Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 DX

January 20, 2003

Cisco IOS Release 12.2(2)DX3

OL-2930-03

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(2)DX3. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(2)DX3, see the "Caveats" section on page 11 and *Caveats for Cisco IOS Release 12.2*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

Contents

These release notes contain the following sections:

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

Early Deployment Releases

These release notes describe the Cisco 7000 family for Cisco IOS Release 12.2(2)DX3, which is an early deployment (ED) release based on Cisco IOS Release 12.2 T. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features. Table 1 shows recent early deployment releases for the Cisco 7000 family.

Table 1 Early Deployment Releases for the Cisco IOS Release 12.2 DX

ED Release	Maintenance Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.2 DX	(2)DX3	Cisco IOS Release 12.2(2)DX3 contains no additional software or hardware features. Cisco IOS Release 12.2(2)DX3 includes caveat fixes only. For more information, see the "Caveats" section on page 11		01/20/2003
Cisco IOS Release 12.2 DX	(2)DX2	Cisco IOS Release 12.2(2)DX2 contains no additional software or hardware features. Cisco IOS Release 12.2(2)DX2 includes caveat fixes only. For more information, see the "Caveats" section on page 11		10/13/2002
Cisco IOS Release 12.2 DX	(2)DX1	Cisco IOS Release 12.2(2)DX1 contains no additional software or hardware features. Cisco IOS Release 12.2(2)DX1 includes caveat fixes only. For more information, see the "Caveats" section on page 11		07/01/2002
Cisco IOS Release 12.2 DX	(1)DX1	Cisco IOS Release 12.2(1)DX1 contains no additional software or hardware features. Cisco IOS Release 12.2(1)DX1 includes caveat fixes only. For more information, see the "Caveats" section on page 11		02/14/2002
Cisco IOS Release 12.2 DX	(1)	Per VRF AAA PPPoE over Gigabit Ethernet PPPoE Session Limit Quality of Service Features for Parallel Express Forwarding (PXF) RADIUS Attribute Screening Virtual Private Dial-up Network Extended Fail-over Conditions VPDN Group Session Limiting	7401ASR PA-2FE	06/4/2001

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 DX and includes the following sections:

Memory Recommendations

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2 DX

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB	128 MB	RAM
Cisco 7400 Series	IP Standard Feature Set	IP	c7400-is-mz	16 MB	128 MB	RAM
	Enterprise Standard Feature Set	Enterprise	c7400-js-mz	16MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(2)DX3 supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers (including the Cisco 7202, Cisco 7204, and Cisco 7206)
- Cisco 7200 VXR routers (including the Cisco 7204VXR and Cisco 7206VXR)
- Cisco 7400 series routers (including the Cisco 7401)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 5.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.2(2)DX3:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 DX Software (c7200-js-mz), Version 12.2(2)DX3, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

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

Feature Set Tables

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

Cisco IOS Release 12.2(2)DX3 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(2)DX3 can include new features supported by the Cisco 7000 family.

All Cisco 7200 platform supported features in Cisco IOS Release 12.2(2)DX3 support the 7200 Enterprise Feature Set of images.

All Cisco 7400 platform supported features in Cisco IOS Release 12.2(2)DX3 support the 7400 Enterprise Feature Set of images.

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

New and Changed Information

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

New Hardware Features in Cisco IOS Release 12.2(2)DX3

There are no new hardware features supported in Cisco IOS Release 12.2(2)DX3.

New Software Features in Cisco IOS Release 12.2(2)DX3

There are no new software features supported in Cisco IOS Release 12.2(2)DX3.

New Hardware Features in Cisco IOS Release 12.2(2)DX2

There are no new hardware features supported in Cisco IOS Release 12.2(2)DX2.

New Software Features in Cisco IOS Release 12.2(2)DX2

There are no new software features supported in Cisco IOS Release 12.2(2)DX2.

New Hardware Features in Cisco IOS Release 12.2(2)DX1

There are no new hardware features supported in Cisco IOS Release 12.2(2)DX1.

New Software Features in Cisco IOS Release 12.2(2)DX1

There are no new software features supported in Cisco IOS Release 12.2(2)DX1.

New Hardware Features in Cisco IOS Release 12.2(1)DX1

There are no new hardware features supported in Cisco IOS Release 12.2(1)DX1.

New Software Features in Cisco IOS Release 12.2(1)DX1

There are no new software features supported in Cisco IOS Release 12.2(1)DX1.

New Hardware Features in Cisco IOS Release 12.2(1)DX

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(1)DX:

7401ASR Router

Platforms: 7400 series routers

The Cisco 7401ASR router provides application-specific features for broadband subscriber aggregation and network application services with high processing performance.

The Cisco 7401ASR router supports the following features:

- Online insertion and removal (OIR)—Allows you to add, replace, or remove port adapters without interrupting the system.
- Environmental monitoring and reporting functions—Allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.
- Downloadable software—Allows you to load new images into Flash memory remotely, without having to physically access the router, for fast, reliable upgrades.
- Small form-factor—One rack-unit (RU) high with stacking capability: 1.72 in. x 17.3 in. x 11.80 in. (4.27 cm x 43.9 cm x 30 cm). The weight is approximately 10.5 lbs (4.76 kg).
- Front-to-back airflow—Allows you to mount the router from either front or back into telco or 19-inch racks and 21-23-inch four-post racks.

The Cisco 7401ASR router supports:

- Two native Ethernet interfaces—Each interface has two physical ports, a Gigabit Ethernet (1000 Mbps) port that uses a Gigabit Interface Converter (GBIC) and a Fast Ethernet/Ethernet port (10/100 Mbps) with an RJ-45 connector. Any two of the four ports are available at any one time.
- Both 25-MHz and 50-MHz port adapter operation.
- A 64- or 128-MB compact Flash disk.
- A single power supply that is available in four options: AC, single –24V DC, single –48V DC, and dual -48V DC.

PA-2FE

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PA-2FE port adapter provides two 10/100-Mbps, 10/100BASET Fast Ethernet/Inter-Switch Link (ISL) interfaces and supports both full-duplex and half-duplex operation. The PA-2FE comes in two models, the PA-2FE-TX and the PA-2FE-FX.

Each Fast Ethernet port on the PA-2FE-TX has an RJ-45 connector to attach to Category 5 unshielded twisted-pair (UTP) cable for 100BASETX. Each Fast Ethernet port on the PA-2FE-FX has an SC-type fiber-optic connector for 100BASEFX.

New Software Features in Cisco IOS Release 12.2(1)DX

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(1)DX:

Per VRF AAA

Platforms: Cisco 7200 and Cisco 7400 series routers

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the Virtual Home Gateway (VHG) to communicate directly with the customer RADIUS server associated with the customer VPN, without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support Per VRF AAA, AAA must be VRF aware. ISPs must be able to define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the network access server (NAS), the specification of the AAA server, which is based on IP addresses and port numbers, may create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

- Virtual Template—Used as a generic interface configuration.
- Service Provider AAA server—Used to associate a remote user with a specific VPN based on the domain name or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

PPPoE over Gigabit Ethernet

Platforms: Cisco 7200 series routers

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 7200 series routers with Gigabit Ethernet line cards.

PPPoE Session Limit

Platforms: Cisco 7200 and Cisco 7400 series routers

The PPPoE Session Limit feature enables you to limit the number of PPPoE sessions that can be created on a router or on an ATM PVC, PVC range, or VC class, or Ethernet subinterface.

Before the introduction of this feature, there was no way to limit the number of PPPoE sessions that could be created on a router. Not having a limit was potentially a problem because it was possible that the router could create so many PPPoE sessions that it would run out of memory.

To prevent the router from using too much memory for virtual access, the PPPoE Session Limit feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. The new **pppoe limit max-sessions** command limits the number of PPPoE sessions that can be created on the router. The modified **pppoe max-sessions** command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

Quality of Service Features for Parallel Express Forwarding (PXF)

Platform: Cisco 7200 VXR using a Network Services Engine (NSE)

The Modular Quality of Service Command-Line Interface (Modular QoS CLI) and many of the associated class-based QoS features are now available on PXF.

The following class-based QoS features are being introduced for PXF:

- Traffic Policing—The **police** command in policy map class configuration mode.
- Class-Based Weighted Fair Queueing (CBWFQ)—The **bandwidth** and **fair-queue** commands in policy map class configuration mode.
- Low Latency Queueing (LLQ)—The **priority** command used in policy map class configuration mode.
- Class-Based Weighted Random Early Detection (CBWRED) and Differentiated Services-Compliant Weighted Random Early Detection (DiffServ-Compliant WRED)—The **random-detect** command used simultaneously with the **bandwidth** command in policy map class configuration mode.
- Flow-Based Weighted Random Early Detection—The **random-detect** command used simultaneously with the **bandwidth** command in policy map class configuration mode.
- Class-Based Marking—The **set** command used in policy map class configuration mode. Class-Based Marking support is limited to 32 traffic classes per traffic policy, and QoS group marking (**set qos-group**) is not supported.

The Committed Access Rate (CAR) feature configured to use an access list with rate-limiting policies (the **access-list rate-limit** command in interface configuration mode) is also now available on PXF. If you wish to rate-limit traffic without using an ACL, use the Modular QoS CLI to configure the Traffic Policing feature.

Because of the addition of the Modular QoS CLI, traditional WRED (the **random-detect** command in interface configuration mode) and Fair Queueing (the **fair-queue** command in interface configuration mode) are no longer configurable. If you would like to configure WRED or Fair Queueing, you can use the Modular QoS CLI to configure Class-Based WRED or Class-Based Weighted Fair Queueing on a per-class rather than a per-interface basis.

The Modular QoS CLI on PXF does not currently support the following match criteria that are available on other Modular QoS CLI-supported platforms:

- Destination address
- Input Interface
- Internet Protocol (IP) values
- Multiprotocol Label Switching (MPLS) values
- Protocol
- Quality of Service (QoS) group values
- Source address

For additional information on the Modular QoS CLI, see the Modular Quality of Service Command-Line Interface document.

RADIUS Attribute Screening

Platforms: Cisco 7200 and Cisco 7400 series routers

The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers’ authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Virtual Private Dial-up Network Extended Fail-over Conditions

Platforms: Cisco 7200 and Cisco 7400 series routers

The Virtual Private Dial-up Network (VPDN) failover has been extended to occur in instances where the receiving node sends an error message to the transmitting node. Before this feature, the failover mechanism would only occur when the transmitting node did not receive a response from the receiving node.

This feature occurs automatically when failover is configured, so this feature has no new command. Failover is configured in the VPDN group by using the **initiate-to** command.

VPDN Group Session Limiting

Platforms: Cisco 7200 and Cisco 7400 series routers

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of VPDN sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group Session Limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the **session-limit** *number* command in VPDN configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the **vpdn session-limit** *session* command in configuration mode) is enforced.

MIBs

Current MIBs

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

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 3.

Table 3 Deprecated and Replacement MIBs

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

Table 3 Deprecated and Replacement MIBs (continued)

Deprecated MIB	Replacement
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Caveats

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

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

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(2)DX3.

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

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/.

Because Cisco IOS Release 12.2(1)DX is the initial base release, there are no resolved caveats. For a list of the resolved caveats, see the next set of release notes for this release version.

Table 4 Caveats Reference for Cisco IOS Release 12.2 DX

DDTS Number	Open in Release	Resolved in Release
CSCds53368		12.2(2)DX1
CSCdt41215		12.2(2)DX3
CSCdt88614		12.2(2)DX3
CSCdt97325		12.2(2)DX1
CSCdu46694		12.2(2)DX2
CSCdv40244		12.2(2)DX3
CSCdv57640		12.2(2)DX2
CSCdw65173		12.2(2)DX2
CSCdw65903		12.2(1)DX1
CSCdx24368		12.2(2)DX1
CSCdx35300		12.2(2)DX1
CSCdx36497		12.2(2)DX2
CSCdy11785		12.2(2)DX3

Table 4 Caveats Reference for Cisco IOS Release 12.2 DX (continued)

CSCdy07954		12.2(2)DX3
CSCdy18789		12.2(2)DX3
CSCdz60229		12.2(2)DX3
CSCin02516		12.2(2)DX2
CSCuk34244		12.2(2)DX1

Open Caveats—Cisco IOS Release 12.2(2)DX3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)DX3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(2)DX3.

Resolved Caveats—Cisco IOS Release 12.2(2)DX3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)DX3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt41215

  A Cisco 7200 or Cisco 7500 series router that is running Cisco IOS Release 12.0(10)S3 or 12.1(5) and that has PA-A3-OC3 port adapter may stop forwarding packets on one or more virtual connections (VCs).

  Workaround: Restore the original working condition by entering the **clear interface** privileged EXEC command.

- CSCdt88614

  A router may experience a Spurious Memory Access when sending an SNMP trap on a Link Down event. Spurious access is an attempt by Cisco IOS Software to access memory in a restricted location.

  This error has typically no impact on router behavior.

  Spurious accesses are counted and recorded, if possible, by Cisco IOS Software. This information is available with the **show alignment** command. The traceback information is necessary to determine the cause and the fix of the spurious accesses.

  This condition indicates a software failure. Enter the **show log**, **show alignment** and **show tech-support** commands, contact your Cisco technical support representative, and provide the representative with the gathered information.

  There are no known workarounds.

- CSCdv40244

  The following continuous stream of "%POT1E1-3-FWFATAL" error messages may occur on a router:

  ```
  %POT1E1-3-FWFATAL: Bay 5: firmware needsresetdue to fw watchdog timeout
  %POT1E1-3-FWFATAL: Bay 4: firmware needsresetdue to fatal software errors
  ```

  This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.1(8.04)and a Cisco 7500 router running Cisco IOS release 12.0(21)S2 configured with a PA-MC-8T1 port adapter, but may also affect the PA-MC-2T1, PA-MC-4T1, PA-MC-8DSX1, PA-MC- 2E1/120, and PA-MC-8E1/120 port adapters.

  There are no known workarounds.

- CSCdy07954

  "session-limit 0" is seen once "initiate-to ip x.x.x.x" is configured in L2TP configuration and deleted by "no initiate-to ip x.x.x.x" Although "session-limit 0" is supposed to be visible only when "accept-dialin" or "request-dialout" option is configured under the vpdn-group, it is also seen when "request-dialin" option is configured under the vpdn-group. The image file is "c7200-is-mz.122-2.DX".

  "session-limit 0" is seen once "initiate-to ip x.x.x.x" is configured in L2TP configuration and deleted by "no initiate-to ip x.x.x.x".

  Workaround: "session-limit 0" can be deleted by re-configuring "initiate-to ip x.x.x.x".

- CSCdy11785

  A Cisco 7206VXR may be restarted because of a bus error at executing show env last comand processes and display the following crashinfo messages:

  ```
  CMD: 'show env last' 16:50:54 JST Thu Jul 4 2002

  -Traceback= 6060A0CC 60608C74 60716E90 60722340 606268FC 60634A9C 60696A9C
  60696A88
  signal= 0xA, code= 0x8, context= 0x62245C90
  ```

  This symptom is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.2(2)DD4.

  There is no known workarounds.

- CSCdy18789

  A system may run out of memory because of a leak in the routing table structures. No explicit triggers (other than routes in the table) are needed to cause this symptom.

  The conditions under which this symptom occurs are not known at this time.

  There is no workaround.

- CSCdz60229

  Cisco devices which run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

Open Caveats—Cisco IOS Release 12.2(2)DX2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)DX2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(2)DX2.

Resolved Caveats—Cisco IOS Release 12.2(2)DX2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)DX2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu46694

  A Cisco 7500 router may experience some packet loss between hosts after Cisco Express Forwarding (CEF) is enabled.

  There are no known workarounds.

- CSCdv57640

  When a virtual-template interface is configured for IP virtual routing and forwarding (VRF) in a Layer 2 Tunnel Protocol (L2TP) dial-in setup, only about 50 percent of the data packets are able to make it across the tunnel.

  Workaround: Disable the **ip route-cache cef** as well as “ip route-cache” interface configuration commands on the virtual template interface to allow all packets to go through the process-switching.

  In addition to fixing the above problem, this also fixes the problem with Vaccess counters, observed after CSCdw01642. The problem was that the counters on the Vaccess interfaces used for L2TP sessions (on LAC and LNS) showed wrong values. That happened only when IP CEF was enabled on high end routers.

- CSCdw65173

  PA-A3 on 7200 stops transmitting traffic when the adapter experiences a very high number of carrier transitions. Carrier transitions in this scenario are due to a clocking loop in the ATM network. After recovery of the ATM network, by rectifying the clocking loop, the ATM PA-A3 does not recover. The ATM PA-A3 exhibits output drops in the show interface output.

  Workaround: shut/no shut the interface.

- CSCdx36497

  A c7200 might crash while running different 12.2T based releases due to a software forced crash per memory corruption in the I/O pool, displaying messages (among others) as follows:

  ```
  memory pool type is I/O
  %SYS-3-OVERRUN: Block overrun at 7333CF8 (red zone 372F5C60)
  ```

  This might happen in systems with high loads on the FE interface, due to an error on the FE driver. This FE driver is specific of the following part numbers equipped with the DEC21140 controller:

  ```
  PA-2FEISL-TX=
  PA-FE-TX=
  C7200-I/O-FE=
  ```

  There are no known workarounds.

- CSCin02516

  When “no ip address” occurs on an interface, the associated adjacency entries have not been removed. If the previous interface’s ip address is re-assigned in its subinterface, the adjacency entry is still pointing to the previous main interface.

  The problem occurs with static arp entries who’s ip addresses are on the same subnet of the interface.

  Workaround: Remove static arp configuration.

Open Caveats—Cisco IOS Release 12.2(2)DX1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)DX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(2)DX1.

Resolved Caveats—Cisco IOS Release 12.2(2)DX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)DX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds53368

  SNMP query on ciscoFlashPartitionEntry object in CISCO-FLASH-MIB for a 7200 device takes approximately 55 secs to return data. We have only seen this problem in the devices with ATA file system.

  There are no known workarounds.

- CSCdt97325

  Cisco routers that are running Cisco IOS Release 12.1, 12.2, or 12.0S with an Advanced Technology Attachment (ATA) sandisk card (of any capacity) may pause indefinitely or be slow to respond to command-line interface (CLI) command input when the SNMP FlashMIB is queried. The FlashMIB queries may also timeout. This problem occurs when the inode numbers of the files in the ATA sandisk are not sequential and when there is a large difference in the inode numbers.

  The following is an example of a directory list with inode numbers that are likely to cause an SNMP timeout when the Flash MIB is queried:

  ```
  gt3-7200-3#dir disk1: Directory of disk1:/
  3 -rw- 1690 shankar
  4 -rw- 1690 sara
  ```

```
5 -rw- 1690 sara1
6 -rw- 1690 sara12
7 -rw- 1690 sara123
8 -rw- 1690 sara1234
10 -rw- 1690 sara12345
11 -rw- 1690 sara123456
12 -rw- 1690 7
9 drw- 0 directory-one
15 -rw- 8623108 c7200-is-mz.121-7.4
14 -rw- 3578452 c7200-boot-mz.del96042
2994 -rw- 4307448 c7200-boot-mz.flo96042
4046 -rw- 3578544 c7200-boot-mz.del96042first
```

Workaround: Exclude the ciscoFlashFileEntry MIB from FlashMIB queries.

- CSCdx24368

  Acct-Session-Time[46] in Network STOP record may report the value as zero for sessions expanding more than 49 days.

  There are no known workarounds.

- CSCdx35300

  GigaEthernet input queue wedged like bellow and excessive input queue drops can be seen on C7401ASR(12.2(2)DD4).

  There are no known workarounds.

- CSCuk34244

  This symptom may be seen on Cisco 7200 or Cisco 7400 platforms when a packet is received via one tunnel and CEF-switched into another tunnel. If a condition occurs after the first tunnel encapsulation has been replaced with the second tunnel encapsulation that requires the newly tunnel-encapsulated packet to be punted from CEF switching to a slower switching path, the router may reload with a DMA error.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(1)DX1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(1)DX1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(1)DX1.

Resolved Caveats—Cisco IOS Release 12.2(1)DX1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(1)DX1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

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

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

Related Documentation

The following sections describe the documentation available for the Cisco 12.2(2)DX3. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

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

Use these release notes with these documents:

Release-Specific Documents

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

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

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

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

  Technical Documents

- *Caveats for Cisco IOS Release* 12.2

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

- *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in *Caveats for Cisco IOS Release 12.2 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 T.

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

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

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

`Platform-Specific Documents

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

- *Cisco 7000 Hardware Installation and Maintenance*
- *Cisco 7000 User Guide*
- *Cisco 7010 User Guide*
- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 VXR Quick Start Guide*
- *Cisco 7202 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7206 Quick Start Guide*
- *Cisco 7401 ASR Installation and Configuration Guide*
- *Cisco 7401 ASR Quick Start Guide*
- *Quick Reference for Cisco 7204 Installation*
- *Quick Start Guide Cisco 7100 Series VPN Router*

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(2)DX3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2 X Releases**: **New Features in Release 12.2 DX**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2 X Releases**: **New Features in Release 12.2 DX**

Cisco IOS Software Documentation Set

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

Documentation Modules

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

On Cisco.com at:

Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

On the Documentation CD-ROM at:

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

Cisco IOS Release 12.2 Documentation Set Contents

Table 5 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

Table 5 Cisco IOS Release 12.2 Documentation Set

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

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

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

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

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

Obtaining Documentation

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

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 17.