line card and is always kept up to date with the RP MFIB table.

In the case of RSP, packets received on non-VIP interface processors are switched by the RP.

MDS can work in conjunction with Cisco Express Forwarding (CEF), unicast distributed fast switching (DFS), or flow switching. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/mds.htm

Multicast Routing Monitor

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multicast Routing Monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. The Manager can reside on the same device as the Test Sender or Test Receiver. You can test a multicast environment using test packets (perhaps before an upcoming multicast event), or you can monitor existing IP multicast traffic.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns. If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. Also, by issuing a certain **show** command, you can see the error reports, if any. You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show** command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

Multicast Source Discovery Protocol

Platforms: Cisco 7200 series, Cisco 7500/RSP, Cisco 12000 series

Multicast Source Discovery Protocol (MSDP) connects multiple Protocol Independent Multicast (PIM) sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain RP.

MSDP depends heavily on MBGP for interdomain operation. You should run MSDP in your domain RPs that act as sources, sending to global groups for announcement to the Internet. See the following document for futher information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/msdp.htm

Multiprotocol Label Switching Traffic Engineering

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

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 versus 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. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mpls_te.htm

NPE-300

Platforms: Cisco 7200 series

The network processing engine NPE-300 is the newest and the highest performance processor in the family of network processing engines for the Cisco 7200 series routers. The NPE-300 performs at a rate of approximately 300,000 packets per second (pps) in fast switching, a 50 percent increase over the NPE-200 performance.

The NPE-300 uses a high-performance 262.5-MHz R7000 RISC processor and can support up to 256 MB of memory, providing superior performance for both enterprise and service provider applications that require processor-intensive services. Network layer services such as traffic management, security, and QoS benefit significantly from the high performance of NPE-300.

A Cisco 7200 VXR router equipped with an NPE-300 can support up to six high-speed port adapters and can also support higher-speed port adapter interfaces including Gigabit Ethernet and OC-12 ATM. The NPE-300 uses synchronous DRAM (SDRAM) for storing all packets received or sent from network interfaces. The SDRAM also stores routing tables and network accounting applications. There are two

independent SDRAM memory arrays in the system that allow concurrent access by port adapters and the processor. The NPE-300 can be configured with up to 256 MB of processor and packet memory, which is double the 128-MB memory limit on the NPE-200. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/72vxicg/index.htm

PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The multichannel E1 and T1 ISDN PRI port adapters (PA-MC-8E1/120, PA-MC-4T1, PA-MC-8T1, and PA-MC-8DSX1) are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-MC-8E1/120, PA-MC-4T1, and PA-MC-8T1 are single-wide modules that integrate channel service unit (CSU) functionality, data service unit (DSU) functionality, and E1 or T1 channel support into the Cisco router. The PA-MC-8DSX1 is a single-wide module that integrates DS1 DSU functionality and DS0 channel support into the Cisco router.

The PA-MC-8E1/120, PA-MC-4T1, PA-MC-8T1, and PA-MC-8DSX1 provide four or eight independent T1 (100-ohm) or E1(120-ohm) connections via RJ-48C connectors. Each T1 or E1 port adapter can provide up to 128 separate full-duplex High-Level Data Link Control (HDLC) fractional or full T1 or E1 channels. Individual T1 connections of the DSX-1 version of the port adapters can connect to external CSUs, to digital cross connects (DACS), or to any other equipment that uses a DSX-1 interface.

See the following documents for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/4815ds1p/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/5083e1p/index.htm

PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-E3 Multichannel E3 synchronous serial port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). The PA-MC-E3 has one channelized E3 high-speed serial interface that provides access to services at E1 (2.048 Mbps) data rates, transferring data bidirectionally. This port adapter divides the E3 signal stream into 16 E1 lines that can be further divided to the 64-kbps level, up to a total of 128 channels. The PA-MC-E3 complies with Consultative Committee for International Telegraph and Telephone/International Telecommunication Union (CCITT/ITU) G.703 physical layer standards and CCITT/ITU G.751 for E3, G.742 for E2, and G.704 and G.706 for E1 fault and alarm detection and response actions. The E1 lines can be configured as channelized, fractional, and unframed. PRI ISDN will be supported in a later release. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/pamce3.htm

PA-MC-T3 Multichannel T3 Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-T3 Multichannel T3 port adapter is available on Cisco 7200 series routers, second-generation Versatile Interface Processor (VIP2) in Cisco 7500 series routers, and the Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-MC-T3 has one channelized T3 high-speed serial interface that provides access to services at T1 data rates, transferring data bidirectionally.

This port adapter divides the T3 signal stream into 28 T1 lines that can be further divided into the 64 kbps level, up to a total of 128 channels. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/pamct3.htm

RFC 1483 Bridged PVC Encapsulation

Platforms: Cisco 12000 series

Using RFC 1483 bridged permanent virtual connection (PVC) encapsulation on a Cisco 12000 series router, a Gigabit Switch Router (GSR) ATM interface can be connected directly to a Catalyst 5000 series switch ATM port. When configuring the GSR ATM interface, you must create a new 1483 half-bridge PVC connection using a multipoint subinterface. Only one PVC half-bridge connection per subinterface is allowed; however, other non-PVC connections (SVC or nonbridged PVC) are allowed on the subinterface. Configure an MTU size of 1500 so that the Catalyst switch will not drop packets. Full bridging in the GSR is not supported. Also note that Ethernet format is supported. IEEE 802.3 format is not supported at this time.

Secure Shell Version 1

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. Two versions of SSH are available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH server feature enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS will work with publicly and commercially available SSH clients.

Before SSH, security was limited to Telnet security. SSH allows strong encryption to be used with Cisco IOS authentication.

Tag Switching

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Tag switching is a novel approach to network layer packet forwarding. The two main components of the tag switching architecture are forwarding and control. Forwarding is accomplished using simple label-swapping techniques, while the existing network layer routing protocols plus mechanisms for binding and distributing tags are used for control. Tag switching can retain the scaling properties of IP and can help improve the scalability of IP networks.

Important Notes

12.0(7)S1 Release

After Cisco IOS 12.0(7)S software was released, two defects were discovered, CSCdp17433 and CSCdp31259, that were severe enough to require a rebuild of the software. Cisco IOS Release 12.0(7)S has been deferred and replaced with Cisco IOS Release 12.0(7)S1. For further details, please refer to the field notice *Cisco IOS 12.0(7)S1* located at the following URL:

http://www.cisco.com/warp/customer/770/fn8571_12031999.shtml

Unicast RPF—New ACL Bypass and Logging Functions

Access Control List (ACL) functions have been added to the Unicast RPF feature that will allow new logging capability and exceptions to Unicast RPF checks. Interface-specific counters for Unicast RPF drops have been included in **show ip interface**.

The **ip verify unicast reverse-path** [*acl*] command enables the checking of source IP addresses in packets that are being Cisco Express Forwarding (CEF) or distributed Cisco Express Forwarding (dCEF)-switched. If the source IP address is known to be reachable through the interface from which the packet was received, the packet is forwarded. Otherwise, the packet is dropped and counted once on the interface over which the packet was received and once globally. The interface counter is part of the **show ip int** *int* output, and the global counter is part of the **show ip traffic** output.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This section only contains open caveats for the current Cisco IOS 12.0 S maintenance release.

Because Cisco IOS Release 12.0 S is based on Release 12.0, many caveats that apply to Release 12.0 will apply to Release 12.0 S. For information on severity 1 and 2 caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*. It is located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

- Open Caveats—Release 12.0(10)S, page 32
- Resolved Caveats—Release 12.0(10)S, page 40
- Resolved Caveats—Release 12.0(9)S, page 45
- Resolved Caveats—Release 12.0(8)S, page 49
- Resolved Caveats—Release 12.0(7)S, page 50
- Resolved Caveats—Release 12.0(6)S, page 52

Open Caveats—Release 12.0(10)S

This section describes possibly unexpected behavior by Release 12.0(10)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdk69452

  In rare instances, a configuration that uses regular expressions might cause the regular expression-matching routine to enter into an infinite loop that results in a software-forced reload.

  Workaround: Replace all occurrences of the regular expression (_.+)* with (_[0-9]+)*.

- CSCdm24072

  A Cisco 7500 series router with a Route Switch Processor 8 (RSP8) will reload with a watchdog timeout if you enter the **memory cache-policy processor uncached** command. There is no workaround.

- CSCdm70663

  A Cisco 7500 router that is running Cisco IOS Release 12.0 T and has a Versatile Interface Processor (VIP) might reload if you enter the **show line** command while several Telnet and if-con sessions are running concurrently. This condition occurs because using if-con to get information from the VIP is unsupported.

  Workaround: Obtain statistics from a VIP using the **show controllers vip** *slot# command* command.

- CSCdm71776

  If the **slave auto-sync config** global configuration command is enabled on a High System Availability (HSA) system and you enter the **config-register** global configuration command followed by the **write memory** command, the master system configuration register will be set to change on the next reboot, but the slave configuration register will not be set to change.

  Workaround: Enter the **slave sync config** privileged EXEC command, which will update the slave configuration register for the next reboot.

- CSCdp19943

  The online insertion and removal (OIR) of a slave Route Switch Processor (RSP) might cause the master to exhibit RSP-3-BADBUFHDR messages. There is no workaround.

- CSCdp82691

  A Cisco 7500 series router that is running Cisco IOS Release 12.0(7)S1 might experience a bus error exception with the trace pointing at vip_ip_fib_flow_fs.

  Workaround: Disable Cisco Express Forwarding (CEF)-based distributed NetFlow switching.

- CSCdp93974

  Configuring a large number of Virtual Private Networks (VPNs) on a Cisco 7500 series Route Switch Processor (RSP) with a large number of channelized interfaces might result in a FIBDISABLE message. This message indicates that the RSP has not received a FIB keepalive from the line card within the expected length of time. When this situation occurs, the RSP functions as if the interprocess communication (IPC) mechanism has failed and disables Cisco Express Forwarding (CEF) on that line card.

  Workaround: Disable distributed switching.

- CSCdr03002

  A Cisco router might reload if you change the traffic-shaping configuration on an interface while traffic is flowing through that interface.

  Workaround: Shut down the interface, and then make the traffic-shaping configuration changes before bringing the interface back up.

Interfaces and Bridging

- CSCdp71620

  A Cisco Packet OC-3 Interface Processor (POSIP) might reload with a bus error. There is no workaround.

- CSCdp81786

  A Cisco 7500 series router that is running Packet-over-SONET (POS) IP with distributed Cisco Express Forwarding (dCEF) enabled might experience repeated reloads and display the following traceback:

  ```
  Traceback=0x60185954 0x60186DB8
  Enter hex value: 0x60185954 0x60186DB8 0x60185954:posdw_rx_interrupt(0x60185418)+0x53c
  0x60186DB8:posdw_wrapper(0x60186d80)+0x38
  ```

  Workaround: Disable dCEF.

- CSCdp97805

  When a bad transmit packet is generated and sent to the Channelized T3 (CT3) interface, the packet might cause the address of the transmit queue accumulator (txacc) value to not increment correctly for the CT3 interface. In this situation, the output eventually becomes stuck when the txacc value reaches zero.

  Workaround: Configure the CT3 interface with the **tx-queue-limit** *5* interface configuration command to restore the txacc value for the effected CT3 interface.

IP Routing Protocols

- CSCdp29651

  After being upgraded, routing tables might contain Border Gateway Protocol (BGP) routes that are not in the BGP table. This situation seriously impacts connectivity in the network. There is no workaround.

- CSCdp95210

  Under rare circumstances, a link-state advertisement (LSA) on a neighboring router might get stuck in MAXAGE state and not be deleted. In this situation, the LSA cannot be originated again on this router, which might cause the route to become unavailable or cause packets to take another route that is less than optimal. This situation has been seen to occur when an OSPF neighbor runs out of memory and OSPF tables are corrrupted.

  Workaround: Restart the OSPF process by entering the **clear ip ospf proc** command.

- CSCdr10077

  A Cisco router that is running Cisco IOS Release 12.0(9.5)S might reload with a bus error in OSPF while OSPF is attempting to delete an old path. There is no workaround.

Miscellaneous

- CSCdm64207

  If the clock rate or bandwidth value of an interface has been changed from the default value, and Versatile Interface Processor (VIP)-based Class-Based Weighted Fair Queueing (CBWFQ) is enabled on the interface, the CBWFQ weights are chosen based on the default bandwidth of the interface instead of the modified bandwidth. There is no workaround.

- CSCdm69594

  The interface delay metric is set incorrectly for port channel interfaces where one or more Gigabit Ethernet interfaces are grouped into a channel. The delay for a single Gigabit Ethernet interface is 10 microseconds. The delay for a port channel made up of one or more Gigabit Ethernets is 100 microseconds. The incorrect setting might seriously impact routing protocols that use interface delay as part of the metric (for example, Enhanced Interior Gateway Routing Protocol (EIGRP)), and might cause the routing protocol to take a route through a single interface over a route through a port channel.

  Workaround: Manually configure an appropriate delay under the port channel interface by entering the **delay** *tens of microseconds* interface configuration command.

- CSCdm78020

  Performance OC-48 POS and QOC-12 POS line cards might not fragment Multiprotocol Label Switching (MPLS) packets or send Internet Control Message Protocol (ICMP) messages if the DF bit is set in the header of the IP Payload of MPLS packets requiring fragmentation.

  Workaround: Change the maximum transmission unit (MTU) on the interface to be less than or equal to the MTU on the next hop.

- CSCdm78372

  A Cisco 7200 series router might pause indefinitely if the E1/T1 port adapter channels that are configured for hardware compression are deconfigured while there is traffic. There is no workaround.

- CSCdm79087

  When hardware compression is configured on an E1/T1 port adapter interface, the hardware compression will not take effect until after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface. There is no workaround.

- CSCdm79499

  Under some circumstances, a Packet-over-SONET (POS) interface with Frame Relay encapsulation might have an incomplete adjacency. There is no workaround.

- CSCdm84026

  If you copy an image from disk0: to slot1:, you can boot from the image in disk0: but not from the image in slot1:. If you try to boot from the image in slot1:, you will receive an error message with an incorrect checksum. There is no workaround.

- CSCdp09791

  If you upgrade a Cisco 7200 series router from the Cisco IOS Release 11.1 CC to Cisco IOS Release 12.0(4)S, the Simple Network Management Protocol (SNMP) counters for serial (T1) interfaces might produce unreliable data. The router might experience traffic rates over 10 to 15 Mbps for T1 interfaces.

All serial T1 interfaces will exhibit this behavior. Serial interfaces on a 4xT1 PA (73-1389-05) and on a Channelized 8xT1 PA (73-2488-05) might also exhibit this behavior. There is no workaround.

- CSCdp13747

  This condition occurs with two Cisco 12000 series Gigabit Switch Routers (GSRs) that are running Cisco IOS Release 12.0(8.5)S and are connected back-to-back with a CHOC-12/STM-4 IR-SC STS3/STM1 line card. If **no keepalive** is enabled on the CHOC-12/STM-4 IR-SC STS3/STM1 line card interface, and a reload is initiated simultaneously on the two back-to-back routers, the CHOC-12/STM-4 IR-SC STS3/STM-1 interface will appear to be up, but no traffic will travel across the interface.

  Workaround: Be sure that **keepalive** is enabled on the CHOC-12/STM-4 IR-SC STS3/STM-1 interface.

- CSCdp17238

  There is no way to poll the line card CPU statistics with Simple Network Management Protocol (SNMP).

  Workaround: Perform the following steps:

  – Use Telnet to reach the router.

  – Attach the appropriate line card.

  – Enter the **show processes** [**cpu**] EXEC command.

- CSCdp20755

  In Cisco IOS Release 12.0 S, fast-switching policy-routed traffic might break when policy-routed fast switching is configured on the tunnel interface itself.

  Workaround: Enter the **tunnel sequence-datagrams** interface configuration command on all tunnel interfaces.

- CSCdp22959

  On a Cisco 7200 VXR series router that is running Cisco IOS Release 12.0(6)S, the structure that holds a pointer to a pak header might get corrupted and cause the router to reload. There is no workaround.

- CSCdp23658

  Tunnels that are configured for multicast routing and multicast distributed switching might cause a Cisco 12000 series Gigabit Switch Router (GSR) to reload with a bus error.

  Workaround: Do not configure the tunnel for multicast routing by entering the **ip pim** {**foo-mode**} interface configuration command. If you must configure the tunnel interface for multicast routing, enter the **no ip mroute-cache** interface configuration command.

- CSCdp26186

  On a Cisco 12000 series Gigabit Switch Router (GSR), per-subinterface features on Frame Relay subinterfaces are not supported by CHOC12, POSIP, and DS3 line cards. There is no workaround.

- CSCdp33875

  More than 50 milliseconds of traffic is lost when a protection fiber is cut. Although Dynamic Packet Transport (DPT) is intended to protect traffic against fiber failures in fewer than 50 milliseconds, this timing is not yet met for all traffic patterns. There is no workaround.

- CSCdp38365

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running gsr-k4p-mz.with Cisco IOS Release 12.0(6.5)S might reload with a bus error at PC 0x60477E30, address 0xDEADBEF3. There is no workaround.

- CSCdp39983

  A Cisco Versatile Interface Processor (VIP) 2/40 that is running Cisco IOS Release 12.0(7)S might reload in find_next_non_zero_acl_elem. There is no workaround.

- CSCdp39985

  A Versatile Interface Processor (VIP) 2/40 that is running Cisco IOS Release 12.0(7)S might experience a memory corruption that results in a software-forced reload. There is no workaround.

- CSCdp40366

  If a CHOC-12/STM-4 IR-SC STS3/STM-1 line card interface on a Cisco router running Cisco IOS Release 12.0(8.5)S is configured for PPP encapsulation, and a reload is initiated on the router, you will need to enter the **shut** command followed by the **no shut** command on the CHOC-12/STM-4 IR-SC STS3/STM-1 interface. There is no workaround.

- CSCdp40493

  A Cisco 12000 series Gigabit Switch Router (GSR) might exhibit the following message while booting:

  ```
  %SYS-2-INTSCHED: 'idle' at level 1 -Process= "Exec", ipl= 1, pid= 2
  ```

  There is no workaround.

- CSCdp44950

  With distributed Cisco Express Forwarding (dCEF) enabled on a VIP2-50 Versatile Interface Processor and a PA-2 Fast Ethernet Inter-Switch Link (FEISL) port adapter, the following tracebacks are received:

  ```
  %SYS-5-CONFIG_I: Configured from console by console
  %IPC-5-INVALID: Sequence Structure port index=0x0
  -Traceback= 60357518 60357EA0 6015BDB8 6023F2CC 6023F2B8
  ```

  These messages are reported repeatedly until dCEF is disabled, and the VIP/PA combination is unplugged and reinserted. This problem does not occur with a PA-FE. There is no workaround.

- CSCdp48087

  A Cisco 12000 series Gigabit Switch Router (GSR) with dual gigabit route processors (GRPs) might exhibit the following error message if the primary GRP reloads and the secondary GRP takes over:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 2: No window > message, LC to RP IPC is
  non-operational
  ```

  This error message will disable the line card, and the line card must be reloaded manually before it comes back online. There is no workaround.

- CSCdp49781

  If the Cisco OC-12/STM-4 Packet-over-SONET/Synchronous Digital Hierarchy (SDH) line card encounters a hardware error, the error recovery software does not recover properly. In this situation, the line card must be reloaded. There is no workaround.

- CSCdp51945

  On a Cisco 7500 series RSP router, an Simple Network Managment Protocol (SNMP) get query of cieNumberOfConnections (.1.3.6.1.4.1.9.9.52.1.3.1.0) results in spurious access. This condition can also lead to a memory leak in the IP SNMP process. There is no workaround.

- CSCdp56613

  When fast switching an IP frame that is fewer than 46 bytes in length to an ATM interface, the router always sets the length in the ATM adaption layer 5 (AAL5) header to 54 bytes even though the length should be equal to the IP frame length plus the length of the AAL5 header, which is 8 bytes. There is no workaround.

- CSCdp58522

  Cisco OC-48c/STM16c and Cisco QOC-12 line cards for the Cisco 12000 series Gigabit Switch Router (GSR) are not differentiating outgoing traffic by protocol type. There is no workaround.

- CSCdp58964

  A Cisco router that is running Cisco IOS Release 12.0(7)S or Cisco IOS Release 12.0(8)S will disable Cisco Express Forwarding (CEF) with a FIB-3-NOMEM failure even though there appears to be plenty of memory. There is no workaround.

- CSCdp64182

  A Cisco 7000 series router might reload when a Multiprotocol Label Switching/Terminal Equipment (MPLS/TE) tunnel is deleted. There is no workaround.

- CSCdp64229

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(7)S1 might experience a condition where “FIB NDB msg chunks” is using up all the memory. This condition is likely to occur when the gigabit route processor (GRP) is trying to send interprocess communication (IPC) messages to the line card and that line card is not functioning properlly, which causes the GRP to queue the packets indefinitely. This condition can also result in the slow failure of the router because of leaking memory. There is no workaround.

- CSCdp67797

  A Gigabit Ethernet connection might not function properly and be unable to see the MAC address of a Gigabit Switch Router (GSR) across the link.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command, and reinsert the Gigabit Interface Converter (GBIC).

- CSCdp69135

  On a Cisco 12000 series Gigabit Switch Router (GSR), the counters in the **show tag forwarding** command might not display the correct results. There is no workaround.

- CSCdp74436

  Entering the **write memory** command simultaneously on both the console and a vty might cause a Cisco router to pause indefinitely. The **write memory** command should not be entered simultaneously on different vtys. There is no workaround.

- CSCdp78089

  When the environmental values for voltage get corrupted and a Cisco 12008 Gigabit Switch Router (GSR) has all slots at the critical warning level, entering the **show run** command causes the router to shut down. This condition is more likely to occur after a router has been up and running for several weeks or more. There is no workaround.

- CSCdp78912

  A Cisco 12000 series Gigabit Switch Router (GSR) OC-12 line card might reload with the following traceback:

  ```
  lc_bma_error_analyze+0x4f8 lc_error_interrupt_handler+0x44 bflc_intr_dispatch+0x88]
  ```

  There is no workaround.

- CSCdp79049

  On a Cisco router where a CT3 port adapter is used as an outgoing interface, the router from the remote side of the router with the CT3 port adapter cannot ping a router on the other side of the router with the CT3 port adapter until the queueing strategy is changed.

  Workaround: Change the queueing strategy from weighted fair queueing (WFQ) to first-in first-out (FIFO) or from FIFO to WFQ.

- CSCdp82244

  On a Cisco 7200 series router, the serial drivers may cause a memory leak when a reparented packet is sent. There is no workaround.

- CSCdp82562

  When a new Cisco IOS image is being loaded on a Cisco router, some line card slots might fail and display “state =Not Yet Determined” or “state =Mbus Agent Downloading.”

  Workaround: Power off and then power on the slots in question by entering the **test mbus power** *slot* **off** command followed by the **test mbus power** *slot* **on** command. This action foreces a reset and another download of the MBus agent RAM code.

- CSCdp85414

  The contents of a directory listing on a Cisco 7500 series Route Switch Processor (RSP) might appear intermittently. There is no workaround.

- CSCdp90558

  When the **atm pvp** interface configuration command is entered on a Cisco 12000 Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(8.5)S or higher releases, two F4 Operation, Administration, and Maintenance (OAM) virtual circuits (VCs) are automatically created. There is no workaround.

- CSCdp90696

  If an interface card is replaced online through an online insertion and removal (OIR) with a card of a different type, the Hot Standby Router Protocol (HSRP) configuration might not be carried over to the new card.

  Workaround: Remove HSRP from the configuration before removing the card.

- CSCdp92691

  CPU utilization might increase dramatically after you configure an 802.1Q trunk on a Cisco 7500 series Route Switch Processor (RSP). The CPU load might jump from 10 to 15 percent without the trunk to 25 to 35 percent with the trunk enabled. Enabling the 802.1Q trunk also removes the **ip route-cache distributed** command from the configuration and causes the interface to stop being autonomously switched. There is no workaround.

- CSCdp93008

  The gigabit port on a Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(8)S might stop receiving packets and exhibit the following error message:

  ```
  SLOT 4:5d00h: %LCGE-3-SOP: Rx SOP. (source=0x40, halt_minor0=0x2)
  SLOT 4:5d00h: %GSR-3-INTPROC: Proc stack: 40174F70
  -Traceback= 4013E004 40241B00 400BA944
  ```

  The port reports that it is in an up/up state, but it does not respond to pings.

  Workaround: Restart the line card.

- CSCdp93988

  A Cisco 7200 series router might reload because of memory corruption and exhibit the following error message:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 520 bytes failed fr om 0x60395028, pool
  Processor, alignment 0 -Process= "Pool Manager", ipl= 4, pid= 4
  -Traceback= 603C84DC 603C9F88 60395030 603D4578 603C2C34 603C2C20
  ```

  There is no workaround.

- CSCdp96382

  A Cisco 7500 series route switch processor (RSP) might experience an unexpected reload when a file is copied simultaneously to disk0: from two vtys. There is no workaround.

- CSCdr00694

  A Cisco router that is running Cisco IOS Release 12.0(9)S or later releases might experience problems if you attempt to format, delete, or squeeze slot0: immediately after the **show version** command is entered or immediately after the router reloads. This is a flash timing-related issue, and subsequent commands that you enter will not be effected. There is no workaround.

- CSCdr01649

  A Versatile Interface Processor (VIP) might reload in chunk_free while it is processing a FIB. There is no workaround.

- CSCdr07940

  A Cisco router might reload if a load-sharing route changes while a **show ip cef detail** command is waiting at the More prompt displaying that route. There is no workaround.

- CSCdr08160

  Under heavy traffic on the outbound side of a SRP port adapter, packets will get queued on holdq if the TX ring is full. These packets will be accounted as process switched instead of route-cache switched. There is no workaround.

- CSCdr09895

  Under heavy traffic, a PA-A3 port adapter might experience a SAR0 reload. If this condition occurs on a Cisco 7200 series router, you must reload the router to recover normal operation. On a Cisco 7500 series RSP, this situation might result in commands from the RSP to the port adapter failing, but the port adapter should be able to recover without a router reload. There is no workaround.

TCP/IP Host-Mode Services

- CSCdk69541

  If a Cisco router is running Cisco IOS Release 12.0 S and the "ip tcp path-mtu-discovery" feature is enabled, the router might experience a TCP timer problem and reload. This situation occurs when the router is experiencing a heavy load that includes a large number of Border Gateway Protocol (BGP) peer routers exchanging routing packets.

  Workaround: Disable the **ip tcp path-mtu-discovery** feature by entering the **no ip tcp path-mtu-discovery** command.

Wide-Area Networking

- CSCdp58690

  A Cisco 7507 router that is running Cisco IOS Release12.0(8)S might experience a Route Switch Processor (RSP) watchdog timeout in pim/atm/avl_get_next. The affected system image file is slot0:rsp-pv-mz.120-8.S.bin. There is no workaround.

- CSCdp65239

  The input queue on a Cisco 7500 series router might show 76/75, which can result on the line going down on a High-Speed Serial Interface (HSSI) port adapter even though the VIP console shows that the queue is empty and the line protocol is up. This condition only occurs when PPP encapsulation is enabled.

  Workaround: Move the card to a new slot, change to High-Level Data Link Control (HDLC), or reload the router.

Resolved Caveats—Release 12.0(10)S

All the caveats listed in this section are resolved in Release 12.0(10)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdp45379

  A Cisco 7200 series router with an NPE-300 network processing engine installed might not boot up when certain Cisco IOS Release 12.0(5)XE3 subset images are installed. The router will pause indefinitely in the early stage of booting up, and a power cycle is required to resume. For systems set for auto boot, you will need to enter the **break** command to abort the boot process and break out to the ROM monitor before the 12.0(5)XE3 image is launched for execution. You will then need to either modify the software configuration register to revert to a manual boot of some other known good image, or you will need to switch the PCMCIA flash card with a known good image in case the system is set for a default image boot from the slot0: PCMCIA card. There is no workaround.

Interfaces and Bridging

- CSCdm06860

  Cisco IOS Release 11.1(24)CC might return a wrong value for MIB object cardType for PA-POSSW-MM/SM port adapters due to the Simple Network Management Protocol (SNMP) agent in the Cisco IOS Release 11.1(24)CC. Values for PA-POSSW 401 are returned instead of values for PA-POSSW 564 and PA-POSSW 564. There is no workaround.

- CSCdm11933

  CT3/CE3 port adapters on a Cisco 7200 series router might drop TX packets under bursts of heavy traffic instead of putting them in a hold queue if the number of outstanding transmit packets temporarily exceeds the number specified by the TX limit. There is no workaround.

- CSCdp60859

  When a channel on a CT3/CE3 port adapter is continually overstressed by traffic, other nonstressed channels might experience some transmit packet drops. There is no workaround.

- CSCdp99579

  Configuring an Async interface in any Cisco 7500 series Route Switch Processor (RSP) will prevent the proper parsing of interface name for CT3/CE3 port adapters.

  Workaround: Deconfigure any Async interface, and then write the configuration to NVRAM and reload the router. Or, you can move the VIP from slot 0 to another slot.

- CSCdr00681

  A Channelized T3 Interface Processor (CT3IP) driver on a Cisco 7500 series router might leak particles from the receiving side, which results in the CT3IP seeing all serial interfaces as flapping after a few hours. This situation can be observed by checking input errors in the **show interface** output. There is no workaround.

IP Routing Protocols

- CSCdp18787

  A Cisco router that has tag switching enabled and is running Cisco IOS Release 12.0(5)T might reload if a tag advertisement appears in a certain time window when a related routing update takes place. An ATM interface transition might cause this condition. There is no workaround.

- CSCdp43545

  Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels might bounce under certain conditions if there is a very heavy traffic load on a Gigabit Switch Router (GSR) line card. This condition has been observed when a routing loop is present and the card is generating Internet Control Message Protocol (ICMP) “TTL expired” messages, and when the card is used as the data sink for ICMP ECHO requests from a traffic generator. There is no workaround.

- CSCdp72309

  A Cisco router that is running Cisco IOS Release 12.0(8)S might reload with a bus error at ospf_default_networkupdate after links flap or the **clear ip bgp** {*****} EXEC command is entered. There is no workaround.

- CSCdp85688

  When a Multicast Routing Monitor (MRM) Test Sender is instructed by an MRM Manager to send test packets out of all interfaces that are configured for multicast routing, which is the default option, the MRM might experience a leak in the small buffers.

  Workaround: Configure the MRM Manager with the **senders** {**access-list-number** | **access-list-name**} [*target-only*] command.

Miscellaneous

- CSCdm64005

  A PA-T3 port adapter might exhibit a timing problem resulting in dropped packets. There is no workaround.

- CSCdm75813

  Writing to an AT Attachment (ATA) device might cause the device to become unusable and result in an “ATA_Status time out waiting for 1” error message.

  Workaround: Reload the Cisco IOS software.

- CSCdm94333

  In APS configurations in which working and protect interfaces are in different routers, if a direct link between the two routers fails and is replaced by an indirect IP route, then the router containing the working interface will have no IP address for the router that is housing the protect interface. The resulting communications failure might result in both interfaces being deselected or both interfaces being selected. There is no workaround.

- CSCdp16749

  When Turbo Access Control Lists (Turbo ACLs) are enabled when the **access-list compiled** command is entered, reloading or reinstalling multiple access lists might cause a reload or an alignment error. This condition is most likely to occur on Cisco 12000 series Gigabit Switch Router (GSR) line cards, and usually occurs when many access list lines are being copied into the configuration.

  Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

- CSCdp34046

  If an output rate limit is configured on a non-Versatile Interface Processor (VIP) interface (for example, AIP or FIP) on a Cisco 7500 series Route Switch Processor (RSP) with Cisco Express Forwarding (CEF) enabled, packets cannot be switched out of that interface.

  Workaround: Disable CEF.

- CSCdp46780

  After the primary clock scheduler card (CSC) has been removed, a Cisco OC-48/STM-16 Packet-over-SONET/SDH line card might not recover from being switched to the secondary CSC card and report error messages.

  Workaround: Reload the line card.

- CSCdp54069

  A Cisco PA-2T3 port adapter might show increasing overruns in the **show interface** command output display when one of the two ports is in a DOWN state.

  Workaround: Configure the **serial restart** *0* command on the DOWN interface, or put the DOWN port in ADMIN SHUT state.

- CSCdp54813

  A Cisco 7500 series router will often reload when switching onto an IP tunnel if sending to the tunnel destination involves Multiprotocol Label Switching (MPLS) label imposition. There is no workaround.

- CSCdp61411

  A Cisco 7200 series router might receive a large number of alignment errors in the Cisco Express Forwarding (CEF) FastPath, which causes severe performance degradation.

  Workaround: Disable CEF by entering the **no ip cef** global configuration command.

- CSCdp64140

  Two Cisco 12000 series Gigabit Switch Routers (GSRs) that are connected by a Gigabit Ethernet connection might exhibit “GRP-4-CORRUPT” error messages when one of the routers is upgraded to Cisco IOS Release 12.0(8)S. There is no workaround.

- CSCdp71623

  Packets that have been padded by the previous hop that are received by a Versatile Interface Processor (VIP) Ethernet/Fast Ethernet/Gigabit Ethernet router might be dropped if those packets are supposed to be processed by the Route Processor rather than by the VIP.

  Workaround: Disable distributed Cisco Express Forwarding (dCEF) on the ingress interface.

- CSCdp72483

  If a Cisco 12012 or Cisco 12016 Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(7)S or 12.0(8)S with dual gigabit route processors (GRPs) experiences a failover, full bandwidth line cards might not boot correctly, and the router will exhibit a "MBUS-3-INSUFF_BW" message. A microcode reload is needed to make the line cards function properly again. This condition is rare.

  Workaround: If you are upgrading a GSR with dual GRPs and full fabric line cards to Cisco IOS Release 12.0(7)S or 12.0(8)S, check that all line cards initialize correctly after a dual GRP failover. You can test this condition by entering the **redundancy force-failover** EXEC command. If the check fails, then you will need to use a different image.

- CSCdp74038

  On Gigabit Ethernet line cards, 802.1Q packets that are 512 bytes and larger might get dropped on input. There is no workaround.

- CSCdp74616

  On the Cisco OC-48c/STM-16c and Cisco QOC-12 line cards for the Cisco 12000 series Gigabit Switch Router (GSR), there is a timing problem during initialization that might cause the line cards to reload if Multiprotocol Label Switching (MPLS) packets are received before the initialization is complete. There is no workaround.

- CSCdp78781

  A memory leak in a Cisco 12000 series Gigabit Switch Router (GSR) line card in the Cisco Express Forwarding (CEF) line card statistics might not clear quickly and exhibit high memory utilization. In this situation, the router exhibits the following stack trace:

  ```
  glc1-lc-m.120-8.3.S.symbols read in Enter hex value: 400A0314 400A1DC0 4027D3EC
  40279794 4009AA6C 4009AA58 0x400A0314:report_malloc_failure(0x400a02d4)+0x40
  0x400A1DC0:malloc(0x400a1aa4)+0x31c
  0x4027D3EC:fib_collect_frpvc_rxstats(0x4027d3b4)+0x38
  0x40279794:fib_lc_stats_background(0x402796c0)+0xd4
  0x4009AA6C:r4k_process_dispatch(0x4009aa58)+0x14
  0x4009AA58:r4k_process_dispatch(0x4009aa58)+0x0
  ```

  Workaround: Limit the size of the access lists, or do not use access lists.

- CSCdp80282

  Packets that are sourced from a Cisco 7500 series router with Multiprotocol Label Switching (MPLS) enabled and exit the router through a T1 or Channelized T1 connection will not be sent correctly. Other traffic traversing the router is not affected. There is no workaround.

- CSCdp82125

  A Route Switch Processor (RSP)-based router with one or more Versatile Interface Processors (VIPs) that is running Cisco IOS Release 12.0 S (or any image with tag support) might experience a memory leak with Cisco Express Forwarding (CEF) and tag switching enabled and the **no ip route-cache distributed** command configured. This memory leak can be detected by repeatedly entering the **show process memory** | **include OSPF** command on the RSP console or vty.

  Workaround: Enable distributed CEF instead of CEF, or turn off tag switching.

- CSCdp88204

  If the **tx-ring-limit** command is entered on a Cisco 7500 series Route Switch Processor (RSP) that is running Cisco IOS Release 12.0 S, the router might experience a NULL pointer access, and the Versatile Interface Processor (VIP) might reload. This situation occurs during line flapping and when the router is being configured. There is no workaround.

- CSCdp89965

  Under rare circumstances, a tunnel might have a drop adjacency on the line card while simultaneously having a valid adjacency on the on the Route Processor (RP).

  Workaround: Enter the **clear cef linecard** command to download the correct information to the line card.

- CSCdp86111

  When Cisco Express Forwarding (CEF) is configured as part of a large configuration (typically with access lists), following boot traffic that is directly addressed to the interfaces of a router might not be received. This condition can be observed on enabled interfaces where IP interfaces appear to be up, but the CEF interfaces are down.

  Workaround: Perform one of the following steps.

  – Boot without CEF enabled.

  – Disable and then re-enable CEF.

  – Enter the **no shutdown** command on each of the interfaces that are effected.

- CSCdp91476

  The fix for this DDTS adds a 32-bit overflow counter that can be used in conjunction with the existing 32-bit counter to get the full 64-bit value. In addition, a true 64-bit counter has also been added to the MIB. SNMP v1 managers and Cisco IOS Release 11.X releases are limited to using the 32-bit overflow counters; the 64-bit counters will be invisible to them. SNMP v2 and SNMP v3 managers that are running on top of Cisco IOS Release 12.X releases will be able to use either the 32-bit overflow counters or the 64-bit counters.

- CSCdr01116

  A Cisco 12000 Gigabit Switch Router (GSR) that is configured for 802.1Q trunking over a Gigabit Ethernet interface might not form OSPF or EIGRP adjacencies when **ip route-cache flow** is configured on the main Gigabit Ethernet interface.

  Workaround: Configure and use Gigabit Ethernet subinterfaces or disable flow switching by entering the **no ip route-cache flow** command.

TCP/IP Host-Mode Services

- CSCdp63037

  Border Gateway Protocol (BGP) sessions on Cisco 12000 series Gigabit Switch Router (GSR) might fail to send updates when the router establishes passive BGP sessions because of problems with the flow control of BGP and TCP.

  Workaround: Use an inbound Access Control List (ACL) to deny any traffic destined for the port, and always open the session actively.

Wide-Area Networking

- CSCdp51767

  A Cisco 7500 series Route Switch Processor (RSP) with a VIP2-50 Versatile Interface Processor and a PA-A3 port adapter might not react to available bit rate (ABR) explicit rate (ER) congestion marking. In this situation, the output rate of an ABR connection does not decrease upon the reception of a Resource Management (RM) cell with an ER field value that is lower than the CCR value. There is no workaround.

Resolved Caveats—Release 12.0(9)S

All the caveats listed in this section are resolved in release 12.0(9)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdm81049

  If a serial interface is flapping up and down repeatedly, the router might pause indefinitely with a stack trace indicating that it is in usecdelay() as a result of cbus_mci_serial_reset() being called while at interrupt level. This situation rarely occurs.

  Workaround: Enter the **shutdown** interface configuration command on the serial interace that is flapping up and down.

- CSCdp23786

  A Cisco router that is running Cisco IOS Release 12.0(7)T cannot execute boot configuration commands from Flash, and exhibits the following error message:

  ```
  %Error opening nvram:/startup-config (File system is in an inconsistent state)
  ```

  When this message is displayed, no configuration is loaded. If you enter the **copy startup-config running-config** command and then enter the **no shutdown** interface configuration command, the router will come back on line. There is no workaround.

- CSCdp56057

  Cisco 3620 routers and Cisco 3640 routers might exhibit traceback messages after being reloaded. The tracebacks occur because of uninitialized semaphore attempts to become locked. This situation does not affect the router functions. There is no workaround.

- CSCdp57908

  This caveat adds support for a new revision of a hardware component that fixes a previous error. For the benefit of users that have not upgraded to the new hardware, it will also exhibit a warning error message that indicates the old hardware revision.

  Cisco 7200 series routers with NPE-175 or NPE-225 network processing engines must upgrade to Cisco IOS releases that incorporate this change (for example, Cisco IOS Release 12.0(9) and later releases or Cisco IOS Release 12.0(9)S and later releases). Use of older Cisco IOS releases might result in unpredictable malfunctions. Please see the following document for further information:

  http://www.cisco.com/warp/customer/770/fn8611.shtml

IBM Connectivity

- CSCdp09919

  Remote source-route bridging (RSRB) might change frame types. This situation occurs on Cisco routers that are running RSRB where one side of the RSRB is running Cisco IOS Release 11.0 and the other side is running Cisco IOS Release 12.0. The frame that is moving along the source-route translational bridging (SR/TLB) and RSRB bridge will be changed from an Ethernet Type II frame to an IEEE 802.3 Ethernet frame.

  Workaround: Configure the 90-compatible option by entering the **source-bridge transparent** *ring-group pseudo-ring bridge-number tb-group* [*90-compatible*] global configuration command.

Interfaces and Bridging

- CSCdm19573

  A Cisco 7200 series router that is running Cisco IOS Release 11.1(22)CC or Cisco IOS Release 11.1(25)CC with a PA-CT3 might experience problems with local-area transport (LAT) services under the following conditions:

  If you are using transparent bridging with LAT enabled on a serial interface, you might not see LAT services when entering the **show lat service** command, even when the remote link (also using transparent bridging with LAT enabled) is advertising LAT services. There is no workaround.

- CSCdp18313

  A Cisco 7206VXR router that is running Cisco IOS Release 12.0(6.5)T2 and has a network processing engine (NPE)-300 network processing engine might reload with a bus error. There is no workaround.

IP Routing Protocols

- CSCdp26552

  Open Shortest Path First (OSPF) and summary link-state advertisement (LSA) is not installed in the routing table.

  Workaround: Clear the routing table and restart the OSPF process.

- CSCdp30454

  The dataless header register is not working properly in Cisco IOS Release 12.0(7)S. There is no workaround.

- CSCdp39843

  If a Cisco router receives a Resource Reservation Protocol Reserve (RESV) message to refresh a label-switched path (LSP) for which it is the source, and if the RESV message contains a Multiprotocol Label Switching (MPLS) label other than the one previously received, the router will attempt to perform a label change operation. If the label change operation fails, the router might reload while executing the appropriate error handling procedures. This situation rarely occurs. There is no workaround.

- CSCdp57762

  A Cisco router that is running Cisco IOS Release 12.0(05.06)S03 or later releases up to Cisco IOS Release 12.0(8.5)S might not send withdraw requests and not delete the entry from the IP routing table under the following *SOFT RESET* conditions:

- The **neighbor soft-reconfiguration** router configuration command is entered on the router for a particular peer.
- The **route-map** global configuration command is entered to modify attributes.
- There is a used entry and a received-only entry for a given prefix, and the **neighbor filter-list**, **neighbor distribute-list**, or **neighbor prefix-list** router configuration commands or the **route-map** global configuration command is entered to deny this prefix.
- The **soft clear bgp** EXEC command is entered.

Symptoms of this situation include the prefix being present in the Border Gateway Protocol (BGP) table with the received-only path, the prefix remaining in the IP table, and the prefix not being withdrawn from all the other peers to which it has advertised. These symptoms do not occur if both peers are route-refresh capable, soft-reconfiguration inbound is not configured, the filter that you apply does not result in a deny for a prefix, if you do a hard reset, or the soft reconfiguration is done through route-refresh.

Workaround: If you have soft cleared the session after applying the filter, enter the **clear ip bgp** {*} [**soft out**] EXEC command.

Alternate workaround: Upgrade to Cisco IOS Release 12.0(8.5)S.

Miscellaneous

- CSCdk77704

  If you enable fancy queueing on an interface where it is the default, the queueing behavior might not function properly. There is no workaround.

- CSCdp17433

  The Forwarding Information Base (FIB) scanner might not free a locked FIB entry so the FIB path chunks will never be freed, resulting in a memory leak. There is no workaround.

- CSCdp35794

  When Access Control Lists (ACLs) are used, Gigabit and Fast Ethernet line cards might experience data corruption. This situation is likely to happen for non-Address Resolution Protocol (ARP) standard Ethernet style (RFC 826) encapsulation packets.

  When extended or compiled ACLs are used, a Gigabit Switch Router (GSR) with Gigabit Ethernet (GE) or Fast Ethernet (FE) line cards might experience line-card failures or corruption of internal queueing structures. This failure might result in incorrect traffic forwarding behavior for packets received on affected cards.

  This failure will not occur if ACLs are not used. Even when ACLs are configured, the occurrence of this failure is still rare. Conditions that will increase the frequency of the error occurring are the use of compiled access lists, large amounts of traffic with nonstandard Ethernet encapsulations, or the presence of large amounts of ARP traffic.

  Workaround: Reset the card by entering the **microcode reload** [*slot-number*] global configuration command.

- CSCdp38982

  When a first label switch router (LSR) is sending Multiprotocol Label Switching (MPLS) encapsulated IP frames to a second LSR that is removing the last label and sending the resultant IP frame onto an Inter-Switch Link (ISL), then IP packets of less than 44 bytes will be received as cyclic redundancy check (CRC) errors. There is no workaround.

- CSCdp41376

  Multiprotocol Label Switching (MPLS) imposition load balancing adjacency entry updates might cause the Gigabit Switch Router (GSR) performance line cards to reload. There is no workaround.

- CSCdp42529

  A Cisco 7200 VXR router might experience a situation where switched virtual circuits (SVCs) are disconnected intermittently and then recovered after 7 to 20 hours. There is no workaround.

- CSCdp46780

  After the primary clock scheduler card (CSC) has been removed, a Cisco OC-48/STM-16 Packet-over-SONET/SDH line card might not recover from being switched to the secondary CSC card and report error messages.

  Workaround: Reload the line card.

- CSCdp47676

  Under certain timing conditions on some Versatile Interface Processors (VIPs), 2-port High-Speed Serial Interfaces (HSSIs) or PA-2T3s might experience abnormal transmit underruns as indicated by the **show interfaces** EXEC command. There is no workaround.

- CSCdp52926

  Output committed access rate (CAR) might not function properly when running on a non-Versatile Interface Processor (VIP) interface. Traffic does not pass properly through the output interface that is enabled with CAR. There is no workaround.

- CSCdp54813

  A Cisco 7500 series router will often reload when switching onto an IP tunnel if sending to the tunnel destination involves Multiprotocol Label Switching (MPLS) label imposition. There is no workaround.

- CSCdp58615

  A Versatile Interface Processor (VIP) might reload after distributed committed access rate (DCAR) is configured and traffic is present on the VIP interface. The condition returns to normal after the VIP reloads. There is no workaround.

- CSCdp58675

  Received packets that had been padded by the previous hop are corrupted by the Multiprotocol Label Switching (MPLS) distributed Cisco Express Forwarding (dCEF) label imposition code, which will result in IP checksum errors at their final destination or at an intermediate hop, depending on the network configuration.

  Workaround: Disable dCEF globally or on a per-VIP interface basis.

- CSCdp64140

  Two Cisco 12000 series Gigabit Switch Routers (GSRs) that are connected by a Gigabit Ethernet (GigE) connection might exhibit “GRP-4-CORRUPT” error messages when one of the routers is upgraded to Cisco IOS Release 12.0(8)S. There is no workaround.

Wide-Area Networking

- CSCdm56380

  When an ATM switch is not configured, a permanent virtual circuit (PVC) or one of the subinterfaces might be shut down on the other side of the ATM switch, but the Simple Network Management Protocol (SNMP) agent reflects that the subinterface shows the subinterface as being UP(AdminStatus and OperStatus). There is no workaround.

Resolved Caveats—Release 12.0(8)S

All the caveats listed in this section are resolved in release 12.0(8)S. This section describes only severity 1 and 2 caveats.

IP Routing Protocols

- CSCdp15126

  If you enable policy routing on a Fast Ethernet Inter-Switch Link subinterface, the packet that is destined for the next hop is not policy routed. Instead, the packet is sent along the default route. There is no workaround.

Miscellaneous

- CSCdm82546

  The Gigabit Switch Router (GSR) Performance line cards do not have the ability to load balance between IP and tag adjacencies. There is no workaround.

- CSCdp05571

  Entering the **show access-list** [#] command will report statistics for matches to fast Access Control List (ACL) items. Statistics are reported on an item by item basis and appear in parenthesis to right of the item. The statistics reported represent the running sum of matches to the item on all interfaces. This new command output fixes the problem of statistics for ACLs not being displayed in previous releases.

- CSCdp10843

  When disabling distributed Cisco Express Forwarding (dCEF) on a running system, clean up all forwarding entries on the line card and move all incoming packets to the Route Processor (RP). The intent is to leave line card forwarding in the state it would have been in if dCEF had never been enabled in the first place.

  Midpoints for Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnel link-state packets (LSPs) do not get cleaned up when dCEF is disabled so when packets arrive at a Versatile Interface Processor (VIP) with the MPLS labels for these stale midpoint entries, the VIP will not forward these packets correctly.

  Workaround: Reload any line card on which dCEF has been disabled if that line card is, or might be at some point, an incoming interface for an MPLS-TE tunnel LSP.

- CSCdp21343

  Some permanent virtual connections (PVCs) in ATM line cards do not function. The **show atm vc** command indicates that the ATM PVC peak and average rates are zero. The state of any sub-interfaces remain INACTIVE. During a reload when the shut ATM sub-interface is encountered, all subsequent sub-interfaces within that interface will be ignored.

  Workaround: Ensure that the ATM interface is not shut. Enter the **shut** and **no shut** commands on each affected ATM sub-interface.

- CSCdp21424

  Under certain conditions, a Cisco 7200 or 7500 series router with a multichannel E1/T1 port adapter might exhibit the following error message:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=Serial3/0:0
  ```

  There is no workaround.

- CSCdp31259

  Enhanced OC48 Packet-Over-SONET (POS) line cards will not boot correctly if the fabric downloader is upgraded while running affected images. This problem can be triggered by the following commands:

Command	Mode
service upgrade all	configuration
upgrade all all	enabled exec
upgrade fabric-downloader all	enabled exec
upgrade fabric-downloader [slot#]	enabled exec

  The problem causes the line card to boot incorrectly. Changing to a different version of code is required to correctly load the card once the fabric downloader upgrade has been executed. The upgrade will need to be reinstalled after reload.

  Workaround: Do not upgrade the fabric downloader by avoiding the upgrade commands.

- CSCdp31471

  The available bit rate (ABR) feature on PA-A3 does not work. The PA-A3 driver can send and receive forward resource management (FRM) cells but backward resource management (BRM) cells cannot be transmitted. There is no workaround.

Resolved Caveats—Release 12.0(7)S

This section describes possibly unexpected behavior by Release 12.0(7)S. This section describes only severity 1 and 2 caveats.

IBM Connectivity

- CSCdm89688

  A Cisco 7000 series router with two CIP cards that are both running **tn3270-server** might unexpectedly reload with a software forced crash if you remove the **client ip** configuration command. There is no workaround.

Miscellaneous

- CSCdm70554

  A Gigabit EtherChannel (GigE) line card might pause indefinitely in FABL START state when the secondary Gigabit Route Processor (GSR) is in the chassis.

  Workaround: Remove the secondary Gigabit Route Processor (GSR).

- CSCdm72149

  When formatting a PCMCIA card with Cisco IOS Release 12.0 S, the command might fail if you have not formatted your bootflash.

  Workaround: Format your bootflash and try the operation again.

- CSCdm74152

  A Cisco router that is running Cisco IOS Release 12.0(4.6)T through 12.0(5)T might experience problems with fast switching if Cisco Express Forwarding (CEF) is disabled.

  Workaround: Enable Cisco Express Forwarding (CEF), and then disable CEF to remove it from the unwanted interfaces.

- CSCdm77266

  A Cisco 12000 router that is running the "gsr-k4-p" software image in Cisco IOS Release 12.0(5.5)S2 might reload if you simultaneously configure Border Gateway Protocol (BGP) neighbors and static routes and Multicast Source Discovery Protocol (MSDP). There is no workaround.

- CSCdm89160

  After you upgrade the ROM monitor on a Cisco router, the router might not reload properly and exhibit the following error message:

  ```
  *** Cache Error Exception *** Cache Err Reg = 0xa4240560 data reference, primary
  cache, data field error , error on SysAD Bus PC = 0xbfc00e04, Cause = 0x8000,
  Status Reg = 0x30408404 Tiger Masked Interrupt Register = 0x000000ff Tiger
  Interrupt Value Register = 0x0000000c
  ```

  This situation occurs only when the following conditions exist:

  1) The router is running one of the following IOS software images: 11.2(17)GS1; 12.0(5.5)S1 and later versions prior to this fix; 12.0(5.6)S and later versions prior to this fix; or 12.0(6.0.2)S and later versions prior to this fix.

  2) You have manually upgraded the ROM monitor using either the **upgrade rom slot** [**RP-slot#**] command or the **upgrade all all** command. If you used the **upgrade all all** command, answering "yes" when prompted to upgrade the Route Processor (RP) ROM monitor will cause this situation to occur.

  Workaround: Do not upgrade the ROM monitor.

- CSCdp00618

  A Route/Switch Processor (RSP) might reload while unprovisioning a channelized interface under heavy traffic. There is no workaround.

Resolved Caveats—Release 12.0(6)S

This section describes possibly unexpected behavior by Release 12.0(6)S. This section describes only severity 1 and 2 caveats.

IP Routing Protocols

- CSCdk70273

  If there are more than 31 OSPF interfaces, flooding does not work, starting from the 32nd OSPF interface. There is no workaround.

- CSCdm34431

  An RSP4 Route/Switch Processor that is running Cisco IOS Release 12.0(3.6)T or 12.0(4)T might reload with the following error message if you issue the **copy tftp running** command to update the configuration while the Versatile Interface Processor (VIP) or Route/Switch Processor (RSP) is under a heavy traffic load:

  ```
  ipfib_policy_forward vip_ip_fib_flow amdfe_rx_interrupt s_amdfe_check
  ```

  This situation occurs when the RSP is running with a VIP2-50 Versatile Interface Processor, a Fast Ethernet port adaptor, and PA-A3 and is configured with distributed Cisco Express Fowarding (dCEF), policy routing, and NetFlow.

  Workaround: Avoid reloading the configuration with the **copy tftp running** command.

- CSCdm51092

  A Cisco router might reload if you enter the same **no ip msdp mesh-group** *foo peer-address* command twice. There is no workaround.

- CSCdm59659

  When “debug ip icmp” is enabled on a line card in a Cisco 12000 series Gigabit Switch Router (GSR), it cannot be disabled. There is no workaround.

- CSCdm60244

  A Cisco router might reload if you perform a router_id change or issue the **clear ip bgp** {*****} command when Multicast Border Gateway Protocol (MBGP) is enabled.

  Workaround: Avoid issuing the **clear ip bgp** {*****} command or changing router_id.

- CSCdm94032

  Border Gateway Protocol (BGP) routes might not be withdrawn if deterministic med is not enabled.

  Workaround: Configure deterministic med by issuing the **bgp deterministic med** command.

ISO CLNS

- CSCdm61381

  A Cisco 2500 series router might reload if you issue the **no router isis** [*tag*] command. There is no workaround.

Miscellaneous

- CSCdm09656

  After you load the image on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S and Release 12.0 T, issuing the **no shutdown** command on a T1 controller that is up causes the T1 controller to go down. Channels created under that controller also go down. This only happens with T1 and does not occur on Cisco 7200 series routers.

  Workaround: Issue the **shutdown** command followed by the **no shutdown** command on the T1 controller. If this fails, perform a microcode reload to bring the controller back up.

- CSCdm12259

  The rate limit on a Gigabit Switch Router (GSR) might not work properly if input Committed Access Rate (CAR) based on QoS groups is configured. There is no workaround.

- CSCdm66427

  If you use the "log" keyword in an Access Control List (ACL) that is used to filter routes, it might result in alignment errors that cause increased CPU utilization and interfere with normal router operation.

  Workaround: Remove the "log" keyword from the configuration.

Wide-Area Networking

- CSCdm49871

  A Cisco router reloads when you deconfigure a routing protocol (for example, when you issue the **no ipx routing** command). The problem exists in Cisco IOS Release 12.0(3)T and Release 12.0(3)S and later releases. At least one Frame Relay interface must be configured and at least one Frame Relay map (an association between a DLCI and a level 3 protocol address) must be established by Inverse ARP.

  Workaround:

  (a) Disable Inverse ARP for the routing protocol to be deconfigured (for example, for IPX routing, use the **no frame-relay inverse-arp ipx** *dlci* interface configuration command).

  (b) Clear the Frame Relay Inverse ARP cache using the **clear frame-relay-inarp** executive command.

  (c) Remove the routing protocol from the router (for example, for IPX routing, use the **no ipx routing** global configuration command).

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family and Cisco 12000 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, 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 CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 54

Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

  On CCO at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on CCO at:

  Technical Documents

- Caveats for Cisco IOS Release 12.0

  As a supplement to the caveats listed in the "Caveats" section in these release notes, see *Caveats for Cisco IOS Release 12.0*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0.

  On CCO at:

  Technical Documents: Documentation Home Page: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Caveats**

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

Platform-Specific Documents

These documents are available for the Cisco 7000 family and Cisco 12000 series routers on CCO and the Documentation CD-ROM:

- Installation and Configuration Guides
- Configuration Notes
- User Guides
- Hardware Installation and Maintenance Guides

- Regulatory Compliance and Safety Documentation

On CCO 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 Release 12.0 S 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 CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 S**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 S**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, and several other supporting documents, which are 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 two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, 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 CCO and the Documentation CD-ROM, two master documents provide information for the Cisco IOS software documentation set.

You can reach these documents on CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

You can reach these documents on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

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

You can reach the Cisco IOS documentation set on CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 8 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set

Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	X.25 over ISDN AppleTalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 and T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles Dial-Out Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *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
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signalling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

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

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

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

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

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

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

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

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

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

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

We appreciate and value your comments.

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