



# Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2

September 22, 2006



## Note

- This publication applies to these platforms:
  - [CAT6000-SUP720/MSFC3](#)
  - [7600-SUP720/MSFC3](#)
  - [CAT6000-SUP32/MSFC2A](#) (not supported in all releases)
  - [7600-SUP32/MSFC2A](#) (not supported in all releases)
  - [CAT6000-SUP2/MSFC2](#) (not supported in all releases)
  - [7600-SUP2/MSFC2](#) (not supported in all releases)
- These release notes are for Cisco IOS Release 12.2SX on both the supervisor engine and the MSFC. If you are running the Catalyst operating system on the supervisor engine and Cisco IOS Release 12.2SX only on the MSFC, refer to this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_8\\_1/ol\\_4563.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_1/ol_4563.htm)

The most current release notes for 12.2SX on the supervisor engine and MSFC are available on Cisco.com at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol\\_4164.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm)



## Caution

Cisco IOS running on the supervisor engine and the MSFC supports redundant configurations where the supervisor engines and MSFCs are identical. If they are not identical, one will boot first and become active and hold the other supervisor engine and MSFC in a reset condition.



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

Copyright © 2003–2006 Cisco Systems, Inc. All rights reserved.

# Contents

This publication consists of these sections:

- [Chronological List of Releases, page 2](#)
- [Hierarchical List of Releases, page 4](#)
- [Supported Hardware, page 10](#)
- [Unsupported Hardware, page 79](#)
- [FPD Image Packages, page 80](#)
- [Cisco IOS Software Modularity, page 105](#)
- [Feature Sets, page 106](#)
- [New Features, page 135](#)
- [Unsupported Features and Commands, page 200](#)
- [Limitations and Restrictions, page 202](#)
- [Caveats, page 212](#)
- [Troubleshooting, page 430](#)
- [System Software Upgrade Instructions, page 432](#)
- [Related Documentation, page 433](#)
- [Documentation Feedback, page 438](#)
- [Cisco Product Security Overview, page 438](#)
- [Product Alerts and Field Notices, page 439](#)
- [Obtaining Technical Assistance, page 440](#)
- [Obtaining Additional Publications and Information, page 441](#)

## Chronological List of Releases



### Note

- 
- See the [“Feature Sets” section on page 106](#) for information about which releases are deferred.
  - See the [“Hierarchical List of Releases” section on page 4](#) for information about parent releases.
- 

This is a chronological list of the 12.2SX releases:

- 22 Sep 2006—Release 12.2(18)SXF6
- 18 Sep 2006—Release 12.2(18)SXE6a
- 15 Sep 2006—Release 12.2(18)SXD7a
- 10 Jul 2006—Release 12.2(18)SXF5
- 08 Jun 2006—Release 12.2(18)SXE6
- 17 Apr 2006—Release 12.2(17d)SXB11a
- 27 Mar 2006—Release 12.2(18)SXF4

- 16 Feb 2006—Release 12.2(18)SXF3
- 13 Feb 2006—Release 12.2(18)SXE5
- 20 Jan 2006—Release 12.2(18)SXF2
- 22 Dec 2005—Release 12.2(18)SXF1
- 15 Dec 2005—Release 12.2(18)SXD7
- 17 Nov 2005—Release 12.2(17d)SXB11
- 10 Oct 2005—Release 12.2(18)SXE4
- 12 Sep 2005—Release 12.2(18)SXF
- 22 Aug 2005—Release 12.2(18)SXE3
- 22 Aug 2005—Release 12.2(18)SXD6
- 16 Aug 2005—Release 12.2(17d)SXB10
- 21 Jul 2005—Release 12.2(17d)SXB9
- 23 Jun 2005—Release 12.2(18)SXE2
- 16 May 2005—Release 12.2(18)SXD5
- 02 May 2005—Release 12.2(17d)SXB8
- 18 Apr 2005—Release 12.2(18)SXE1
- 11 Apr 2005—Release 12.2(18)SXE
- 24 Mar 2005—Release 12.2(18)SXD4
- 01 Mar 2005—Release 12.2(17d)SXB7
- 21 Dec 2004—Release 12.2(17d)SXB6
- 13 Dec 2004—Release 12.2(18)SXD3
- 01 Nov 2004—Release 12.2(17d)SXB5
- 22 Oct 2004—Release 12.2(18)SXD2
- 30 Sep 2004—Release 12.2(18)SXD1
- 07 Sep 2004—Release 12.2(17d)SXB4
- 17 Aug 2004—Release 12.2(17d)SXB3
- 26 Jul 2004—Release 12.2(18)SXD
- 21 Jul 2004—Release 12.2(17d)SXB2
- 01 Jun 2004—Release 12.2(17d)SXB1
- 23 Apr 2004—Release 12.2(17a)SX4
- 22 Apr 2004—Release 12.2(17b)SXA2
- 05 Mar 2004—Release 12.2(17d)SXB
- 05 Mar 2004—Release 12.2(17a)SX3
- 29 Jan 2004—Release 12.2(17a)SX2
- 31 Dec 2003—Release 12.2(17b)SXA
- 30 Oct 2003—Release 12.2(17a)SX1
- 06 Oct 2003—Release 12.2(17a)SX
- 01 Jul 2003—Release 12.2(14)SX2 (MSFC3 only)

- 28 May 2003—Release 12.2(14)SX1
- 14 Apr 2003—Release 12.2(14)SX

## Hierarchical List of Releases



### Note

See the [“Feature Sets” section on page 106](#) for information about which releases are deferred.

These releases support the hardware listed in the [“Supported Hardware” section on page 10](#):

- Release 12.2(18)SXF6:
  - Date of release: 22 Sep 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF5
- Release 12.2(18)SXF5:
  - Date of release: 10 Jul 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF4
- Release 12.2(18)SXF4:
  - Date of release: 27 Mar 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF3
- Release 12.2(18)SXF3:
  - Date of release: 16 Feb 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF2
- Release 12.2(18)SXF2:
  - Date of release: 20 Jan 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF1, Release 12.2(18)SXE4, Release 12.2(18)SXD7, and Release 12.2(17d)SXB11
- Release 12.2(18)SXF1:
  - Date of release: 22 Dec 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF
- Release 12.2(18)SXF:
  - Date of release: 12 Sep 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on Release [12.2\(18\)SXE3](#), Release [12.2\(18\)SXD6](#), and Release [12.2\(17d\)SXB10](#)

- Release 12.2(18)SXE6a:
  - Date of release: 18 Sep 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE6
- Release 12.2(18)SXE6:
  - Date of release: 08 Jun 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE5
- Release 12.2(18)SXE5:
  - Date of release: 13 Feb 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE4
- Release 12.2(18)SXE4:
  - Date of release: 10 Oct 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE3
- Release 12.2(18)SXE3:
  - Date of release: 22 Aug 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE2
- Release 12.2(18)SXE2:
  - Date of release: 23 Jun 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE1
- Release 12.2(18)SXE1:
  - Date of release: 18 Apr 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE
- Release 12.2(18)SXE:
  - Date of release: 11 Apr 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on [Release 12.2\(18\)SXD4](#) and [12.2\(17d\)SXB7](#)
- Release 12.2(18)SXD7a:
  - Date of release: 15 Sep 2006
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD7

- Release 12.2(18)SXD7:
  - Date of release: 15 Dec 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD6
- Release 12.2(18)SXD6:
  - Date of release: 22 Aug 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD5
- Release 12.2(18)SXD5:
  - Date of release: 16 May 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD4
- Release 12.2(18)SXD4:
  - Date of release: 24 Mar 2005
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD3
- Release 12.2(18)SXD3:
  - Date of release: 13 Dec 2004
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD2
- Release 12.2(18)SXD2:
  - Date of release: 22 Oct 2004
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD1
- Release 12.2(18)SXD1:
  - Date of release: 30 Sep 2004
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD
- Release 12.2(18)SXD:
  - Date of release: 26 Jul 2004
  - Parent in Release 12.2S: [12.2\(18\)S](#) (not all features in Release 12.2(18)S are supported)
  - Based on [Release 12.2\(17d\)SXB2](#)

**Note**

For information about Release 12.2(18)S, refer to these publications on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/index.htm>

- Release 12.2(17d)SXB11a:
  - Date of release: 17 Apr 2006
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB11
- Release 12.2(17d)SXB11:
  - Date of release: 17 Nov 2005
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB10
- Release 12.2(17d)SXB10:
  - Date of release: 16 Aug 2005
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB9
- Release 12.2(17d)SXB9:
  - Date of release: 21 Jul 2005
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB8
- Release 12.2(17d)SXB8:
  - Date of release: 24 Apr 2005
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB7
- Release 12.2(17d)SXB7:
  - Date of release: 01 Mar 2005
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB6
- Release 12.2(17d)SXB6:
  - Date of release: 21 Dec 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB5
- Release 12.2(17d)SXB5:
  - Date of release: 01 Nov 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB4

- Release 12.2(17d)SXB4:
  - Date of release: 07 Sep 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB3
- Release 12.2(17d)SXB3:
  - Date of release: 17 Aug 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB2
- Release 12.2(17d)SXB2:
  - Date of release: 21 Jul 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB1
- Release 12.2(17d)SXB1:
  - Date of release: 01 Jun 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Rebuild based on Release 12.2(17d)SXB and [Release 12.2\(17a\)SX4](#)
- Release 12.2(17d)SXB:
  - Date of release: 05 Mar 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17d\)](#)
  - Based on [Release 12.2\(17b\)SXA](#) and [Release 12.2\(17a\)SX3](#)

**Note**

For information about Release 12.2(17d), refer to these publications on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

- Release 12.2(17b)SXA2 (deferred):
  - Date of release: 22 Apr 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17b\)](#)
  - Rebuild based on Release 12.2(17b)SXA.



- Release 12.2(17b)SXA (deferred):
  - Date of release: 31 Dec 2003
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17b\)](#)
  - Based on [Release 12.2\(17a\)SX1](#).

**Note**

For information about Release 12.2(17b), refer to these publications on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

- Release 12.2(17a)SX4 (deferred):
  - Date of release: 23 Apr 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17a\)](#)
  - Rebuild based on Release 12.2(17a)SX3
- Release 12.2(17a)SX3 (deferred):
  - Date of release: 05 Mar 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17a\)](#)
  - Rebuild based on Release 12.2(17a)SX2
- Release 12.2(17a)SX2 (deferred):
  - Date of release: 29 Jan 2004
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17a\)](#)
  - Rebuild based on Release 12.2(17a)SX1
- Release 12.2(17a)SX1 (deferred):
  - Date of release: 30 Oct 2003
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17a\)](#)
  - Rebuild based on Release 12.2(17a)SX
- Release 12.2(17a)SX (deferred):
  - Date of release: 06 Oct 2003
  - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from [Release 12.2\(17a\)](#)
  - Based on Release 12.2(14)SX1.

**Note**

- For information about Release 12.2(17a), refer to these publications on Cisco.com:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>
  - Release 12.2(14)SX2 (01 Jul 2003) only supports the MSFC3 and is for use with the Catalyst operating system on the Supervisor Engine 720. Release 12.2(14)SX2 has only MSFC3 images. Release 12.2(14)SX2 does not have any Supervisor Engine 720 images.
- 
- Release 12.2(14)SX1 (deferred):
    - Date of release: 28 May 2003
    - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)
    - Rebuild based on Release 12.2(14)SX
  - Release 12.2(14)SX (deferred):
    - Date of release: 14 Apr 2003
    - Parent in Release 12.2S: [12.2\(14\)S](#) (not all features in Release 12.2(14)S are supported)

**Note**

For information about Release 12.2(14)S, refer to these publications on Cisco.com:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/index.htm>

This publication does not describe features that are available in Release 12.2, Release 12.2 T, Release 12.2 S, or other Release 12.2 early deployment releases.

For a list of the Release 12.2 caveats that apply to Release 12.2SX, see the “Caveats” section on [page 212](#) and refer to this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/index.htm>

For a list of the Release 12.2 S caveats that apply to Release 12.2SX, see the “Caveats” section on [page 212](#) and refer to this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122srn.htm>

For general product information about the Catalyst 6500 series switches, refer to the Catalyst 4000, 5000, and 6000 Family Software Product Bulletin (URL below). For general information about Release 12.2SX, refer to the Product Bulletin at these URLs:

<http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/>

<http://www.cisco.com/warp/public/732/releases/release122/122s/pbs/>

## Supported Hardware

These sections describe the hardware supported in Release 12.2SX:

- [Supervisor Engines, page 11](#)
- [Policy Feature Cards, page 18](#)
- [Distributed and Centralized Forwarding Cards, page 22](#)
- [Switch Fabric Modules, page 26](#)

- [Transceivers, page 27](#)
- [10-Gigabit Ethernet Switching Modules, page 30](#)
- [Gigabit Ethernet Switching Modules, page 33](#)
- [Power over Ethernet Daughtercards, page 38](#)
- [10/100/1000 Ethernet Switching Modules, page 39](#)
- [Fast Ethernet Switching Modules, page 43](#)
- [Ethernet/Fast Ethernet \(10/100\) Switching Modules, page 44](#)
- [Ethernet Switching Modules, page 48](#)
- [Optical Services Modules \(OSMs\), page 48](#)
- [Shared Port Adapter \(SPA\) Interface Processors \(SIPs\), page 53](#)
- [Shared Port Adapters \(SPAs\), page 54](#)
- [Services SPA Carrier \(SSC\), page 57](#)
- [Services SPAs, page 57](#)
- [FlexWAN and Enhanced FlexWAN Modules, page 57](#)
- [FlexWAN and Enhanced FlexWAN Module Port Adapters, page 58](#)
- [Service Modules, page 59](#)
- [Fan Trays, page 70](#)
- [Power Supplies, page 71](#)
- [Chassis, page 73](#)

**Note**

- Use the values in the “Power Required” column to determine the exact power requirements for your configuration to ensure that you are within the power budget.
- Daughtercard power is shown separately.
- Enter the **show power** command to display current system power usage.

## Supervisor Engines

- [Supervisor Engine 720 \(CAT6000-SUP720/MSFC3, 7600-SUP720/MSFC3\), page 11](#)
- [Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A\), page 15](#)
- [Supervisor Engine 2 \(CAT6000-SUP2/MSFC2, 7600-SUP2/MSFC2\), page 18](#)

### Supervisor Engine 720 (CAT6000-SUP720/MSFC3, 7600-SUP720/MSFC3)

- [Supervisor Engine 720 Common Features, page 12](#)
- [Supervisor Engine 720 with PFC3BXL, page 13](#)
- [Supervisor Engine 720 with PFC3B, page 14](#)
- [Supervisor Engine 720 with PFC3A, page 15](#)

## Supervisor Engine 720 Common Features

- Integrated 720-Gbps Switch Fabric
- 64-MB bootflash device or CompactFlash adapter with 512 MB CompactFlash card (WS-CF-UPG=):
  - 64-MB bootflash device (**sup-bootflash:**) supported in all releases
  - WS-CF-UPG= (**sup-bootdisk:**) supported in:
    - Release 12.2(18)SXE5 and later releases
    - Release 12.2(18)SXF and later releases
  - See this publication:
    - [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_17277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_17277.htm)
- 2 CompactFlash Type II slots (disk0: and disk1:)




---

**Note** Some Supervisor Engine 720 Release 12.2SX images are larger than the bootflash device and must be stored on a CompactFlash card (**sup-bootdisk:** or disk0: or disk1:).

---

- Two Ethernet uplink ports:
  - 1-MB packet buffer per port
  - Port 1—[Gigabit Ethernet SFP](#)
  - Port 2—Configurable as [Gigabit Ethernet SFP](#) or 10/100/1000 Mbps RJ-45
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Port grouping:
  - Number of ports: 2
  - Number of port groups: 1
  - Port ranges per port group: 1–2
- Supervisor Engine 720 requires a high-capacity fan tray (see the “[Fan Trays](#)” section on page 70)
- Supervisor Engine 720 requires a 2500W or higher power supply (see the “[Power Supplies](#)” section on page 71)

## Supervisor Engine 720 with PFC3BXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720-3BXL	7.82 A@42 V	Supervisor Engine 720 with PFC3BXL: <ul style="list-style-type: none"> <li>• 1-GB DRAM</li> <li>• Policy Feature Card 3BXL (PFC3BXL; see the “<a href="#">Policy Feature Cards</a>” section on page 18)</li> <li>• Multilayer Switch Feature Card 3 (MSFC3): <ul style="list-style-type: none"> <li>– 1-GB DRAM</li> <li>– 64-MB bootflash</li> </ul> </li> </ul>	12.2(17b)SXA

## Note

- There are no memory upgrade options for WS-SUP720-3BXL.
- If you install WS-SUP720-3BXL=, upgrade the memory on any DFC3-equipped switching modules. See this document for DFC3 memory upgrades:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)

## Supervisor Engine 720 with PFC3B

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720-3B	6.72 A@42 V	Supervisor Engine 720 with PFC3B: <ul style="list-style-type: none"> <li>• 512-MB DRAM</li> <li>• Policy Feature Card 3B (PFC3B; see the “Policy Feature Cards” section on page 18)</li> <li>• Multilayer Switch Feature Card 3 (MSFC3): <ul style="list-style-type: none"> <li>– 512-MB DRAM</li> <li>– 64-MB bootflash</li> </ul> </li> </ul>	12.2(17d)SXB1

## Note

- See this document for DFC3 memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_16220.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm)
- You can upgrade the WS-SUP720-3B memory to 1-GB DRAM on the Supervisor Engine 720 and 1-GB DRAM on the MSFC3.
  - If you upgrade the memory, upgrade the Supervisor Engine 720, the MSFC3, and any DFC3-equipped switching modules.
  - See this document for Supervisor Engine 720 and MSFC3 memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15538.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15538.htm)

## Supervisor Engine 720 with PFC3A

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720	7.50 A@42 V	Supervisor Engine 720 with PFC3A: <ul style="list-style-type: none"> <li>• 512-MB DRAM</li> <li>• Policy Feature Card 3A (PFC3A; see the “Policy Feature Cards” section on page 18)</li> <li>• Multilayer Switch Feature Card 3 (MSFC3):               <ul style="list-style-type: none"> <li>– 512-MB DRAM</li> <li>– 64-MB bootflash</li> </ul> </li> </ul>	12.2(14)SX

### Note

- See this document for DFC3 memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_16220.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm)
- Except with WS-F6K-PFC3BXL=, do not upgrade the memory on WS-SUP720 or on the MSFC3 on WS-SUP720.

## Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)

These sections describe the Supervisor Engine 32:

- [Supervisor Engine 32 Restrictions, page 15](#)
- [Supervisor Engine 32 Features, page 17](#)

### Supervisor Engine 32 Restrictions

- Supervisor Engine 32 requires a high-capacity fan tray (see the “Fan Trays” section on page 70)
- Supervisor Engine 32 does not support this hardware:
  - WS-F6K-PFC3A Policy Feature Card 3A (PFC3A)
  - WS-F6K-PFC3BXL Policy Feature Card 3BXL (PFC3BXL)
  - DFCs (installed DFCs do not power up with a Supervisor Engine 32)
  - Switch Fabric Modules
  - These switching modules:
    - WS-X6704-10GE 4-port 10-Gigabit Ethernet XENPAK
    - WS-X6748-SFP 48-port Gigabit Ethernet SFP
    - WS-X6724-SFP 24-port Gigabit Ethernet SFP
    - WS-X6816-GBIC 16-port Gigabit Ethernet GBIC
    - WS-X6748-GE-TX 48-port 10/100/1000 RJ-45

- 7600-SIP-600 SPA Interface Processor-600
- Optical Services Modules (OSMs)
- WS-X6182-2PA FlexWAN Module (the WS-X6582-2PA Enhanced FlexWAN Module is supported)
- CISCO7603 3-slot chassis
- These service modules:
  - WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)
  - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) Module
  - WS-SVC-AGM-1-K9 Anomaly Guard Module
  - WS-SVC-ADM-1-K9 Traffic Anomaly Detector Module
  - WS-SVC-CSG-1 Content Services Gateway (CSG)
  - WS-X6066-SLB-APC Content Switching Module (CSM)
  - WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S)
  - WS-SVC-PSD-1 Persistent Storage Device (PSD) Module
  - WS-SVC-WLAN-1-K9 Wireless LAN service module
  - WS-SVC-IPSEC-1 IPsec VPN acceleration services module
- Supervisor Engine 32 does not support Cisco IOS SLB.
- Supervisor Engine 32 cannot support these software features and commands:
  - Egress multicast replication
  - Multicast replication mode detection
  - All fabric configuration commands



## Supervisor Engine 32 Features

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP32-10GE-3B	2.39 A@42 V	Supervisor Engine 32: <ul style="list-style-type: none"> <li>One 10/100/1000 Mbps RJ-45 port</li> <li>WS-SUP32-10GE—two 10-Gigabit Ethernet ports (requires <a href="#">XENPAKs</a>)</li> <li>WS-SUP32-GE—eight Gigabit Ethernet SFP ports (requires <a href="#">Gigabit Ethernet SFPs</a>)</li> <li>QoS port architecture (Rx/Tx): <b>2q8t/1p3q8t</b></li> <li>256-MB DRAM with the “<a href="#">IP BASE SSH LAN ONLY</a>” image (does not apply to the “<a href="#">IP BASE SSH LAN ONLY (MODULAR)</a>” image)</li> <li>512-MB DRAM with all other images</li> <li>256-MB bootflash</li> <li>Policy Feature Card 3B (PFC3B; see the “<a href="#">Policy Feature Cards</a>” section on page 18)</li> <li>Multilayer Switch Feature Card 2A (MSFC2A):               <ul style="list-style-type: none"> <li>256-MB DRAM with the “<a href="#">IP BASE SSH LAN ONLY</a>” image (does not apply to the “<a href="#">IP BASE SSH LAN ONLY (MODULAR)</a>” image)</li> <li>512-MB DRAM with all other images</li> <li>64-MB bootflash</li> </ul> </li> </ul>	12.2(18)SXF
WS-SUP32-GE-3B	1.89 A@42 V		

**Note** See this publication for Supervisor Engine 32 hardware information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/supe\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/supe_gd/index.htm)

## Supervisor Engine 2 (CAT6000-SUP2/MSFC2, 7600-SUP2/MSFC2)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2	3.46 A@42 V	Supervisor Engine 2 with Policy Feature Card 2 (PFC2): <ul style="list-style-type: none"> <li>• ROMMON version 7.1(1) or later</li> <li>• 32-MB bootflash device</li> <li>• 256-MB DRAM (minimum)</li> <li>• dual-port 1000BASE-X GBIC uplinks</li> <li>• QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>• Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2</li> <li>• Multilayer Switch Feature Card 2 (MSFC2) with 256-MB DRAM (minimum)</li> </ul>	12.2(17d)SXB

### Note

- Some Supervisor Engine 2 Release 12.2SX images are larger than the bootflash device. Supervisor Engine 2 ROMMON version 7.1(1) or later supports the MEM-C6K-ATA-1-64M= (64 MB) PCMCIA ATA FlashDisk device. See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78\\_13488.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_13488.htm)
- To use WS-X6K-S2-MSFC2 with 12.2SX releases, upgrade the memory.
  - MSFC2 DRAM—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_6953.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_6953.htm)
  - Supervisor Engine 2 DRAM—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12693.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12693.htm)
  - Supervisor Engine 2 Bootflash—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12667.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12667.htm)
- Supervisor Engine 2 supports all GBICs supported by Release 12.2(17d)SXB and later releases.

## Policy Feature Cards

- [Policy Feature Card Guidelines and Restrictions, page 19](#)
- [Policy Feature Card 3BXL, page 21](#)
- [Policy Feature Card 3B, page 21](#)
- [Policy Feature Card 3A, page 22](#)

## Policy Feature Card Guidelines and Restrictions

- A [Supervisor Engine 2](#) always has a PFC2; there are no PFC options for Supervisor Engine 2.
- The PFC2 supports a theoretical maximum of 128 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 supports a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 partitions the hardware FIB table to route IPv4 unicast, IPv4 multicast, MPLS, and IPv6 unicast and multicast traffic in hardware. Traffic for routes that do not have entries in the hardware FIB table are routed by the MSFC in software.

The defaults for [XL mode](#) are:

- IPv4 unicast and MPLS—512,000 routes
- IPv4 multicast and IPv6 unicast and multicast—256,000 routes

The defaults for [Non-XL mode](#) are:

- IPv4 unicast and MPLS—192,000 routes
- IPv4 multicast and IPv6 unicast and multicast—32,000 routes




---

**Note** The size of the global internet routing table plus any local routes might exceed the non-XL mode default partition sizes.

---

These are the theoretical maximum numbers of routes for the supported protocols (the maximums are not supported simultaneously):

- [XL mode](#):
  - IPv4 and MPLS— Up to 1,007,000 routes
  - IPv4 multicast and IPv6 unicast and multicast—Up to 503,000 routes
- [Non-XL mode](#):
  - IPv4 and MPLS— Up to 239,000 routes
  - IPv4 multicast and IPv6 unicast and multicast—Up to 119,000 routes

Enter the **[mls cef maximum-routes](#)** command to repartition the hardware FIB table. IPv4 unicast and MPLS require one hardware FIB table entry per route. IPv4 multicast and IPv6 unicast and multicast require two hardware FIB table entries per route. Changing the partition for one protocol makes corresponding changes in the partitions of the other protocols. You must enter the **reload** command to put configuration changes made with the **[mls cef maximum-routes](#)** command into effect.




---

**Note** With a non-XL-mode system, if your requirements cannot be met by repartitioning the hardware FIB table, upgrade components as necessary to operate in XL mode.

---

- You cannot use one type of PFC3 (PFC3BXL, PFC3B, or PFC3A) on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- With Release 12.2(17d)SXB and later releases, enter the **show platform hardware pfc mode** command to display the PFC3 mode.

- With Release 12.2(17b)SXA and Release 12.2(17b)SXA2, enter the **show platform earl-mode** command to display the PFC3 mode.
- PFC3A—These restrictions apply to a configuration with a PFC3A and these DFCs:
  - PFC3A and DFC3A—No restrictions (PFC3A mode).
  - PFC3A and DFC3B—The PFC3A restricts DFC3B functionality: the DFC3B functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3BXL—The PFC3A restricts DFC3BXL functionality: the DFC3BXL functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3C—The PFC3A restricts DFC3C functionality: the DFC3C functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3CXL—The PFC3A restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3A (PFC3A mode).
- PFC3B—These restrictions apply to a configuration with a PFC3B and these DFCs:
  - PFC3B and DFC3A—PFC3B functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3B functions as a PFC3A (PFC3A mode).
  - PFC3B and DFC3B—No restrictions (PFC3B mode).
  - PFC3B and DFC3BXL—The PFC3B restricts DFC3BXL functionality: after a reload with a DFC3BXL-equipped module installed, the DFC3BXL functions as a DFC3B (PFC3B mode).
  - PFC3B and DFC3C—The PFC3B restricts DFC3C functionality: the DFC3C functions as a DFC3B (PFC3B mode).
  - PFC3B and DFC3CXL—The PFC3B restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3B (PFC3B mode).
- PFC3BXL—These restrictions apply to a configuration with a PFC3BXL and these DFCs:
  - PFC3BXL and DFC3A—PFC3BXL functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3BXL functions as a PFC3A (PFC3A mode).
  - PFC3BXL and DFC3B—PFC3BXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3BXL functions as a PFC3B (PFC3B mode).
  - PFC3BXL and DFC3BXL—No restrictions (PFC3BXL mode).
  - PFC3BXL and DFC3C—Each restricts the functionality of the other: the PFC3BXL functions as a PFC3B and the DFC3C functions as a DFC3B (PFC3B mode).
  - PFC3BXL and DFC3CXL—The PFC3BXL restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3BXL (PFC3BXL mode).
- Summary of the PFC modes:
  - PFC3A mode—Operating mode with a PFC3A or any DFC3As
  - PFC3B mode—Operating mode with PFC3B and any DFC3Bs or DFC3BXLs
  - PFC3BXL mode—Operating mode with PFC3BXL and any DFC3BXLs
- The features that require the PFC3BXL or PFC3B are not supported in PFC3A mode.
- With a PFC3BXL or PFC3B and no DFC3A-equipped switching modules installed at bootup, any DFC3A-equipped switching module installed after bootup remain powered down.

- To use DFC3A-equipped switching modules with a PFC3BXL or PFC3B, the DFC3A-equipped switching modules must be installed at bootup.
- To use DFC3B-equipped switching modules with a PFC3BXL, the DFC3B-equipped switching modules must be installed at bootup.

## Policy Feature Card 3BXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3BXL	2.57 A@42 V	Policy Feature Card 3BXL (PFC3BXL)	
		Supported only with Supervisor Engine 720	12.2(17b)SXA

### Note

- There are no memory upgrade options for WS-F6K-PFC3BXL.
- Use WS-F6K-PFC3BXL= to upgrade a [WS-SUP720](#) or [WS-SUP720-3B](#) with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_16220.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm)

## Policy Feature Card 3B

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3B	2.25 A@42 V	Policy Feature Card 3B (PFC3B)	
		With Supervisor Engine 720	12.2(17d)SXB1
		With Supervisor Engine 32	12.2(18)SXF

### Note

- There are no memory upgrade options for WS-F6K-PFC3B.
- Use [WS-F6K-PFC3BXL=](#) to upgrade a [WS-SUP720-3B](#) with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_16220.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm)

## Policy Feature Card 3A

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3A	2.25 A@42 V	Policy Feature Card 3A (PFC3A)	
		Supported only with Supervisor Engine 720	12.2(14)SX

### Note

- There are no memory upgrade options for WS-F6K-PFC3A.
- WS-F6K-PFC3A is available only on [WS-SUP720](#). It is not orderable.

## Distributed and Centralized Forwarding Cards

- [Distributed Forwarding Card 3CXL](#), page 22
- [Distributed Forwarding Card 3C](#), page 22
- [Distributed Forwarding Card 3BXL](#), page 23
- [Distributed Forwarding Card 3B](#), page 24
- [Distributed Forwarding Card 3A](#), page 25
- [Distributed Forwarding Card \(WS-F6K-DFC\)](#), page 26
- [Centralized Forwarding Card \(WS-X6700-CFC\)](#), page 26



### Note

See the “[Policy Feature Cards](#)” section on page 18 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.

## Distributed Forwarding Card 3CXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3CXL	2.35 A@42 V	Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules	
		Supported only with Supervisor Engine 720 and <a href="#">WS-X6708-10GE</a>	12.2(18)SXF5

## Distributed Forwarding Card 3C

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3C	1.65 A@42 V	Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules	
		Supported only with Supervisor Engine 720 and <a href="#">WS-X6708-10GE</a>	12.2(18)SXF5

## Distributed Forwarding Card 3BXL

- [WS-F6700-DFC3BXL, page 23](#)
- [WS-F6K-DFC3BXL, page 23](#)

### WS-F6700-DFC3BXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3BXL	3.30 A@42 V	Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17d)SXB6

#### Note

- WS-F6700-DFC3BXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3BXL upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15893.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15893.htm)

### WS-F6K-DFC3BXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3BXL	1.47 A@42 V	Distributed Forwarding Card 3BXL (DFC3BXL) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(18)SXD3

#### Note

- See this publication for information about WS-F6K-DFC3BXL memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)
- Supervisor Engine 720 supports a WS-F6K-DFC3BXL on these [WS-X6516-GBIC](#) switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on [WS-X6516-GBIC](#) switching modules:  
<http://www.cisco.com/warp/public/770/fn24494.shtml>

## Distributed Forwarding Card 3B

- [WS-F6700-DFC3B](#), page 24
- [WS-F6K-DFC3B](#), page 24

### WS-F6700-DFC3B

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3B	2.70 A@42 V	Distributed Forwarding Card 3B (DFC3B) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17d)SXB6

#### Note

- WS-F6700-DFC3B uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3B upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15893.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15893.htm)

### WS-F6K-DFC3B

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3B	1.67 A@42 V	Distributed Forwarding Card 3B (DFC3B) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(18)SXD3

#### Note

- See this publication for information about WS-F6K-DFC3B memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)
- Supervisor Engine 720 supports a WS-F6K-DFC3B on these [WS-X6516-GBIC](#) switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, [WS-X6516-GBIC](#) switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on [WS-X6516-GBIC](#) switching modules:  
<http://www.cisco.com/warp/public/770/fn24494.shtml>



## Distributed Forwarding Card 3A

- [WS-F6700-DFC3A, page 25](#)
- [WS-F6K-DFC3A, page 25](#)

### WS-F6700-DFC3A

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3A	3.00 A@42 V	Distributed Forwarding Card 3A (DFC3A) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17a)SX

#### Note

- WS-F6700-DFC3A uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3A memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)

### WS-F6K-DFC3A

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3A	2.57 A@42 V	Distributed Forwarding Card 3A (DFC3A) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(14)SX

#### Note

- See this publication for information about WS-F6K-DFC3A memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)
- Supervisor Engine 720 supports a WS-F6K-DFC3A on these [WS-X6516-GBIC](#) switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:  
<http://www.cisco.com/warp/public/770/fn24494.shtml>

## Distributed Forwarding Card (WS-F6K-DFC)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC	2.10 A@42 V	Distributed Forwarding Card (DFC) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB
		<b>Note</b> Not supported in Release 12.2(18)SXE and Rebuilds	

### Note

- Release 12.2(18)SXE does not support Supervisor Engine 2.
- WS-F6K-DFC requires a Switch Fabric Module.
- See this publication for information about WS-F6K-DFC memory upgrades:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_12409.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm)

## Centralized Forwarding Card (WS-X6700-CFC)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6700-CFC	0.75 A@42 V	Centralized Forwarding Card (CFC) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17a)SX

**Note** There are no memory upgrade options for WS-X6700-CFC.

## Switch Fabric Modules



### Note

- Switch fabric modules are supported only with Supervisor Engine 2.
- Except in [13-slot chassis](#), WS-X6500-SFM2 and WS-C6500-SFM can be used together to provide redundancy.
- 3-slot chassis do not support WS-X6500-SFM2 or WS-C6500-SFM.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6500-SFM2	3.09 A@42 V	Switch Fabric Module, version 2, to support dCEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB

**Note** WS-C6500-SFM2 supports all chassis except 3-slot chassis.

WS-C6500-SFM	2.79 A@42 V	Switch Fabric Module to support dCEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB

**Note** WS-C6500-SFM does not support [13-slot chassis](#) or 3-slot chassis.

## Transceivers

- [X2 Modules, page 27](#)
- [XENPAKs, page 27](#)
- [Small Form-Factor Pluggable \(SFP\) Modules, page 28](#)
- [Gigabit Interface Converters \(GBICs\), page 29](#)

## X2 Modules



Note

[WS-X6708-10GE](#) does not support X2 modules shipped before the release of the WS-X6708-10GE switching module. The unsupported X2 modules are labeled with a number that ends with -01.

Product ID (append “=” for spares)	Product Description	Minimum Software Version
X2-10GB-CX4	10GBASE for CX4 (copper) cable	12.2(18)SXF5
X2-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(18)SXF5
X2-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(18)SXF5
X2-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(18)SXF5
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(18)SXF5

## XENPAKs

Product ID (append “=” for spares)	Product Description	Minimum Software Version
XENPAK-10GB-ZR	10GBASE for any SMF type	12.2(18)SXF
XENPAK-10GB-LW	10GBASE-LW XENPAK Module with WAN PHY for SMF	12.2(18)SXE
	Note XENPAK-10GB-LW operates at an interface speed compatible with SONET/SDH OC-192/STM-64 and supports transmission at a data rate of 9.6Gbps.	
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	12.2(18)SXE
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	12.2(18)SXE
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable	12.2(17d)SXB1
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(17a)SX1
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(17a)SX1

Product ID (append “=” for spares)	Product Description	Minimum Software Version
XENPAK-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX
	<b>Note</b> Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with Part No. 800-24557-01, as described in this external field notice (CSCee47030):  <a href="http://www.cisco.com/warp/public/770/fn29736.shtml">http://www.cisco.com/warp/public/770/fn29736.shtml</a>	
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX

## Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:

- [Gigabit Ethernet SFPs, page 28](#)
- [Fast Ethernet SFPs, page 28](#)

### Gigabit Ethernet SFPs

Product ID (append “=” for spares)	Product Description	Minimum Software Version
GLC-BX-D	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength	12.2(18)SXE
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	12.2(18)SXE
GLC-ZX-SM	1000BASE-ZX SFP module	12.2(17d)SXB1
CWDM-SFP	1000BASE coarse wavelength-division multiplexing (CWDM) SFP module	12.2(17a)SX
GLC-T	1000BASE-T SFP module	12.2(17a)SX
GLC-LH-SM	1000BASE-LX/LH SFP	12.2(17a)SX
GLC-SX-MM	1000BASE-SX SFP	12.2(14)SX

### Fast Ethernet SFPs



**Note**

Only [WS-X6148-FE-SFP](#) supports these Fast Ethernet SFPs.

Product ID (append “=” for spares)	Product Description	Minimum Software Version
GLC-FE-100BX-U	100BASE-BX10-U SFP	12.2(18)SXF2
GLC-FE-100BX-D	100BASE-BX10-D SFP	12.2(18)SXF2
GLC-FE-100EX	100BASEEX SFP	12.2(18)SXF
GLC-FE-100ZX	100BASEZX SFP	12.2(18)SXF

Product ID (append “=” for spares)	Product Description	Minimum Software Version
GLC-FE-100FX	100BASEFX SFP	12.2(18)SXF
GLC-FE-100LX	100BASELX SFP	12.2(18)SXF

## Gigabit Interface Converters (GBICs)



### Note

The support listed in this section applies to all modules that use GBICs, including OSM LAN ports and OSM Gigabit Ethernet WAN ports.

Product ID (append “=” for spares)	Product Description	Minimum Software Version
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	12.2(18)SXE
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	12.2(17a)SX
CWDM-GBIC	Coarse wave division multiplexing (CWDM) GBIC	12.2(14)SX
WS-G5483	1000BASET GBIC	12.2(14)SX
WS-G5484	Short wavelength, 1000BASE-SX	12.2(14)SX
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	12.2(14)SX
WS-G5487	Extended distance, 1000BASE-ZX	12.2(14)SX

## 10-Gigabit Ethernet Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6708-10G-3C (WS-X6708-10GE with WS-F6700-DFC3C)	10.58A @42 V	8-port 10-Gigabit Ethernet <b>X2</b> module <ul style="list-style-type: none"> <li>• dCEF720</li> <li>• Supports egress multicast replication</li> <li>• QoS port architecture (Rx/Tx): <b>8q4t/1p7q4t</b></li> <li>• Dual switch-fabric connections</li> <li>• Number of ports: 8 Number of port groups: 8 Port ranges per port group: 1 port in each group</li> </ul>	
WS-X6708-10G-3CXL (WS-X6708-10GE with WS-F6700-DFC3CXL)	11.28A @ 42V		
		Supported only with Supervisor Engine 720	12.2(18)SXF5

### Note

- Installation of a WS-X6708-10GE switching module in a chassis other than the following prevents operation at levels that are fully NEBS-compliant:
  - WS-C6503-E
  - WS-C6504-E
  - WS-C6506-E
  - WS-C6509-E
  - WS-C6509-NEB-A
  - CISCO7604
  - CISCO7609
- WS-X6708-10G-3C and WS-X6708-10G-3CXL are the orderable product IDs.
- The front panel is labeled WS-X6708-10GE.
- Cisco IOS software commands display WS-X6708-10GE with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- WS-X6708-10GE ports do not support **VACL capture**. (CSCsb59015)
- WS-X6708-10GE is not supported in the **WS-C6503** and **CISCO7603** chassis.
- In a **13-slot chassis**, WS-X6708-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6708-10GE ports, STP BPDUs are not exempt from **Traffic Storm Control** suppression. Do not configure Traffic Storm Control on STP-protected WS-X6708-10GE ports that interconnect network devices.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6704-10GE	6.28 A@42 V	4-port 10-Gigabit Ethernet <a href="#">XENPAK</a> <ul style="list-style-type: none"> <li>• CEF720 with <a href="#">WS-X6700-CFC</a> (adds 0.75 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3BXL</a> (adds 3.30 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3B</a> (adds 2.70 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3A</a> (adds 3.00 A@42 V)</li> <li>• Supports egress multicast replication</li> <li>• QoS port architecture (Rx/Tx):               <ul style="list-style-type: none"> <li>– With DFC3: <b>8q8t/1p7q8t</b></li> <li>– With CFC: <b>1q8t/1p7q8t</b></li> </ul> </li> <li>• Dual switch-fabric connections</li> <li>• Number of ports: 4</li> <li>• Number of port groups: 4</li> <li>• Port ranges per port group: 1 port in each group</li> </ul>	
		Supported only with Supervisor Engine 720	12.2(17a)SX

**Note**

- WS-X6704-10GE requires one of the following:
  - [WS-F6700-DFC3BXL](#) (3.30 A@42 V)
  - [WS-F6700-DFC3B](#) (2.70 A@42 V)
  - [WS-F6700-DFC3A](#) (3.00 A@42 V)
  - [WS-X6700-CFC](#) (0.75 A@42 V)
- WS-X6704-10GE ships with [WS-X6700-CFC](#) installed unless ordered with [WS-F6700-DFC3BXL](#), [WS-F6700-DFC3B](#), or [WS-F6700-DFC3A](#).
- WS-X6704-10GE is supported in the [WS-C6503-E](#) chassis.
- WS-X6704-10GE is not supported in the [WS-C6503](#) and [CISCO7603](#) chassis.
- In a [13-slot chassis](#), WS-X6704-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6704-10GE ports, STP BPDUs are not exempt from [Traffic Storm Control](#) suppression. Do not configure Traffic Storm Control on STP-protected WS-X6704-10GE ports that interconnect network devices.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6502-10GE	3.30 A @42 V	1-port 10-Gigabit Ethernet <ul style="list-style-type: none"> <li>With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A @42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A @42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A @42 V)</li> </ul> </li> <li>With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A @42 V)</li> <li>QoS port architecture (Rx/Tx): <b>1p1q8t/1p2q1t</b></li> <li>Number of ports: 1 Number of port groups: 1 Port ranges per port group: 1 port in 1 group</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
<b>Note</b> WS-X6502-10GE does not support ISL encapsulation.			
<b>Optical Interface Module (OIM) for WS-X6502-10GE</b>			
WS-G6488		10GBASE-LR serial 1310 nm long-reach OIM	12.2(14)SX
WS-G6483		10GBASE-ER serial 1550 nm extended-reach OIM	12.2(14)SX



## Gigabit Ethernet Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6748-SFP	5.32 A@42 V	48-port <a href="#">Gigabit Ethernet SFP</a> <ul style="list-style-type: none"> <li>• CEF720 with <a href="#">WS-X6700-CFC</a> (adds 0.75 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3BXL</a> (adds 3.30 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3B</a> (adds 2.70 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3A</a> (adds 3.00 A@42 V)</li> <li>• Supports egress multicast replication</li> <li>• QoS architecture:               <ul style="list-style-type: none"> <li>– With DFC3: <b>2q8t/1p3q8t</b></li> <li>– With CFC: <b>1q8t/1p3q8t</b></li> </ul> </li> <li>• Dual switch-fabric connections</li> <li>• Number of ports: 48 Number of port groups: 4 Port ranges per port group:               <ul style="list-style-type: none"> <li>1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23</li> <li>2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24</li> <li>25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47</li> <li>26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48</li> </ul> </li> </ul>	
		Supported only with Supervisor Engine 720	12.2(17d)SXB

### Note

- WS-X6748-SFP requires one of the following:
  - [WS-F6700-DFC3BXL](#) (3.30 A@42 V)
  - [WS-F6700-DFC3B](#) (2.70 A@42 V)
  - [WS-F6700-DFC3A](#) (3.00 A@42 V)
  - [WS-X6700-CFC](#) (0.75 A@42 V)
- WS-X6748-SFP ships with [WS-X6700-CFC](#) installed unless ordered with [WS-F6700-DFC3BXL](#), [WS-F6700-DFC3B](#), or [WS-F6700-DFC3A](#).
- WS-X6748-SFP is supported in the [WS-C6503-E](#) chassis.
- WS-X6748-SFP is not supported in the [WS-C6503](#) and [CISCO7603](#) chassis.
- In a [13-slot chassis](#), WS-X6748-SFP is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-SFP ports, STP BPDUs are not exempt from [Traffic Storm Control](#) suppression. Do not configure Traffic Storm Control on STP-protected WS-X6748-SFP ports that interconnect network devices.
- See the “[Small Form-Factor Pluggable \(SFP\) Modules](#)” section on page 28.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6724-SFP	2.23 A@42 V	24-port <a href="#">Gigabit Ethernet SFP</a> <ul style="list-style-type: none"> <li>• CEF720 with <a href="#">WS-X6700-CFC</a> (adds 0.75 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3BXL</a> (adds 3.30 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3B</a> (adds 2.70 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3A</a> (adds 3.00 A@42 V)</li> <li>• Supports egress multicast replication</li> <li>• QoS architecture:               <ul style="list-style-type: none"> <li>– With DFC3: <b>2q8t/1p3q8t</b></li> <li>– With CFC: <b>1q8t/1p3q8t</b></li> </ul> </li> <li>• Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24</li> </ul>	
		Supported only with Supervisor Engine 720	12.2(17a)SX

**Note**

- WS-X6724-SFP requires one of the following:
  - [WS-F6700-DFC3BXL](#) (3.30 A@42 V)
  - [WS-F6700-DFC3B](#) (2.70 A@42 V)
  - [WS-F6700-DFC3A](#) (3.00 A@42 V)
  - [WS-X6700-CFC](#) (0.75 A@42 V)
- WS-X6724-SFP ships with [WS-X6700-CFC](#) installed unless ordered with [WS-F6700-DFC3BXL](#), [WS-F6700-DFC3B](#), or [WS-F6700-DFC3A](#).
- WS-X6724-SFP is supported in the [WS-C6503-E](#) chassis.
- WS-X6724-SFP is not supported in the [WS-C6503](#) and [CISCO7603](#) chassis.
- On WS-X6724-SFP ports, STP BPDUs are not exempt from [Traffic Storm Control](#) suppression. Do not configure Traffic Storm Control on STP-protected WS-X6724-SFP ports that interconnect network devices.
- See the “[Small Form-Factor Pluggable \(SFP\) Modules](#)” section on page 28.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6816-GBIC		16-port Gigabit Ethernet GBIC <ul style="list-style-type: none"> <li>dCEF256</li> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>Dual switch-fabric connections</li> <li>Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
	3.84 A@42 V	With Supervisor Engine 720	12.2(14)SX
	5.94 A@42 V	With Supervisor Engine 2	12.2(17d)SXB

**Note**

- WS-X6816-GBIC requires one of these for use with Supervisor Engine 720:
  - [WS-F6K-DFC3BXL](#) (adds 1.47 A@42 V)
  - [WS-F6K-DFC3B](#) (adds 1.67 A@42 V)
  - [WS-F6K-DFC3A](#) (adds 2.57 A@42 V)
- WS-X6816-GBIC requires [WS-F6K-DFC](#) for use with Supervisor Engine 2.
- In a [13-slot chassis](#), WS-X6816-GBIC is supported only in slots 9 through 13 and does not power up in other slots.

WS-X6516A-GBIC	3.62 A@42 V	16-port Gigabit Ethernet GBIC <ul style="list-style-type: none"> <li>CEF256</li> <li>With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>1-MB per-port packet buffers</li> <li>Supports egress multicast replication</li> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516-GBIC	3.40 A@42 V	16-port Gigabit Ethernet GBIC	
		<ul style="list-style-type: none"> <li>• CEF256</li> <li>• With Supervisor Engine 720: <ul style="list-style-type: none"> <li>– dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>• With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>• 512-KB per-port packet buffers</li> <li>• QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>• Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

**Note**

- Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information:  
<http://www.cisco.com/warp/public/770/fn24494.shtml>

WS-X6416-GBIC	2.81 A@42 V	16-port Gigabit Ethernet GBIC	
		<ul style="list-style-type: none"> <li>• QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>• Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6416-GE-MT	2.50 A@42 V	16-Port Gigabit Ethernet MT-RJ	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6316-GE-TX	5.15 A@42 V	16-port Gigabit Ethernet RJ-45	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6408A-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6408-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

**Note**

- Caveat CSCec65943 prevents support of the WS-X6408-GBIC switching module in Release 12.2(17a)SX.
- Caveat CSCec65943 is resolved in Release 12.2(17a)SX1 and later releases.

## Power over Ethernet Daughtercards


**Note**

The power over Ethernet (PoE) daughtercard “Power Required” values do not include the power drawn by phones.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-FE48X2-AF	0.42 A@42 V	IEEE 802.3af PoE daughtercard for <a href="#">WS-X6148X2-RJ-45</a> and <a href="#">WS-X6196-RJ-21</a> .	
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2
WS-F6K-GE48-AF	0.18 A@42 V	IEEE 802.3af PoE daughtercard for <a href="#">WS-X6548-GE-TX</a> and <a href="#">WS-X6148-GE-TX</a>	
		With Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-F6K-FE48-AF	0.18 A@42 V	IEEE 802.3af PoE daughtercard for <a href="#">WS-X6148-RJ-45</a> and <a href="#">WS-X6148-RJ-21</a>	
		With Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 2	12.2(17d)SXB
WS-F6K-VPWR-GE	0.42 A@42 V	PoE daughtercard for <a href="#">WS-X6548-GE-TX</a> and <a href="#">WS-X6148-GE-TX</a>	
		With Supervisor Engine 720	12.2(17a)SX
		With Supervisor Engine 2	12.2(17d)SXB
WS-F6K-VPWR	None	PoE daughtercard for <a href="#">WS-X6348-RJ-45</a> , <a href="#">WS-X6348-RJ-21V</a> , <a href="#">WS-X6148-RJ-45</a> , and <a href="#">WS-X6148-RJ-21</a>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB

## 10/100/1000 Ethernet Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6748-GE-TX	7.00 A@42 V	48-port 10/100/1000 RJ-45 <ul style="list-style-type: none"> <li>• CEF720 with <a href="#">WS-X6700-CFC</a> (adds 0.75 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3BXL</a> (adds 3.30 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3B</a> (adds 2.70 A@42 V)</li> <li>• dCEF720 with <a href="#">WS-F6700-DFC3A</a> (adds 3.00 A@42 V)</li> <li>• Supports egress multicast replication</li> <li>• QoS architecture:               <ul style="list-style-type: none"> <li>– With DFC3: <b>2q8t/1p3q8t</b></li> <li>– With CFC: <b>1q8t/1p3q8t</b></li> </ul> </li> <li>• Dual switch-fabric connections</li> <li>• Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		Supported only with Supervisor Engine 720	12.2(17a)SX

### Note

- WS-X6748-GE-TX requires one of the following:
  - [WS-F6700-DFC3BXL](#) (3.30 A@42 V)
  - [WS-F6700-DFC3B](#) (2.70 A@42 V)
  - [WS-F6700-DFC3A](#) (3.00 A@42 V)
  - [WS-X6700-CFC](#) (0.75 A@42 V)
- WS-X6748-GE-TX ships with [WS-X6700-CFC](#) installed unless ordered with [WS-F6700-DFC3BXL](#), [WS-F6700-DFC3B](#), or [WS-F6700-DFC3A](#).
- WS-X6748-GE-TX is supported in the [WS-C6503-E](#) chassis.
- WS-X6748-GE-TX is not supported in the [WS-C6503](#) and [CISCO7603](#) chassis.
- In a [13-slot chassis](#), WS-X6748-GE-TX is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-GE-TX ports, STP BPDUs are not exempt from [Traffic Storm Control](#) suppression. Do not configure Traffic Storm Control on STP-protected WS-X6748-GE-TX ports that interconnect network devices.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-GE-TX WS-X6548V-GE-TX WS-X6548-GE-45AF	2.98 A@42 V 3.40 A@42 V 3.16 A@42 V	48-port 10/100/1000 Mbps <ul style="list-style-type: none"> <li>• RJ-45</li> <li>• CEF256</li> <li>• WS-X6548-GE-TX supports <a href="#">WS-F6K-VPWR-GE</a> and <a href="#">WS-F6K-GE48-AF</a></li> <li>• WS-X6548V-GE-TX has <a href="#">WS-F6K-VPWR-GE</a></li> <li>• WS-X6548-GE-45AF has <a href="#">WS-F6K-GE48-AF</a></li> <li>• QoS port architecture (Rx/Tx): <b>1q2t/1p2q2t</b></li> <li>• Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48</li> </ul>	
		With Supervisor Engine 720 (except <a href="#">WS-F6K-GE48-AF</a> )	12.2(17a)SX
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 2	12.2(17d)SXB

**Note**

- Release 12.2(17b)SXA and later releases provide support for more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules.
- WS-X6548-GE-TX and WS-X6548V-GE-TX do not support these features:
  - With Release 12.2(17a)SX and Release 12.2(17a)SX1, more than 1 Gbps of traffic per EtherChannel
  - [WS-F6K-DFC3A](#)
  - ISL trunking
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control



Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148A-GE-TX WS-X6148A-GE-45AF	2.50 A@42 V 2.68 A@42 V	48-port 10/100/1000 Mbps <ul style="list-style-type: none"> <li>• RJ-45</li> <li>• WS-X6148A-GE-TX supports <a href="#">WS-F6K-GE48-AF</a></li> <li>• WS-X6148A-GE-45AF has <a href="#">WS-F6K-GE48-AF</a></li> <li>• QoS port architecture (Rx/Tx): <b>1q2t/1p3q8t</b></li> <li>• Number of ports: 48 Number of port groups: 6 Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48</li> <li>• The aggregate bandwidth of each port group is 1 Gbps.</li> </ul>	
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2

**Note** WS-X6148A-GE-TX and WS-X6148A-GE-45AF do not support these features:

- [WS-F6K-DFC3A](#), [WS-F6K-DFC3B](#), or [WS-F6K-DFC3BXL](#)
- Traffic storm control

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-GE-TX WS-X6148V-GE-TX WS-X6148-GE-45AF	2.47 A@42 V 2.89 A@42 V 2.65 A@42 V	48-port 10/100/1000 Mbps <ul style="list-style-type: none"> <li>• RJ-45</li> <li>• WS-X6148-GE-TX supports <a href="#">WS-F6K-VPWR-GE</a> and <a href="#">WS-F6K-GE48-AF</a></li> <li>• WS-X6148V-GE-TX has <a href="#">WS-F6K-VPWR-GE</a></li> <li>• WS-X6148-GE-45AF has <a href="#">WS-F6K-GE48-AF</a></li> <li>• QoS port architecture (Rx/Tx): <b>1q2t/1p2q2t</b></li> <li>• Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48</li> </ul>	
		With Supervisor Engine 720 (except <a href="#">WS-F6K-GE48-AF</a> )	12.2(17a)SX
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		<a href="#">WS-F6K-GE48-AF</a> with Supervisor Engine 2	12.2(17d)SXB

**Note** WS-X6148-GE-TX, WS-X6148V-GE-TX, and WS-X6148-GE-45AF do not support these features:

- More than 1 Gbps of traffic per EtherChannel
- [WS-F6K-DFC3A](#), [WS-F6K-DFC3B](#), or [WS-F6K-DFC3BXL](#)
- ISL trunking
- Jumbo frames
- 802.1Q tunneling
- Traffic storm control

WS-X6516-GE-TX	3.45 A@42 V	16-port 10/100/1000BASE-T <ul style="list-style-type: none"> <li>• CEF256</li> <li>• With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>– dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>• With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>• QoS port architecture (Rx/Tx): <b>1p1q4t/1p2q2t</b></li> <li>• Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

## Fast Ethernet Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-FE-SFP	2.30 A@42 V	48-port 100BASE-FX <ul style="list-style-type: none"> <li>Requires <a href="#">Fast Ethernet SFPs</a></li> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p3q8t</b></li> <li>Number of ports: 48 Number of port groups: 3 Port ranges per port group: 1–16, 17–32, and 33–48</li> </ul>	
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2
WS-X6524-100FX-MM	1.90 A@42 V	24-port 100FX Ethernet multimode <ul style="list-style-type: none"> <li>CEF256</li> <li>With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>QoS port architecture (Rx/Tx): <b>1p1q0t/1p3q1t</b></li> <li>Number of ports: 24 Number of port groups: 1 Port ranges per port group: 1–24</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6324-100FX-SM WS-X6324-100FX-MM	1.52 A@42 V 1.52 A@42 V	24-port 100FX Ethernet <ul style="list-style-type: none"> <li>Single mode and multimode MT-RJ</li> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6224-100FX-MT	1.90 A@42 V	24-port 100FX Ethernet Multimode MT-RJ	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

## Ethernet/Fast Ethernet (10/100) Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-RJ-45	2.90 A@42 V	48-port 10/100TX RJ-45	
		<ul style="list-style-type: none"> <li>CEF256</li> <li>With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>QoS port architecture (Rx/Tx): <b>1p1q0t/1p3q1t</b></li> <li>Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-RJ-21	2.90 A@42 V	48-port 10/100TX RJ-21	
		<ul style="list-style-type: none"> <li>• CEF256</li> <li>• With Supervisor Engine 720:               <ul style="list-style-type: none"> <li>– dCEF256 with <a href="#">WS-F6K-DFC3BXL</a> (adds 1.47 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3B</a> (adds 1.67 A@42 V)</li> <li>– dCEF256 with <a href="#">WS-F6K-DFC3A</a> (adds 2.57 A@42 V)</li> </ul> </li> <li>• With Supervisor Engine 2, dCEF256 with <a href="#">WS-F6K-DFC</a> (adds 2.10 A@42 V)</li> <li>• QoS port architecture (Rx/Tx): <b>1p1q0t/1p3q1t</b></li> <li>• Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6148X2-RJ-45 WS-X6148X2-45AF	2.65 A@42 V 2.92 A@42 V	96-port 10/100TX RJ-45	
		<ul style="list-style-type: none"> <li>• QoS port architecture (Rx/Tx): <b>1p1q0t/1p3q1t</b></li> <li>• WS-X6148X2-RJ-45 supports <a href="#">WS-F6K-FE48X2-AF</a></li> <li>• WS-X6148X2-45AF has <a href="#">WS-F6K-FE48X2-AF</a></li> </ul>	
		With Supervisor Engine 720	12.2(18)SXF3
		With Supervisor Engine 32	12.2(18)SXF3
		With Supervisor Engine 2	12.2(18)SXF3
WS-X6196-RJ-21 WS-X6196-21AF	2.74 A@42 V 3.16 A@42 V	96-port 10/100TX RJ-21	
		<ul style="list-style-type: none"> <li>• QoS port architecture (Rx/Tx): <b>1p1q0t/1p3q1t</b></li> <li>• WS-X6196-RJ-21 supports <a href="#">WS-F6K-FE48X2-AF</a></li> <li>• WS-X6196-21AF has <a href="#">WS-F6K-FE48X2-AF</a></li> </ul>	
		With Supervisor Engine 720	12.2(18)SXF3
		With Supervisor Engine 32	12.2(18)SXF3
		With Supervisor Engine 2	12.2(18)SXF3

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6348-RJ-45 WS-X6348-RJ-45V	2.39 A@42 V 2.39 A@42 V	48-port 10/100TX RJ-45 <ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>WS-X6348-RJ-45 supports <a href="#">WS-F6K-VPWR</a></li> <li>WS-X6348-RJ-45V has <a href="#">WS-F6K-VPWR</a></li> <li>Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6348-RJ-21V	2.39 A@42 V	48-port 10/100TX RJ-21 <ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Has <a href="#">WS-F6K-VPWR</a></li> <li>Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6248-RJ-45	2.69 A@42 V	48-port 10/100TX RJ-45 <ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6248A-TEL	2.69 A@42 V	48-port 10/100TX RJ-21 <ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6248-TEL	2.69 A@42 V	48-port 10/100TX RJ-21	
		<ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 48</li> <li>Number of port groups: 4</li> <li>Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6148A-RJ-45 WS-X6148A-45AF	2.39 A@42 V 2.57 A@42 V	48-port 10/100TX RJ-45	
		<ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1p1q4t/1p3q8t</b></li> <li>WS-X6148A-RJ-45 supports <a href="#">WS-F6K-FE48-AF</a></li> <li>WS-X6148A-45AF has <a href="#">WS-F6K-FE48-AF</a></li> <li>Number of ports: 48</li> <li>Number of port groups: 6</li> <li>Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48</li> </ul>	
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2
WS-X6148-RJ-45 WS-X6148-RJ-45V WS-X6148-45AF	2.39 A@42 V 2.39 A@42 V 2.57 A@42 V	48-port 10/100TX RJ-45	
		<ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>WS-X6148-RJ-45 supports <a href="#">WS-F6K-VPWR</a> and <a href="#">WS-F6K-FE48-AF</a></li> <li>WS-X6148-RJ-45V has <a href="#">WS-F6K-VPWR</a></li> <li>WS-X6148-45AF has <a href="#">WS-F6K-FE48-AF</a></li> <li>Number of ports: 48</li> <li>Number of port groups: 4</li> <li>Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720 (except with <a href="#">WS-F6K-FE48-AF</a> )	12.2(14)SX
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-RJ-21 WS-X6148-RJ-21V WS-X6148-21AF	2.39 A@42 V 2.39 A@42 V 2.57 A@42 V	48-port 10/100TX RJ-21 <ul style="list-style-type: none"> <li>128-KB per-port packet buffers</li> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>WS-X6148-RJ-21 supports <a href="#">WS-F6K-VPWR</a> and <a href="#">WS-F6K-FE48-AF</a></li> <li>WS-X6148-RJ-21V has <a href="#">WS-F6K-VPWR</a></li> <li>WS-X6148-21AF has <a href="#">WS-F6K-FE48-AF</a></li> <li>Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48</li> </ul>	
		With Supervisor Engine 720 (except <a href="#">WS-F6K-FE48-AF</a> )	12.2(14)SX
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		<a href="#">WS-F6K-FE48-AF</a> with Supervisor Engine 2	12.2(17d)SXB

## Ethernet Switching Modules

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6024-10FL-MT	1.52 A@42 V	24-port 10BASE-FL MT-RJ <ul style="list-style-type: none"> <li>QoS port architecture (Rx/Tx): <b>1q4t/2q2t</b></li> <li>Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24</li> </ul>	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

## Optical Services Modules (OSMs)

- [OSM Guidelines and Restrictions, page 49](#)
- [Gigabit Ethernet WAN, page 49](#)
- [OC-48 Packet over SONET, page 50](#)
- [OC-48 DPT/Packet over SONET, page 50](#)
- [OC-12 Packet over SONET, page 51](#)
- [OC-3 Packet over SONET, page 51](#)



- [OC-12 Channelized](#), page 52
- [CT3/T1 Channelized/Unchannelized](#), page 52
- [OC-12 ATM](#), page 53

## OSM Guidelines and Restrictions

- [Cisco IOS Software modularity](#) does not support OSMs.
- Supervisor Engine 32 does not support OSMs.
- With Release 12.2(18)SXD and later releases, OSMs require a minimum of 128 MB of dynamic random-access memory (SDRAM)—See this publication for memory upgrade procedures:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/osmodule/app\\_upgr.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/osmodule/app_upgr.htm)
- OSMs are CEF256 modules.
- OSM WAN port numbering starts with 1.
- On OSMs with Gigabit Ethernet GBIC Layer 2 LAN ports:
  - OSM LAN port numbering starts with 1.
  - The LAN ports are in a single port group.
- In releases earlier than Release 12.2(18)SXD1, [WS-SVC-WLAN-1-K9](#) has not been tested with OSMs.
- The [OSM-2+4GE-WAN+](#) and the OC-12 Packet-over-SONET OSMs have been tested with the service modules and [WS-SUP720](#).
- In releases earlier than Release 12.2(18)SXD1, except for the OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs, the following service modules have not been tested with other OSMs:
  - [WS-X6066-SLB-APC](#) content switching module (CSM)
  - [WS-SVC-IDSM2-K9](#) intrusion detection system module
  - [WS-SVC-NAM-2](#) and [WS-SVC-NAM-1](#) network analysis modules (NAMs)
  - [WS-SVC-SSL-1](#) SSL services module

## Gigabit Ethernet WAN

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
OSM-4GE-WAN-GBIC	3.59 A @42 V	4-port Gigabit Ethernet WAN (GBIC); CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-2+4GE-WAN+	5.08 A @42 V	4-port Gigabit Ethernet WAN (GBIC) with two Layer 2 LAN ports; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-48 Packet over SONET



Note

Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-10C48-POS-SS OSM-10C48-POS-SI OSM-10C48-POS-SL	4.25 A@42 V	1-port OC-48/STM-16 SONET/SDH OSM, SM-SR; CEF256 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR; CEF256 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-10C48-POS-SI+ OSM-10C48-POS-SL+ OSM-10C48-POS-SS+	3.90 A@42 V	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR; CEF256 Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR; CEF256 Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-SR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-48 DPT/Packet over SONET



Note

Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-20C48/1DPT-SS OSM-20C48/1DPT-SI OSM-20C48/1DPT-SL	5.75 A@42 V	2-port OC-48 DPT/POS, SM-SR; CEF256 2-port OC-48 DPT/POS, SM-IR; CEF256 2-port OC-48 DPT/POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-12 Packet over SONET



Note

Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-40C12-POS-MM OSM-40C12-POS-SI OSM-40C12-POS-SL	4.78 A@42 V	4-port OC-12c/STM-4c POS, MM; CEF256 4-port OC-12c/STM-4c POS, SM-IR; CEF256 4-port OC-12c/STM-4c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-40C12-POS-SI+	4.55 A@42 V	Enhanced 4-port OC-12c/STM-4c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-20C12-POS-MM+ OSM-20C12-POS-MM OSM-20C12-POS-SI OSM-20C12-POS-SL	3.36 A@42 V	2-port OC-12c/STM-4c POS, MM; CEF256 2-port OC-12c/STM-4c POS, MM; CEF256 2-port OC-12c/STM-4c POS, SM-IR; CEF256 2-port OC-12c/STM-4c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-20C12-POS-SI+	3.36 A@42 V	Enhanced 2-port OC-12c/STM-4c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-3 Packet over SONET



Note

Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-160C3-POS-MM OSM-160C3-POS-SI OSM-160C3-POS-SL	5.09 A@42 V	16-port OC-3c/STM-1c POS, MM; CEF256 16-port OC-3c/STM-1c POS, SM-IR; CEF256 16-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-160C3-POS-SI+	4.80 A@42 V	Enhanced 16-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
OSM-80C3-POS-MM OSM-80C3-POS-SI OSM-80C3-POS-SL	3.57 A@42 V	8-port OC-3c/STM-1c POS, MM; CEF256 8-port OC-3c/STM-1c POS, SM-IR; CEF256 8-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-80C3-POS-SI+ OSM-80C3-POS-SL+	3.57 A@42 V	Enhanced 8-port OC-3c/STM-1c POS, SM-IR; CEF256 Enhanced 8-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-40C3-POS-SI	2.44 A@42 V	4-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-40C3-POS-SI+	2.44 A@42 V	Enhanced 4-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-12 Channelized



**Note** Also has four Layer 2 LAN ports.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
OSM-1CHOC12/T3-SI OSM-1CHOC12/T1-SI	4.40 A@42 V 2.80 A@42 V	1-port channelized OC-12, SM-IR; CEF256 1-port channelized OC-12, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## CT3/T1 Channelized/Unchannelized



**Note** OSM-12CT3/T1 has mini-SMB connectors for use with 75-Ohm copper coax cable.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
OSM-12CT3/T1	2.80 A@42 V	12-port channelized/unchannelized CT3/T1; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## OC-12 ATM



Note

Also has four Layer 2 LAN ports.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
OSM-20C12-ATM-MM OSM-20C12-ATM-SI	3.62 A@42 V	2-port OC-12/STM-4 ATM OSM, MM; CEF256 2-port OC-12/STM-4 ATM OSM, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-20C12-ATM-MM+ OSM-20C12-ATM-SI+	4.00 A@42 V	Enhanced 2-port OC-12/STM-4 ATM OSM, MM; CEF256 Enhanced 2-port OC-12/STM-4 ATM OSM, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

## Shared Port Adapter (SPA) Interface Processors (SIPs)



Note

- See the [“FPD Image Packages” section on page 80](#) for information about additional procedures required to support SIPs with Release 12.2(18)SXE and later releases.
- 7600-SIP-400 and 7600-SIP-600 are not supported in [PFC3A mode](#).
- [Cisco IOS Software modularity](#) does not support SIPs.

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
7600-SIP-600	8.14 A@42 V	SPA Interface Processor-600	
		<b>Note</b> 7600-SIP-600 has a <a href="#">WS-F6700-DFC3BXL</a> .	
		Supported only with Supervisor Engine 720	12.2(18)SXF
<b>Note</b> Supervisor Engine 32 does not support 7600-SIP-600.			
7600-SIP-400	6.31 A@42 V	SPA Interface Processor-400	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF
7600-SIP-200	5.72 A@42 V	SPA Interface Processor-200	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF

## Shared Port Adapters (SPAs)

These sections describe SPAs:

- [Ethernet SPAs, page 54](#)
- [POS SPAs, page 55](#)
- [ATM SPAs, page 55](#)
- [SFPs for OC3 and OC12 POS and ATM SPAs, page 56](#)
- [Serial SPAs, page 56](#)



Note

Cisco IOS Software modularity does not support SPAs.

## Ethernet SPAs

These sections describe Ethernet SPAs:

- [10-Gigabit Ethernet SPAs, page 54](#)
- [Gigabit Ethernet SPAs, page 54](#)

### 10-Gigabit Ethernet SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1XTENGE-XFP	<a href="#">7600-SIP-600</a>	1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics	12.2(18)SXF
<b>XFP Modules Supported in SPA-1XTENGE-XFP</b>			
XFP-10GLR-OC192LR	10-Gigabit Ethernet LR (10 km)		

### Gigabit Ethernet SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-10X1GE	<a href="#">7600-SIP-600</a>	10-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
SPA-5X1GE	<a href="#">7600-SIP-600</a>	5-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
SPA-2X1GE	<a href="#">7600-SIP-400</a>	2-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
<b>SFPs Supported in Gigabit Ethernet SPAs</b>			
SFP-GE-S	Extended Temperature SX SFP		
SFP-GE-L	Extended Temperature LX/LH SFP		
SFP-GE-Z	Extended Temperature ZX SFP		

## POS SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-OC192POS-VSR	<a href="#">7600-SIP-600</a>	1-port OC-192c/STM-64 POS/RPR SPA, VSR-1	12.2(18)SXF2
SPA-2XOC3-POS	<a href="#">7600-SIP-200</a> <a href="#">7600-SIP-400</a>	2-port OC-3c/STM-1c POS SPA <b>Note</b> Requires <a href="#">SFPs</a> .	12.2(18)SXE
SPA-4XOC3-POS	<a href="#">7600-SIP-200</a> <a href="#">7600-SIP-400</a>	4-port OC-3c/STM-1c POS SPA <b>Note</b> Requires <a href="#">SFPs</a> .	12.2(18)SXE
SPA-1XOC12-POS	<a href="#">7600-SIP-400</a>	1-port OC-12c/STM-4c POS SPA <b>Note</b> Requires an <a href="#">SFP</a> .	12.2(18)SXE
SPA-OC192POS-LR	<a href="#">7600-SIP-600</a>	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR	12.2(18)SXF
SPA-OC192POS-XFP	<a href="#">7600-SIP-600</a>	1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics	12.2(18)SXF
		<b>XFP Modules Supported in SPA-OC192POS-XFP</b>	
		XFP-10GLR-OC192SR Single-Mode (SM) Short Reach (SR)	
		XFP-10GER-OC192IR Single-Mode (SM) Intermediate Reach (IR-2)	
SPA-OC192POS-VSR	<a href="#">7600-SIP-600</a>	1-port OC-192c/STM-64 POS/RPR SPA, VSR-1	12.2(18)SXF1

## ATM SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-2XOC3-ATM	<a href="#">7600-SIP-200</a> <a href="#">7600-SIP-400</a>	2-port OC-3c/STM-1c ATM SPA <b>Note</b> Requires <a href="#">SFPs</a> .	12.2(18)SXE
SPA-4XOC3-ATM	<a href="#">7600-SIP-200</a> <a href="#">7600-SIP-400</a>	4-port OC-3c/STM-1c ATM SPA <b>Note</b> Requires <a href="#">SFPs</a> .	12.2(18)SXE
SPA-1XOC12-ATM	<a href="#">7600-SIP-400</a>	1-Port OC-12c/STM-4c ATM SPA <b>Note</b> Requires an <a href="#">SFP</a> .	12.2(18)SXE
SPA-1XOC48-ATM	<a href="#">7600-SIP-400</a>	1 port OC-48c/STM-16 ATM SPA	12.2(18)SXF

## SFPs for OC3 and OC12 POS and ATM SPAs

Product ID (append “=” for spares)	Product Description
SFP-OC3-MM	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC3-SR	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-IR1	OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR1	OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR2	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC12-MM	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC12-SR	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-IR1	OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength
SFP-OC12-LR1	OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-LR2	OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector

## Serial SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-8XCHT1/E1	<a href="#">7600-SIP-200</a>	8-Port Channelized T1/E1 SPA	12.2(18)SXE
SPA-2XT3/E3	<a href="#">7600-SIP-200</a>	2-port Clear Channel T3/E3 SPA	12.2(18)SXE
SPA-4XT3/E3	<a href="#">7600-SIP-200</a>	4-port Clear Channel T3/E3 SPA	12.2(18)SXE
SPA-2XCT3/DS0	<a href="#">7600-SIP-200</a>	2-port Channelized T3 to DS0 SPA	12.2(18)SXE
SPA-4XCT3/DS0	<a href="#">7600-SIP-200</a>	4-port Channelized T3 to DS0 SPA	12.2(18)SXE



## Services SPA Carrier (SSC)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
7600-SSC-400	5.43 A@42 V	Services SPA Carrier (SSC)	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF2

**Note** 7600-SSC-400 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.

## Services SPAs



**Note**

See the [“FPD Image Packages” section on page 80](#) for information about additional procedures required to support SPA-IPSEC-2G with Release 12.2(18)SXE and later releases.

Product ID (append “=” for spares)	Carrier	Product Description	Minimum Software Version
SPA-IPSEC-2G	<a href="#">7600-SSC-400</a>	IPsec SPA	12.2(18)SXE2

**Note** SPA-IPSEC-2G does not support TACACS+ authentication for IPsec. (CSCee33200)

## FlexWAN and Enhanced FlexWAN Modules



**Note**

- In releases earlier than Release 12.2(18)SXD1, [WS-SVC-WLAN-1-K9](#) has not been tested with the FlexWAN or Enhanced FlexWAN modules.
- The following service modules have not been tested with the Enhanced FlexWAN module and Release 12.2(17b)SXA, Release 12.2(17b)SXA2, or Release 12.2(17d)SXB:
  - [WS-X6066-SLB-APC](#) content switching module (CSM)
  - [WS-SVC-IDSM2-K9](#) intrusion detection system module
  - [WS-SVC-NAM-2](#) and [WS-SVC-NAM-1](#) network analysis modules (NAMs)
  - [WS-SVC-SSL-1](#) SSL services module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6582-2PA	2.50 A@42 V	Enhanced FlexWAN Module; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
<b>Note</b> See the “ <a href="#">FPD Image Packages</a> ” section on page 80 for information about additional procedures required to support WS-X6582-2PA with Release 12.2(18)SXE and later releases.			
WS-X6182-2PA	2.38 A@42 V	FlexWAN Module	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB
<b>Note</b> Supervisor Engine 32 does not support WS-X6182-2PA.			

## FlexWAN and Enhanced FlexWAN Module Port Adapters

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PA-2FE	2-port Fast Ethernet Port Adapter (supported only in <a href="#">WS-X6582-2PA</a> )	12.2(18)SXE
PA-1FE	1-port Fast Ethernet Port Adapter (supported only in <a href="#">WS-X6582-2PA</a> )	12.2(18)SXE
PA-POS-10C3	1-port Packet over SONET OC3c/STM1 Port Adapter	12.2(18)SXE
PA-POS-20C3	2-port POS OC3c/STM1	12.2(17b)SXA
<b>SFPs for PA-POS-20C3</b>		
SFP-OC3-MM	Short range, multimode fiber	12.2(17b)SXA
SFP-OC3-IR1	Intermediate range, single-mode fiber	12.2(17b)SXA
SFP-OC3-LR1	Long range, single-mode fiber	12.2(17b)SXA
PA-POS-OC3MM PA-POS-OC3SMI PA-POS-OC3SML	Packet over SONET (OC-3)	12.2(14)SX
PA-A6-OC3MM	1-port ATM OC-3c/STM-1 multimode port adapter, enhanced	12.2(14)SX
PA-A6-OC3SMI	1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced	12.2(14)SX
PA-A6-OC3SML	1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced	12.2(14)SX
PA-A6-T3	1-port ATM DS3 port adapter, enhanced	12.2(14)SX
PA-A6-E3	1-port ATM E3 port adapter, enhanced	12.2(14)SX
PA-A3-OC3MM PA-A3-OC3SMI PA-A3-T3 PA-A3-OC3SML PA-A3-E3 PA-A3-8T1IMA PA-A3-8E1IMA	ATM with traffic shaping  <b>Note</b> These port adapters do not support LANE when installed in the FlexWAN module.	12.2(14)SX

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PA-T3 PA-T3+ PA-2T3 PA-2T3+ PA-E3 PA-2E3 PA-MC-T3 PA-MC-E3 PA-MC-2T3+	T3/E3 (clear-channel and channelized)	12.2(14)SX
PA-4T+ PA-8T-V35 PA-8T-X21 PA-8T-232 PA-MC-2E1/120 PA-MC-8T1 PA-MC-8E1/120 PA-MC-2T1 PA-MC-4T1	T1/E1	12.2(14)SX
PA-4E1G/75 PA-4E1G/120	T1/E1	12.2(17)SX
PA-MC-8TE1+	Multichannel T1/E1 8PRI  <b>Note</b> This port adapter does not support ISDN PRI when installed in the FlexWAN module.	12.2(14)SX
PA-H PA-2H	HSSI	12.2(14)SX
PA-MC-STM-1	Multichannel STM-1	12.2(14)SX

## Service Modules



### Note

For any service modules that runs its own software, see the service module software release notes for information about the minimum required service module software version.

- [Application Control Engine \(ACE\) Module, page 60](#)
- [Wireless Services Module \(WiSM\), page 60](#)
- [Application-Oriented Networking Module, page 61](#)
- [WebVPN Services Module, page 61](#)
- [Anomaly Guard Module, page 61](#)
- [Traffic Anomaly Detector Module, page 62](#)
- [Wireless LAN Service Module \(WLSM\), page 63](#)
- [Persistent Storage Device \(PSD\) Module, page 63](#)
- [Multi-Processor WAN Application Module \(MWAM\), page 64](#)
- [Content Services Gateway \(CSG\) Module, page 64](#)
- [Communication Media Module \(CMM\), page 65](#)

- [IPsec VPN Acceleration Services Module](#), page 66
- [Content Switching Module with SSL \(CSM-S\)](#), page 67
- [Content Switching Module \(CSM\)](#), page 68
- [Firewall Services Module](#), page 68
- [Intrusion Detection System Modules \(IDSMs\)](#), page 69
- [Network Analysis Modules \(NAMs\)](#), page 69
- [Secure Sockets Layer \(SSL\) Services Module](#), page 70

## Application Control Engine (ACE) Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Versions
ACE10-6500-K9	5.23 A@42 V	Application Control Engine (ACE) module	
		With Supervisor Engine 720	12.2(18)SXF4

ACE10-6500-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/ace/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/ace/index.htm)

See the ACE10-6500-K9 software release notes for information about the minimum required ACE10-6500-K9 software version.

### Note

- [Cisco IOS Software modularity](#) does not support ACE10-6500-K9.
- Supervisor Engine 32 does not support ACE10-6500-K9.
- Supervisor Engine 2 does not support ACE10-6500-K9.

## Wireless Services Module (WiSM)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-WISM-1-K9	6.07 A@42 V	Wireless Services Module (WiSM)	
		With Supervisor Engine 720	12.2(18)SXF2

WS-SVC-WISM-1-K9 runs its own software—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/c44/index.htm>

See the WS-SVC-WISM-1-K9 software release notes for information about the minimum required WS-SVC-WISM-1-K9 software version.

### Note

- In Release 12.2(18)SXF4, [Cisco IOS Software modularity](#) does not support WS-SVC-WISM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-WISM-1-K9.
- Supervisor Engine 2 does not support WS-SVC-WISM-1-K9.

## Application-Oriented Networking Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-AON-1-K9	4.00 A@42 V	Application-Oriented Networking (AON) Module	
		With Supervisor Engine 720	12.2(18)SXE1

WS-SVC-AON-1-K9 runs its own software—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/aon/index.htm>

See the WS-SVC-AON-1-K9 software release notes for information about the minimum required WS-SVC-AON-1-K9 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-AON-1-K9.
- Supervisor Engine 32 does not support WS-SVC-AON-1-K9.
- Supervisor Engine 2 does not support WS-SVC-AON-1-K9.

## WebVPN Services Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-WEBVPN-K9	2.94 A@42 V	WebVPN Services Module	
		With Supervisor Engine 720	12.2(18)SXE2 12.2(17d)SXB7
		With Supervisor Engine 32	12.2(18)SXF

WS-SVC-WEBVPN-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/webvpn/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/webvpn/index.htm)

See the WS-SVC-WEBVPN-K software release notes for information about the minimum required WS-SVC-WEBVPN-K software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-WEBVPN-K9.
- Supervisor Engine 2 does not support WS-SVC-WEBVPN-K9.

## Anomaly Guard Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-AGM-1-K9	4.00 A@42 V	Anomaly Guard Module	
		With Supervisor Engine 720	12.2(18)SXD3
		With Supervisor Engine 2	12.2(18)SXD3

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
---------------------------------------	-------------------	---------------------	-----------------------------

WS-SVC-AGM-1-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/index.htm)

See the WS-SVC-AGM-1-K9 software release notes for information about the minimum required WS-SVC-AGM-1-K9 software version.

#### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-AGM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-AGM-1-K9.
- In Release 12.2(18)SXD3 and rebuilds, WS-SVC-AGM-1-K9 has not been tested with OSMs or FlexWAN modules.

## Traffic Anomaly Detector Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-ADM-1-K9	4.00 A@42 V	Traffic Anomaly Detector Module	
		With Supervisor Engine 720	12.2(18)SXD3
		With Supervisor Engine 2	12.2(18)SXD3

WS-SVC-ADM-1-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/index.htm)

See the WS-SVC-ADM-1-K9 software release notes for information about the minimum required WS-SVC-ADM-1-K9 software version.

#### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-ADM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-ADM-1-K9.
- In Release 12.2(18)SXD3 and rebuilds, WS-SVC-ADM-1-K9 has not been tested with OSMs or FlexWAN modules.

## Wireless LAN Service Module (WLSM)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-WLAN-1-K9	3.10 A@42 V	Wireless LAN service module	
		With Supervisor Engine 720	12.2(18)SXD

WS-SVC-WLAN-1-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/wlsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/wlsm/index.htm)

See the WS-SVC-WLAN-1-K9 software release notes for information about the minimum required WS-SVC-WLAN-1-K9 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-WLAN-1-K9.
- Supervisor Engine 32 does not support WS-SVC-WLAN-1-K9.
- Supervisor Engine 2 does not support WS-SVC-WLAN-1-K9.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-WLAN-1-K9 has not been tested with OSMs or FlexWAN modules.

## Persistent Storage Device (PSD) Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-PSD-1	4.00 A@42 V	Persistent Storage Device Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-PSD-1 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/psd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/psd/index.htm)

See the WS-SVC-PSD-1 software release notes for information about the minimum required WS-SVC-PSD-1 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-PSD-1.
- Supervisor Engine 32 does not support WS-SVC-PSD-1.
- With Release 12.2(18)SXD1 and later, WS-SVC-PSD-1 maintains state when an [NSF with SSO](#) redundancy mode switchover occurs.

## Multi-Processor WAN Application Module (MWAM)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-MWAM-1	3.57 A@42 V	Multi-Processor WAN Application Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 32	12.2(18)SXF5
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-MWAM-1 runs its own software—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/mwam/index.htm>

See the WS-SVC-MWAM-1 software release notes for information about the minimum required WS-SVC-MWAM-1 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-MWAM-1.
- With Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an [NSF with SSO](#) redundancy mode switchover occurs.
- With Releases earlier than Release 12.2(18)SXD1, WS-SVC-MWAM-1 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.

## Content Services Gateway (CSG) Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CSG-1	3.00 A@42 V	Content Services Gateway (CSG) Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-CSG-1 runs its own software—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrts/csg/index.htm>

See the WS-SVC-CSG-1 software release notes for information about the minimum required WS-SVC-CSG-1 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-CSG-1.
- Supervisor Engine 32 does not support WS-SVC-CSG-1.



## Communication Media Module (CMM)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CMM	6.00 A@42 V	Communication Media Module	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-CMM runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/cmm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/cmm/index.htm)

See the WS-SVC-CMM software release notes for information about the minimum required WS-SVC-CMM software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-CMM.
- Supervisor Engine 32 does not support WS-SVC-CMM.

### Communication Media Module Port Adapters

WS-SVC-CMM-6E1	6-Port E1 Interface Port Adapter	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-6T1	6-Port T1 Interface Port Adapter	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-ACT	Adhoc Conferencing and Transcoding Port Adapter	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-24FXS	24-Port FXS Interface Port Adapter	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB

## IPsec VPN Acceleration Services Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-IPSEC-1	1.89 A@42 V	IPsec VPN Acceleration Services Module	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-IPSEC-1 uses the Cisco IOS software that is running on the supervisor engine and MSFC—See this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_14459.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14459.htm)

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-IPSEC-1.
- Supervisor Engine 32 does not support WS-SVC-IPSEC-1.
- With Release 12.2(18)SXE and later releases, WS-SVC-IPSEC-1 requires an advanced services image (see the “[Feature Sets](#)” section on page 106).
- With releases earlier than Release 12.2(18)SXE, WS-SVC-IPSEC-1 requires a k9 image (see the “[Feature Sets](#)” section on page 106).
- WS-SVC-IPSEC-1 does not support TACACS+ authentication for IPsec. (CSCee33200)
- WS-SVC-IPSEC-1 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.
- WS-SVC-IPSEC-1 does not maintain state when a single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode switchover occurs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-IPSEC-1 has not been tested with [OSM-1CHOC12/T1-SI](#) or [OSM-12CT3/T1](#).
- To avoid reloads with software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases), do not configure the single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode with a WS-SVC-IPSEC-1 module installed. In software releases where caveat CSCed17605 is not resolved, the WS-SVC-IPSEC-1 module does not maintain state when an SRM with SSO redundancy mode switchover occurs.

## Content Switching Module with SSL (CSM-S)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6066-SLB-S-K9	2.15 A @42 V	Content Switching Module with SSL (CSM-S)	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 2	12.2(18)SXD

WS-X6066-SLB-S-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/csm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/index.htm)

See the WS-X6066-SLB-S-K9 software release notes for information about the minimum required WS-X6066-SLB-S-K9 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-X6066-SLB-S-K9.
- Supervisor Engine 32 does not support WS-X6066-SLB-S-K9.
- With Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-S-K9 maintains state when an [NSF with SSO](#) redundancy mode switchover occurs.
- WS-X6066-SLB-S-K9 does not maintain state when a single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode switchover occurs.
- The [OSM-2+4GE-WAN+](#) and the OC-12 Packet-over-SONET OSMs have been tested with the WS-X6066-SLB-S-K9 content switching module.
- In releases earlier than Release 12.2(18)SXD1, the WS-X6066-SLB-S-K9 content switching module has not been tested with other OSMs or the Enhanced FlexWAN module.

## Content Switching Module (CSM)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6066-SLB-APC	3.00 A@42 V	Content Switching Module	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 2	12.2(17d)SXB

WS-X6066-SLB-APC runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/csm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/index.htm)

See the WS-X6066-SLB-APC software release notes for information about the minimum required WS-X6066-SLB-APC software version.

### Note

- Supervisor Engine 32 does not support WS-X6066-SLB-APC.
- With Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-APC maintains state when an **NSF with SSO** redundancy mode switchover occurs.
- WS-X6066-SLB-APC does not maintain state when a single router mode with stateful switchover (**SRM with SSO**) redundancy mode switchover occurs.
- The **OSM-2+4GE-WAN+** and the OC-12 Packet-over-SONET OSMs have been tested with the WS-X6066-SLB-APC content switching module and **WS-SUP720**.
- In releases earlier than Release 12.2(18)SXD1, WS-X6066-SLB-APC has not been tested with other OSMs or the Enhanced FlexWAN module.

## Firewall Services Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-FWM-1-K9	4.09 A@42 V	Firewall Services Module; CEF256	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-FWM-1-K9 runs its own software—See these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm)

See the WS-SVC-FWM-1-K9 software release notes for information about the minimum required WS-SVC-FWM-1-K9 software version.

### Note

- With Release 12.2(18)SXD3 and later Cisco IOS releases and with Firewall Services Module Software Release 2.3(1), WS-SVC-FWM-1-K9 maintains state when an **NSF with SSO** redundancy mode switchover occurs.
- WS-SVC-FWM-1-K9 does not maintain state when a single router mode with stateful switchover (**SRM with SSO**) redundancy mode switchover occurs.

## Intrusion Detection System Modules (IDSMs)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-IDSM2-K9	2.50 A@42 V	Intrusion Detection System Module 2; CEF256	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-IDSM2-K9 runs its own software—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm>

See the WS-SVC-IDSM2-K9 software release notes for information about the minimum required WS-SVC-IDSM2-K9 software version.

### Note

- WS-SVC-IDSM2-K9 has been tested with [OSM-2+4GE-WAN+](#) and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-IDSM2-K9 has not been tested with other OSMs or the Enhanced FlexWAN module.

## Network Analysis Modules (NAMs)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-NAM-2	3.47 A@42 V	Network Analysis Module 2; CEF256	
WS-SVC-NAM-1	2.89 A@42 V	Network Analysis Module 1; CEF256	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-NAM-2 and WS-SVC-NAM-1 run their own software—See this publication for more information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/fam\\_mod/svc\\_namx/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/fam_mod/svc_namx/index.htm)

See the WS-SVC-NAM-2 and WS-SVC-NAM-1 software release notes for information about the minimum required WS-SVC-NAM-2 and WS-SVC-NAM-1 software version.

### Note

- With Release 12.2(17b)SXA and rebuilds and Release 12.2(17d)SXB and rebuilds, WS-SVC-NAM-2 and WS-SVC-NAM-1 support single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode.
- WS-SVC-NAM-2 and WS-SVC-NAM-1 have been tested with [OSM-2+4GE-WAN+](#) and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-NAM-2 and WS-SVC-NAM-1 have not been tested with other OSMs or the Enhanced FlexWAN module.

## Secure Sockets Layer (SSL) Services Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-SSL-1	2.94 A@42 V	Secure Sockets Layer (SSL) Services Module	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-SSL-1 runs its own software—See this publication for more information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/ssl\\_mod/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/ssl_mod/index.htm)

See the WS-SVC-SSL-1 software release notes for information about the minimum required WS-SVC-SSL-1 software version.

### Note

- [Cisco IOS Software modularity](#) does not support WS-SVC-SSL-1.
- WS-SVC-SSL-1 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.
- WS-SVC-SSL-1 does not maintain state when a single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode switchover occurs.
- WS-SVC-SSL-1 has been tested with [OSM-2+4GE-WAN+](#) and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-SSL-1 has not been tested with other OSMs or the Enhanced FlexWAN module.

## Fan Trays

- [High-Capacity Fan Trays, page 71](#)
- [Standard-Capacity Fan Trays, page 71](#)



### Note

- Enter the **show environment status | include fan** command or the **show environment cooling** command to display information about the installed fan trays.
- To use a high-capacity fan tray with a Supervisor Engine 2, you must enter the **hw-module fan-tray version 2** command and then remove and quickly reinsert the fan tray.

## High-Capacity Fan Trays

These high-capacity fan trays support both all supervisor engines.

Product ID (append “=” for spares)	Power Allocated at 42 V	Product Description	Minimum Software Version
WS-C6503-E-FAN	1.37 A@42 V	High-capacity fan tray for <a href="#">WS-C6503-E</a> chassis	12.2(14)SX
	<b>Note</b> In releases earlier than Release 12.2(18)SXD, WS-C6503-E-FAN requires the same power as FAN-MOD-3HS.		
FAN-MOD-3HS	2.98 A@42 V	High-capacity fan tray for <a href="#">WS-C6503</a> and <a href="#">CISCO7603</a> chassis	12.2(14)SX
FAN-MOD-6HS	4.29 A@42 V	High-capacity fan tray for <a href="#">CISCO7606</a> chassis	12.2(14)SX
WS-C6506-E-FAN	2.35 A@42 V	High-capacity fan tray for <a href="#">WS-C6506-E</a> chassis	12.2(14)SX
WS-C6K-6SLOT-FAN2	12 V fan	High-capacity fan tray for <a href="#">WS-C6506</a> chassis	12.2(14)SX
FAN-MOD-09	5.75 A@42 V	High-capacity fan tray for <a href="#">WS-C6509-NEB-A</a> and <a href="#">CISCO7609</a> chassis	12.2(14)SX
WS-C6509-E-FAN	3.58 A@42 V	High-capacity fan tray for <a href="#">WS-C6509-E</a> chassis	12.2(14)SX
WS-C6K-9SLOT-FAN2	12 V fan	High-capacity fan tray for <a href="#">WS-C6509</a> chassis	12.2(14)SX
WS-C6K-13SLT-FAN2	7.10 A@42 V	High-capacity fan tray for <a href="#">WS-C6513</a> and <a href="#">CISCO7613</a> chassis	12.2(14)SX

## Standard-Capacity Fan Trays

These standard-capacity fan trays support only Supervisor Engine 2.

Product ID (append “=” for spares)	Power Allocated at 42 V	Product Description	Minimum Software Version
FAN-MOD-3	None	Standard-capacity fan tray for <a href="#">WS-C6503</a> and <a href="#">CISCO7603</a> chassis	12.2(17d)SXB
FAN-MOD-6	None	Standard-capacity fan tray for <a href="#">CISCO7606</a> chassis	12.2(17d)SXB
WS-C6K-6SLOT-FAN	12 V fan	Standard-capacity fan tray for <a href="#">WS-C6506</a> chassis	12.2(17d)SXB
WS-C6509-NEB-FAN	12 V fan	Standard fan tray for <a href="#">WS-C6509-NEB</a> chassis	12.2(17d)SXB
WS-C6K-9SLOT-FAN	12 V fan	Standard-capacity fan tray for <a href="#">WS-C6509</a> chassis	12.2(17d)SXB
WS-C6K-13SLT-FAN	12 V fan	Standard-capacity fan tray for <a href="#">WS-C6513</a> and <a href="#">CISCO7613</a> chassis	12.2(17d)SXB

## Power Supplies

- [CISCO7606 Power Supplies, page 72](#)
- [WS-C6504-E and CISCO7604 Power Supplies, page 72](#)
- [WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies, page 72](#)
- [All Other Power Supplies, page 72](#)

## CISCO7606 Power Supplies

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PWR-2700-AC	2700 W AC power supply	12.2(18)SXE
PWR-2700-DC	2700 W DC power supply	12.2(18)SXE

## WS-C6504-E and CISCO7604 Power Supplies

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PWR-2700-DC/4	2700 W DC power supply	12.2(18)SXE

## WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PWR-1400-AC	1,400 W AC power supply	12.2(17a)SX
PWR-950-AC	950 W AC power supply	12.2(14)SX
PWR-950-DC	950 W DC power supply	12.2(14)SX

## All Other Power Supplies

Product ID (append “=” for spares)	Product Description	Minimum Software Version
WS-CAC-6000W	6,000 W AC power supply  <b>Note</b> <ul style="list-style-type: none"> <li>Limited to 4,000 W in <a href="#">WS-C6509</a> and <a href="#">WS-C6506</a>.</li> <li>With releases earlier than Release 12.2(18)SXD, limited to 4,000 W in <a href="#">WS-C6506-E</a> and <a href="#">WS-C6509-E</a>.</li> </ul>	12.2(18)SXD



Product ID (append “=” for spares)	Product Description	Minimum Software Version
PWR-4000-DC	4,000 W DC power supply	12.2(14)SX
WS-CAC-4000W	4,000 W AC power supply	12.2(14)SX
+WS-CAC-3000W	3,000 W AC power supply  <b>Note</b> <ul style="list-style-type: none"> <li>Required with Supervisor Engine 720 in <a href="#">WS-C6509-NEB</a> or OSR7609.</li> <li>Included in the WS-6509-NEB-UPGRD= upgrade kit.</li> </ul>	12.2(17a)SX
WS-CAC-3000W	3,000 W AC power supply	12.2(14)SX
WS-CAC-2500W	2,500 W AC power supply	12.2(14)SX
WS-CDC-2500W	2,500 W DC power supply	12.2(14)SX

## Chassis

- [13-Slot Chassis, page 73](#)
- [9-Slot Chassis, page 74](#)
- [6-Slot Chassis, page 76](#)
- [4-Slot Chassis, page 77](#)
- [3-Slot Chassis, page 78](#)

### 13-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6513	Catalyst 6513 chassis: <ul style="list-style-type: none"> <li>13 slots</li> <li>64 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires <a href="#">WS-C6K-13SLT-FAN2</a></li> <li>Does not support <a href="#">WS-C6500-SFM</a></li> <li>These modules are supported only in slots 9 through 13 and do not power up in other slots:               <ul style="list-style-type: none"> <li><a href="#">WS-X6708-10GE</a></li> <li><a href="#">WS-X6704-10GE</a></li> <li><a href="#">WS-X6748-SFP</a></li> <li><a href="#">WS-X6816-GBIC</a></li> <li><a href="#">WS-X6748-GE-TX</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spare)	Product Description	Minimum Software Version
CISCO7613	Cisco 7613 chassis: <ul style="list-style-type: none"> <li>• 13 slots</li> <li>• 64 chassis MAC addresses</li> <li>• Use with Supervisor Engine 720 requires <a href="#">WS-C6K-13SLT-FAN2</a></li> <li>• Does not support <a href="#">WS-C6500-SFM</a></li> <li>• These modules are supported only in slots 9 through 13 and do not power up in other slots:               <ul style="list-style-type: none"> <li>– <a href="#">WS-X6708-10GE</a></li> <li>– <a href="#">WS-X6704-10GE</a></li> <li>– <a href="#">WS-X6748-SFP</a></li> <li>– <a href="#">WS-X6816-GBIC</a></li> <li>– <a href="#">WS-X6748-GE-TX</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

## 9-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6509-E	Catalyst 6509 chassis: <ul style="list-style-type: none"> <li>• 9 horizontal slots</li> <li>• 1024 chassis MAC addresses</li> <li>• Requires <a href="#">WS-C6509-E-FAN</a></li> <li>• Requires 2,500 W or higher power supply</li> <li>• With releases earlier than Release 12.2(18)SXD, <a href="#">WS-CAC-6000W</a> is limited to 4,000 W in WS-C6509-E</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6509	Catalyst 6509 chassis: <ul style="list-style-type: none"> <li>9 horizontal slots</li> <li>1024 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires <a href="#">WS-C6K-9SLOT-FAN2</a></li> <li><a href="#">WS-CAC-6000W</a> is limited to 4,000 W in WS-C6509</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
WS-C6509-NEB-A	Catalyst 6509-NEB chassis <ul style="list-style-type: none"> <li>9 vertical slots</li> <li>64 chassis MAC addresses</li> <li>No fan tray upgrade required for use with Supervisor Engine 720</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
WS-C6509-NEB	Catalyst 6509-NEB chassis: <ul style="list-style-type: none"> <li>9 vertical slots</li> <li>1024 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 or Supervisor Engine 32 requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication: <a href="http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16162.htm">http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16162.htm</a></li> </ul>	
	With Supervisor Engine 720	12.2(17a)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
CISCO7609	Cisco 7609 chassis <ul style="list-style-type: none"> <li>9 vertical slots</li> <li>64 chassis MAC addresses</li> <li>No fan tray upgrade required for use with Supervisor Engine 720</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spare)	Product Description	Minimum Software Version
OSR-7609	Cisco 7609 chassis: <ul style="list-style-type: none"> <li>9 vertical slots</li> <li>1024 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication: <a href="http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16162.htm">http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16162.htm</a></li> </ul>	
	With Supervisor Engine 720	12.2(17a)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

## 6-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6506-E	Catalyst 6506 chassis: <ul style="list-style-type: none"> <li>6 slots</li> <li>1024 chassis MAC addresses</li> <li>Requires <a href="#">WS-C6506-E-FAN</a></li> <li>Requires 2,500 W or higher power supply</li> <li>With releases earlier than Release 12.2(18)SXD, <a href="#">WS-CAC-6000W</a> is limited to 4,000 W in WS-C6506-E</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
WS-C6506	Catalyst 6506 chassis: <ul style="list-style-type: none"> <li>6 slots</li> <li>1024 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires <a href="#">WS-C6K-6SLOT-FAN2</a></li> <li><a href="#">WS-CAC-6000W</a> limited to 4,000 W in WS-C6506</li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spare)	Product Description	Minimum Software Version
CISCO7606	Cisco 7606 chassis: <ul style="list-style-type: none"> <li>• 6 slots</li> <li>• 64 chassis MAC addresses</li> <li>• Use with Supervisor Engine 720 requires <a href="#">FAN-MOD-6HS</a></li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

## 4-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6504-E	Catalyst 6504-E chassis: <ul style="list-style-type: none"> <li>• 4 slots</li> <li>• 64 chassis MAC addresses</li> <li>• Does not support: <ul style="list-style-type: none"> <li>– <a href="#">Supervisor Engine 2</a></li> <li>– <a href="#">WS-X6500-SFM2</a></li> <li>– <a href="#">WS-C6500-SFM</a></li> <li>– <a href="#">WS-F6K-DFC</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720	12.2(18)SXE
	With Supervisor Engine 32	12.2(18)SXF
CISCO7604	Cisco 7604 chassis: <ul style="list-style-type: none"> <li>• 4 slots</li> <li>• 64 chassis MAC addresses</li> <li>• Does not support: <ul style="list-style-type: none"> <li>– <a href="#">Supervisor Engine 2</a></li> <li>– <a href="#">WS-X6500-SFM2</a></li> <li>– <a href="#">WS-C6500-SFM</a></li> <li>– <a href="#">WS-F6K-DFC</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720:	12.2(18)SXE
	With Supervisor Engine 32	12.2(18)SXF

### 3-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6503-E	<ul style="list-style-type: none"> <li>3 slots</li> <li>64 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires <a href="#">WS-C6503-E-FAN</a></li> <li>With Release 12.2(18)SXD and later releases, WS-C6503-E supports:               <ul style="list-style-type: none"> <li><a href="#">WS-X6704-10GE</a></li> <li><a href="#">WS-X6748-SFP</a></li> <li><a href="#">WS-X6724-SFP</a></li> <li><a href="#">WS-X6748-GE-TX</a></li> </ul> </li> <li>With releases earlier than Release 12.2(18)SXD, WS-C6503-E has the same support restrictions as <a href="#">WS-C6503</a>.</li> <li>WS-C6503-E does not support:               <ul style="list-style-type: none"> <li><a href="#">WS-X6500-SFM2</a></li> <li><a href="#">WS-C6500-SFM</a></li> <li><a href="#">WS-F6K-DFC</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
WS-C6503	Catalyst 6503 chassis: <ul style="list-style-type: none"> <li>3 slots</li> <li>64 chassis MAC addresses</li> <li>Use with Supervisor Engine 720 requires <a href="#">FAN-MOD-3HS</a></li> <li>Does not support:               <ul style="list-style-type: none"> <li><a href="#">WS-X6708-10GE</a></li> <li><a href="#">WS-X6704-10GE</a></li> <li><a href="#">WS-X6748-SFP</a></li> <li><a href="#">WS-X6724-SFP</a></li> <li><a href="#">WS-X6748-GE-TX</a></li> <li><a href="#">WS-X6500-SFM2</a></li> <li><a href="#">WS-C6500-SFM</a></li> <li><a href="#">WS-F6K-DFC</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append “=” for spare)	Product Description	Minimum Software Version
CISCO7603	Cisco 7603 chassis: <ul style="list-style-type: none"> <li>• 3 slots</li> <li>• 64 chassis MAC addresses</li> <li>• Use with Supervisor Engine 720 requires <a href="#">FAN-MOD-3HS</a></li> <li>• Does not support: <ul style="list-style-type: none"> <li>– <a href="#">WS-X6708-10GE</a></li> <li>– <a href="#">WS-X6704-10GE</a></li> <li>– <a href="#">WS-X6748-SFP</a></li> <li>– <a href="#">WS-X6724-SFP</a></li> <li>– <a href="#">WS-X6748-GE-TX</a></li> <li>– <a href="#">WS-X6500-SFM2</a></li> <li>– <a href="#">WS-C6500-SFM</a></li> <li>– <a href="#">WS-F6K-DFC</a></li> </ul> </li> </ul>	
	With Supervisor Engine 720:	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB

**Note** Supervisor Engine 32 does not support CISCO7603.

## Unsupported Hardware

The following hardware is not supported:

- See the “[Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A\)](#)” section on [page 15](#) for information about hardware that is not supported with the Supervisor Engine 32.
- With a Supervisor Engine 720, [WS-X6516-GBIC](#) hardware revisions 5.0 through 5.4 with a DFC3 installed.

Supervisor Engine 720 supports a DFC3 on these [WS-X6516-GBIC](#) hardware revisions:

- Lower than 5.0
- 5.5 and higher

With a Supervisor Engine 720 and a DFC3 installed, [WS-X6516-GBIC](#) hardware revisions 5.0 through 5.3 do not power up. Without a DFC3, [WS-X6516-GBIC](#) hardware revisions 5.0 through 5.4 operate in bus mode.

See external field notice 24494 for more information:

<http://www.cisco.com/warp/public/770/fn24494.shtml>

- These service modules:
  - WS-X6381-IDS Intrusion Detection System (IDS) Module
  - WS-X6380-NAM Network Analysis Module (NAM)
- Supervisor Engine 1 (WS-X6K-S1A-MSFC2, WS-X6K-SUP1A-MSFC)
- WS-X6624-FXS, WS-X6608-T1, and WS-X6608-E1 voice modules

- WS-X6101-OC12-MMF and WS-X6101-OC12-SMF ATM LANE modules
- WS-X6302-MSM Multilayer Switch Module
- Catalyst 6000 series chassis
- These power supplies cannot support high-capacity fan trays:
  - WS-CAC-1300W
  - WS-CDC-1300W
  - WS-CAC-1000W

Unsupported modules remain powered down if detected and do not affect system behavior.

## FPD Image Packages



### Note

- Field Programmable Device (FPD) image packages were first introduced on the Catalyst 6500 series switches and Cisco 7600 series routers in Release 12.2(18)SXE.
- FPD image packages update FPD images. If a discrepancy exists between an FPD image and the Cisco IOS image, the module that has the FPD discrepancy is deactivated until the discrepancy is resolved.

These sections describe FPD packages:

- [FPD-Image Dependant Modules, page 80](#)
- [FPD Image Package Contents, page 81](#)
- [FPD Upgrades, page 104](#)

## FPD-Image Dependant Modules

In Release 12.2(18)SXE and later releases, these modules use FPD images:

- Shared Port Adapter ([SPA](#)) Interface Processors ([SIPs](#))
- Shared Port Adapters
- Enhanced FlexWAN Module ([WS-X6582-2PA](#))



### Note

With Release 12.2(18)SXE2 and later releases, you do not need to do a separate FPD image upgrade for the Enhanced FlexWAN module, because the Cisco IOS software images contain the FPD image for the Enhanced FlexWAN module. The FPD image package also includes the FPD image for the Enhanced FlexWAN module. (CSCin90971)



## FPD Image Package Contents

These sections describe the FPD image package contents:

- [Release 12.2\(18\)SXF6 FPD Image Package Contents, page 81](#)
- [Release 12.2\(18\)SXF5 FPD Image Package Contents, page 81](#)
- [Release 12.2\(18\)SXF4 FPD Image Package Contents, page 83](#)
- [Release 12.2\(18\)SXF3 FPD Image Package Contents, page 85](#)
- [Release 12.2\(18\)SXF2 FPD Image Package Contents, page 87](#)
- [Release 12.2\(18\)SXF1 FPD Image Package Contents, page 89](#)
- [Release 12.2\(18\)SXF FPD Image Package Contents, page 90](#)
- [Release 12.2\(18\)SXE6a FPD Image Package Contents, page 92](#)
- [Release 12.2\(18\)SXE6 FPD Image Package Contents, page 94](#)
- [Release 12.2\(18\)SXE5 FPD Image Package Contents, page 96](#)
- [Release 12.2\(18\)SXE4 FPD Image Package Contents, page 98](#)
- [Release 12.2\(18\)SXE3 FPD Image Package Contents, page 100](#)
- [Release 12.2\(18\)SXE2 FPD Image Package Contents, page 102](#)
- [Release 12.2\(18\)SXE1 FPD Image Package Contents, page 103](#)

### Release 12.2(18)SXF6 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF6.pkg** command:

### Release 12.2(18)SXF5 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF5.pkg** command:

```
Cisco Field Programmable Device Image Package for IOS
C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXF5.pkg), Version 12.2(18)SXF5
Copyright (c) 2004-2006 by cisco Systems, Inc.
Built Sun 02-Jul-2006 20:09 by
```

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140

	1 CTE1 SPA ROMMON NP	2.12	0.0
	2 CTE1 SPA I/O FPGA	2.5	0.0
2-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	2.5	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	1.4	0.200
4-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	2.5	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	1.4	0.200
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.14	0.0
	2 SNOOP BUS FPGA	0.3	0.0
10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.3	0.100
SIP-400	1 SIP-400 ROMMON	1.3	0.1

	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
-----			
SIP-600	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.3	0.1
	3 SIP-600 PKT ENG FPGA	0.5	0.1
-----			
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.1	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.3	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.48	2.0
	3 CWPA2 CPU0 ROMMON	1.3	0.1
	4 CWPA2 CPU1 ROMMON	1.3	0.1
=====			

## Release 12.2(18)SXF4 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF4.pkg** command:

```
Cisco Field Programmable Device Image Package for IOS
C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXF4.pkg), Version 12.2(18)SXF4
Copyright (c) 2004-2006 by cisco Systems, Inc.
Built Thu 23-Mar-2006 16:01 by
```

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	2.1	0.0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	1.4	0.200
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	1.4	0.200

2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.14	0.0
	2 SNOOP BUS FPGA	0.3	0.0
10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.3	0.100
SIP-400	1 SIP-400 ROMMON	1.3	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
SIP-600	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.3	0.1
	3 SIP-600 PKT ENG FPGA	0.5	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.1	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.3	0.3

CWA2	1 CWA2 I/O FPGA P1	0.37	0.1
	1 CWA2 I/O FPGA P7	0.39	2.0
	2 CWA2 EOS FPGA P1	0.28	0.1
	2 CWA2 EOS FPGA P7	0.48	2.0
	3 CWA2 CPU0 ROMMON	1.3	0.1
	4 CWA2 CPU1 ROMMON	1.3	0.1

## Release 12.2(18)SXF3 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF3.pkg** command:

Cisco Field Programmable Device Image Package for IOS  
 C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXF3.pkg), Version 12.2(18)SXF3  
 Copyright (c) 2004-2006 by cisco Systems, Inc.  
 Built Tue 14-Feb-2006 14:02 by

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	2.1	0.0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1	1-Port POS/RPR SPA IOFPGA	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1	1-Port POS/RPR SPA IOFPGA	1.2	2.0

2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.14	0.0
	2 SNOOP BUS FPGA	0.3	0.0
10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.3	0.100
SIP-400	1 SIP-400 ROMMON	1.3	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
SIP-600	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.3	0.1
	3 SIP-600 PKT ENG FPGA	0.5	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.1	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.3	0.3
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.48	2.0
	3 CWPA2 CPU0 ROMMON	1.3	0.1
	4 CWPA2 CPU1 ROMMON	1.3	0.1

## Release 12.2(18)SXF2 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF2.pkg** command:

Cisco Field Programmable Device Image Package for IOS  
 C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXF2.pkg), Version 12.2(18)SXF2  
 Copyright (c) 2004-2006 by cisco Systems, Inc.  
 Built Thu 19-Jan-2006 01:08 by

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	2.1	0.0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
	1	1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
2-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.14	0.0
	2	SNOOP BUS FPGA	0.3	0.0

10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPsec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
SIP-400	5 SIP-200 ROMMON	1.3	0.100
	1 SIP-400 ROMMON	1.3	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
SIP-600	3 SIP-400 SWITCH FPGA	0.25	0.1
	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.3	0.1
SSC-600	3 SIP-600 PKT ENG FPGA	0.5	0.1
	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.1	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
CWPA2	4 SSC-600 ROMMON	1.3	0.3
	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.48	2.0
	3 CWPA2 CPU0 ROMMON	1.3	0.1
	4 CWPA2 CPU1 ROMMON	1.3	0.1



## Release 12.2(18)SXF1 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF1.pkg** command:

```
Cisco Field Programmable Device Image Package for IOS
C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXF1.pkg), Version 12.2(18)SXF1
Copyright (c) 2004-2005 by cisco Systems, Inc.
Built Wed 21-Dec-2005 09:14 by kellmill
```

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.6	0.0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.4	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.4	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1	1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
	1	1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
2-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1	KATM OC48 SPA IOFPGA	0.14	0.0
	2	SNOOP BUS FPGA	0.3	0.0

10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPsec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.3	0.100
SIP-400	1 SIP-400 ROMMON	1.3	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.25	0.1
SIP-600	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.2	0.1
	3 SIP-600 PKT ENG FPGA	0.5	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.48	2.0
	3 CWPA2 CPU0 ROMMON	1.3	0.1
	4 CWPA2 CPU1 ROMMON	1.3	0.1

## Release 12.2(18)SXF FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXF.pkg** command:

Bundled FPD Image Version Matrix			
Supported Card Types	ID	Image Name	Version
Min. Req. H/W Ver.			
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12
			0.0

	2 T3E3 SPA I/O FPGA	0.24	0.0
	3 T3E3 SPA E3 FPGA	0.6	0.0
	4 T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1 T3E3 SPA ROMMON	2.12	0.0
	2 T3E3 SPA I/O FPGA	0.24	0.0
	3 T3E3 SPA E3 FPGA	0.6	0.0
	4 T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1 CTE1 SPA ROMMON	2.12	0.140
	1 CTE1 SPA ROMMON NP	2.12	0.0
	2 CTE1 SPA I/O FPGA	1.6	0.0
2-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	1.4	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	1.4	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA P1	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA P2	1.2	2.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.14	0.0
	2 SNOOP BUS FPGA	0.3	0.0
10-port GE SPA	1 GE SPA FPGA	1.8	0.0
5-port GE SPA	1 GE SPA FPGA	1.8	0.0
2-port GE SPA	1 GE SPA FPGA	1.8	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.7	0.0
2-port IPsec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500

	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.218	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.131	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.3	0.100
-----			
SIP-400	1 SIP-400 ROMMON	1.3	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.25	0.1
-----			
SIP-600	1 SIP-600 ROMMON	1.3	0.1
	2 SIP-600 I/O FPGA	0.2	0.1
	3 SIP-600 PKT ENG FPGA	0.5	0.1
-----			
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.48	2.0
	3 CWPA2 CPU0 ROMMON	1.3	0.1
	4 CWPA2 CPU1 ROMMON	1.3	0.1
=====			

## Release 12.2(18)SXE6a FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE6a.pkg** command:

Cisco Field Programmable Device Image Package for IOS  
 C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXE6a.pkg), Version 12.2(18)SXE6a  
 Copyright (c) 2004-2006 by cisco Systems, Inc.  
 Built Thu 14-Sep-2006 16:15 by

Bundled FPD Image Version Matrix				
=====				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
=====				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
-----				
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100

	2 CT3 SPA I/O FPGA	2.4	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	1.4	0.200
-----	-----	-----	-----
4-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	2.4	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	1.4	0.200
-----	-----	-----	-----
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
2-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
-----	-----	-----	-----
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA	1.2	2.0
-----	-----	-----	-----
1-port OC-48 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
-----	-----	-----	-----
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
2-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
4-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
2-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.10	0.0
-----	-----	-----	-----
10-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
5-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
2-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
1-port 10GE SPA	1 10GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
1-port 10GE FH SPA	1 10GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
-----	-----	-----	-----
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600

	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.2	0.100
-----			
SIP-400	1 SIP-400 ROMMON	1.2	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
-----			
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1
=====			

## Release 12.2(18)SXE6 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE6.pkg** command:

Cisco Field Programmable Device Image Package for IOS  
 C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXE6.pkg), Version 12.2(18)SXE6  
 Copyright (c) 2004-2006 by cisco Systems, Inc.  
 Built Mon 05-Jun-2006 15:22 by

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
=====				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
-----				
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	2.4	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	1.4	0.200

4-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	2.4	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	1.4	0.200
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
2-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA	1.2	2.0
1-port OC-48 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.10	0.0
10-port GE SPA	1 GE SPA FPGA	1.6	0.0
5-port GE SPA	1 GE SPA FPGA	1.6	0.0
2-port GE SPA	1 GE SPA FPGA	1.6	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.6	0.0
1-port 10GE FH SPA	1 10GE SPA FPGA	1.6	0.0
2-port IPsec SPA	1 PROM	1.1	0.1
	2 Lodi	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100

	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.2	0.100
-----			
SIP-400	1 SIP-400 ROMMON	1.2	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
-----			
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1
=====			

## Release 12.2(18)SX-E5 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE5.pkg** command:

Cisco Field Programmable Device Image Package for IOS  
 C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXE5.pkg), Version 12.2(18)SX-E5  
 Copyright (c) 2004-2006 by cisco Systems, Inc.  
 Built Wed 08-Feb-2006 13:30 by

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
=====				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
-----				
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
-----				
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100



	2 CT3 SPA I/O FPGA	1.1	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	0.15	0.200
-----	-----	-----	-----
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
2-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
-----	-----	-----	-----
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
-----	-----	-----	-----
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA	1.2	2.0
-----	-----	-----	-----
1-port OC-48 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
-----	-----	-----	-----
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
2-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
4-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
2-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
-----	-----	-----	-----
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.10	0.0
-----	-----	-----	-----
10-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
5-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
2-port GE SPA	1 GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
1-port 10GE SPA	1 10GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
1-port 10GE FH SPA	1 10GE SPA FPGA	1.6	0.0
-----	-----	-----	-----
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
-----	-----	-----	-----
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600

	5 SIP-200 ROMMON	1.2	0.100
SIP-400	1 SIP-400 ROMMON	1.2	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.29	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1

## Release 12.2(18)SXE4 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE4.pkg** command:

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0

	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
2-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA	1.2	2.0
1-port OC-48 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.10	0.0
10-port GE SPA	1 GE SPA FPGA	1.6	0.0
5-port GE SPA	1 GE SPA FPGA	1.6	0.0
2-port GE SPA	1 GE SPA FPGA	1.6	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.6	0.0
1-port 10GE FH SPA	1 10GE SPA FPGA	1.6	0.0
2-port IPsec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.2	0.100
SIP-400	1 SIP-400 ROMMON	1.2	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.25	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3

	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1
=====			

## Release 12.2(18)SXE3 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE3.pkg** command:

```
Cisco Field Programmable Device Image Package for IOS
C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXE3.pkg), Version 12.2(18)
SXE3
Copyright (c) 2004-2005 by cisco Systems, Inc.
Built Wed 17-Aug-2005 01:27 by
```

Bundled FPD Image Version Matrix				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
-----				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
-----				
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
-----				
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
-----				
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
-----				
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
-----				
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0

	1 POS SPA IOFPGA P2	3.4	0.200
2-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC-192 POS/SRP FH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
1-port OC-192 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
	1 1-Port POS/RPR SPA IOFPGA	1.2	2.0
1-port OC-48 POS/SRP HH SPA	1 1-Port POS/RPR SPA IOFPGA	1.2	0.0
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port DS3E3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
2-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC48 ATM SPA	1 KATM OC48 SPA IOFPGA	0.10	0.0
10-port GE SPA	1 GE SPA FPGA	1.6	0.0
5-port GE SPA	1 GE SPA FPGA	1.6	0.0
2-port GE SPA	1 GE SPA FPGA	1.6	0.0
1-port 10GE SPA	1 10GE SPA FPGA	1.6	0.0
1-port 10GE FH SPA	1 10GE SPA FPGA	1.6	0.0
2-port IPSec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.2	0.100
SIP-400	1 SIP-400 ROMMON	1.2	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.25	0.1
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4

	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1
=====			

## Release 12.2(18)SX-E2 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE2.pkg** command:

Bundled FPD Image Version Matrix				
=====				
		Min. Req.		
Supported Card Types	ID	Image Name	Version	H/W Ver.
=====				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0
-----				
2-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
-----				
4-port Channelized T3 SPA	1	CT3 SPA ROMMON	2.12	0.100
	2	CT3 SPA I/O FPGA	1.1	0.100
	3	CT3 SPA T3 FPGA R1	0.11	0.100
	3	CT3 SPA T3 FPGA R2	0.15	0.200
-----				
2-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
-----				
4-port OC3 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
-----				
1-port OC12 POS SPA	1	POS SPA IOFPGA P1	3.4	0.0
	1	POS SPA IOFPGA P2	3.4	0.200
-----				
2-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
-----				
4-port OC3 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
-----				
1-port OC12 ATM SPA	1	KATM SPA IOFPGA	1.24	0.0
-----				

2G IPsec SPA	1 PROM	1.1	0.1
	2 LODI	1.21	0.1
	3 Sequoia	1.1	0.1
-----			
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
	5 SIP-200 ROMMON	1.2	0.100
-----			
SIP-400	1 SIP-400 ROMMON	1.1	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
	3 SIP-400 SWITCH FPGA	0.25	0.1
-----			
SSC-600	1 SSC-600 I/O FPGA	1.0	0.3
	2 SSC-600 DP RX FPGA	1.0	0.3
	3 SSC-600 DP TX FPGA P3	0.12288	0.3
	3 SSC-600 DP TX FPGA P4	0.16384	0.4
	3 SSC-600 DP TX FPGA P5	1.3	0.5
	4 SSC-600 ROMMON	1.2	0.3
-----			
CWPA2	1 CWPA2 I/O FPGA P1	0.37	0.1
	1 CWPA2 I/O FPGA P7	0.39	2.0
	2 CWPA2 EOS FPGA P1	0.28	0.1
	2 CWPA2 EOS FPGA P7	0.47	2.0
	3 CWPA2 CPU0 ROMMON	1.2	0.1
	4 CWPA2 CPU1 ROMMON	1.2	0.1
=====			

## Release 12.2(18)SX-E1 FPD Image Package Contents

This is the information displayed by the **show upgrade fpd file c7600-fpd-pkg.122-18.SXE1.pkg** command:

Bundled FPD Image Version Matrix				
=====				
Supported Card Types	ID	Image Name	Version	Min. Req. H/W Ver.
=====				
2-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
4-port T3/E3 Serial SPA	1	T3E3 SPA ROMMON	2.12	0.0
	2	T3E3 SPA I/O FPGA	0.24	0.0
	3	T3E3 SPA E3 FPGA	0.6	0.0
	4	T3E3 SPA T3 FPGA	0.14	0.0
-----				
8-port Channelized T1/E1 SPA	1	CTE1 SPA ROMMON	2.12	0.140
	1	CTE1 SPA ROMMON NP	2.12	0.0
	2	CTE1 SPA I/O FPGA	1.2	0.0

2-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	1.1	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	0.15	0.200
4-port Channelized T3 SPA	1 CT3 SPA ROMMON	2.12	0.100
	2 CT3 SPA I/O FPGA	1.1	0.100
	3 CT3 SPA T3 FPGA R1	0.11	0.100
	3 CT3 SPA T3 FPGA R2	0.15	0.200
2-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
4-port OC3 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
1-port OC12 POS SPA	1 POS SPA IOFPGA P1	3.4	0.0
	1 POS SPA IOFPGA P2	3.4	0.200
2-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
4-port OC3 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
1-port OC12 ATM SPA	1 KATM SPA IOFPGA	1.24	0.0
SIP-200	1 SIP-200 I/O FPGA P1	1.1	0.100
	1 SIP-200 I/O FPGA P4	1.1	0.400
	1 SIP-200 I/O FPGA P6	1.1	0.600
	2 SIP-200 EOS FPGA P1	0.27	0.100
	2 SIP-200 EOS FPGA P450	1.211	0.450
	2 SIP-200 EOS FPGA P5	0.27	0.500
	2 SIP-200 EOS FPGA P550	1.211	0.550
	2 SIP-200 EOS FPGA P6	1.211	0.600
	3 SIP-200 PEG TX FPGA P1	1.129	0.100
	3 SIP-200 PEG TX FPGA P6	1.129	0.600
	4 SIP-200 PEG RX FPGA P1	1.3	0.100
	4 SIP-200 PEG RX FPGA P4	1.3	0.400
	4 SIP-200 PEG RX FPGA P6	1.3	0.600
SIP-400	5 SIP-200 ROMMON	1.2	0.100
	1 SIP-400 ROMMON	1.1	0.1
	2 SIP-400 I/O FPGA	0.82	0.1
CWA2	3 SIP-400 SWITCH FPGA	0.25	0.1
	1 CWA2 I/O FPGA P1	0.37	0.1
	2 CWA2 EOS FPGA P1	0.28	0.1
CWA2	3 CWA2 ROMMON	1.1	0.1

## FPD Upgrades



### Note

With Release 12.2(18)SX2 and later releases, you do not need to do a separate FPD image upgrade for the Enhanced FlexWAN module, because the Cisco IOS software images contain the FPD image for the Enhanced FlexWAN module. The FPD image package also includes the FPD image for the Enhanced FlexWAN module. (CSCin90971)



See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspasw/76fpdspa/index.htm>

## Cisco IOS Software Modularity

These sections describe Cisco IOS Software Modularity:

- [Cisco IOS Software Modularity Images, page 105](#)
- [Cisco IOS Software Modularity Documentation, page 105](#)
- [Cisco IOS Software Modularity Unsupported Features, page 105](#)

## Cisco IOS Software Modularity Images

See the “Supervisor Engine 720 Images in Release 12.2(18)SXF and Rebuilds” section on page 109 and the “Supervisor Engine 32 Images in Release 12.2(18)SXF and Rebuilds” section on page 112 for information about the Cisco IOS Software Modularity images.

## Cisco IOS Software Modularity Documentation

See these publications for information about Cisco IOS Software Modularity:

- Cisco IOS Software Modularity Installation and Configuration:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxfl8/mod\\_iosc.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxfl8/mod_iosc.htm)
- Cisco IOS Software Modularity Command Reference:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxfl8/mod/index.htm>
- Embedded Event Manager:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxfl8/evnt\\_mgr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxfl8/evnt_mgr/index.htm)

## Cisco IOS Software Modularity Unsupported Features

Cisco IOS Software Modularity does not support these features:

- Hardware:
  - All Optical Services Modules (OSMs)
  - All SIPs and SPAs
  - ACE10-6500-K9 Application Control Engine (ACE) module
  - WS-SVC-ADM-1-K9 Traffic Anomaly Detector Module
  - WS-SVC-AGM-1-K9 Anomaly Guard Module
  - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) Module
  - WS-SVC-CMM Communication Media Module

- WS-SVC-CSG-1 Content Services Gateway (CSG) Module
- WS-SVC-IPSEC-1 IPsec VPN Acceleration Services Module
- WS-SVC-MWAM-1 Multi-Processor WAN Application Module
- WS-SVC-PSD-1 Persistent Storage Device Module
- WS-SVC-SSL-1 Secure Sockets Layer (SSL) Services Module
- WS-SVC-WEBVPN-K9 WebVPN Services Module
- WS-SVC-WLAN-1-K9 Wireless LAN service module
- WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S)
- In Release 12.2(18)SXF4, WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)
- Software:
  - See the *Cisco IOS Software Modularity Command Reference* “[Introduction](#)” for detailed information about specific commands that are not supported in Cisco IOS Software Modularity images.
  - IPv6 and all IPv6-related features
  - MPLS and all MPLS-related features
  - Bidirectional Forwarding Detection (BFD), Integrated IS-IS support for BFD over IPv4, and OSPF support for BFD over IPv4
  - Control Plane DSCP Support for RSVP
  - IDSM-2 EtherChannel load balancing
  - Integrated IS-IS Global Default Metric
  - RSVP Scalability Enhancements
  - In Release 12.2(18)SXF4, Multi-VRF (VRF Lite)

## Feature Sets

These sections describe the feature sets in Release 12.2SX:

- [Feature Set Guidelines and Restrictions, page 107](#)
- [Feature Set Descriptions, page 108](#)
- [Feature Sets in Release 12.2\(18\)SXF, page 109](#)
- [Feature Sets in Release 12.2\(18\)SXE and Rebuilds, page 116](#)
- [Feature Sets in Release 12.2\(18\)SXD and Rebuilds, page 118](#)
- [Feature Sets in Release 12.2\(17d\)SXB and Rebuilds, page 125](#)
- [Feature Sets in Release 12.2\(17b\)SXA and Rebuilds \(Deferred\), page 134](#)
- [Feature Sets in Release 12.2\(17a\)SX and Rebuilds \(Deferred\), page 134](#)
- [Feature Sets in Release 12.2\(14\)SX and Rebuilds \(Deferred\), page 134](#)

## Feature Set Guidelines and Restrictions

These are the feature set guidelines and restrictions:

- There are no 12.2SX boot loader images: none are required.
- The releases includes strong encryption images. Strong encryption images are subject to U.S. and local country export, import, and use laws. The country and class of end users eligible to receive and use Cisco encryption solutions are limited. See this publication for more information:  
[http://www.cisco.com/cgi-bin/Software/Crypto/crypto\\_main.pl](http://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl)
- Many TFTP server implementations cannot transfer 16 MB or larger files. To transfer 16 MB or larger files, you might need to use FTP or rcp. See this online publication for procedures:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/ffun\\_c/ffcprt2/fcf008.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/ffun_c/ffcprt2/fcf008.htm)
- These features are not supported in Release 12.2(18)SXD and later releases:
  - Apollo Domain
  - AppleTalk EIGRP
  - Banyan Vines
  - Exterior Gateway Protocol (EGP)
  - HP Probe
  - IEEE 802.10 VLANs
  - IGRP
  - LAN Extension
  - NetWare Asynchronous Services Interface (NASI)
  - Next Hop Resolution Protocol (NHRP) for IPX
  - Novell Link-State Protocol (NLSP)
  - Simple Multicast Routing Protocol (SMRP) for Appletalk
  - Xerox Network Systems (XNS)
  - Xremote
- With releases earlier than Release 12.2(18)SXE, use of the EGP, BGP4, and IS-IS routing protocols requires the additional purchase of the InterDomain Routing Feature License (FR-IRC6), except when the price of the feature set already includes FR-IRC6.
- In Release 12.2(17d)SXB and later releases, the price of any Cisco 7600 series router feature set (part numbers starting with “S763”) includes FR-IRC6.
- In Release 12.2(17b)SXA and later releases, the price of the “IP MPLS, IPv6, and BGP Feature Set” image (S733ZK9M-122\* or S763ZK9M-122\*) includes FR-IRC6.

## Feature Set Descriptions

This section lists all of the features that are unique to each feature set and some of the features that are common to all feature sets. See the [“New Features” section on page 135](#) for a more complete list of supported features.

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
<a href="#">Firewall Feature Set</a>					X
<b>Note</b> Not required with the <a href="#">WS-SVC-FWM-1-K9</a> Firewall Services Module.					
<a href="#">TCP Intercept</a>					X
IPsec Network Security			X		X
<b>Note</b> <ul style="list-style-type: none"> <li>The <a href="#">SPA-IPSEC-2G</a> and the <a href="#">IPsec VPN Acceleration Services Module</a> support IPsec Network Security in hardware.</li> <li>Without a SPA-IPSEC-2G or IPsec VPN Acceleration Services Module, the <a href="#">IPsec Network Security</a> feature (configured with the <b>crypto ipsec</b> command) is supported in software only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.</li> </ul>					
MPLS (Search for “MPLS” in the <a href="#">“New Features” section on page 135</a> for information about supported MPLS features.)			X		X
VPNs (Search for “VPN” in the <a href="#">“New Features” section on page 135</a> for information about supported VPN features.)			X		X
<a href="#">DECNet</a>				X	X
<a href="#">ISO CLNS</a>				X	X
<a href="#">Novell IPX</a>				X	X
IPv6 (Search for “IPv6” in the <a href="#">“New Features” section on page 135</a> for information about supported IPv6 features.)			X	X	X
SLB (Search for “SLB” in the <a href="#">“New Features” section on page 135</a> for information about supported SLB features.)			X	X	X
<a href="#">IS-IS</a>			X	X	X
<a href="#">BGP4</a>		X	X	X	X
<a href="#">MBGP</a>		X	X	X	X
VRF Lite (Search for “VRF Lite” in the <a href="#">“New Features” section on page 135</a> for information about supported VRF Lite features.)		X	X	X	X
<a href="#">Bidirectional PIM</a>		X	X	X	X
<a href="#">EIGRP</a>		X	X	X	X
<a href="#">MSDP</a>		X	X	X	X
<a href="#">OSPF</a>		X	X	X	X

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
PBR (Search for “PBR” in the <a href="#">“New Features” section on page 135</a> for information about supported PBR features.)		X	X	X	X
NetFlow (Search for “NetFlow” in the <a href="#">“New Features” section on page 135</a> for information about supported NetFlow features.)	X	X	X	X	X
<a href="#">EIGRP Stub Routing</a>	X	X	X	X	X
<a href="#">HSRP</a>	X	X	X	X	X
<a href="#">IGMP</a>	X	X	X	X	X
<a href="#">IPsec Triple DES Encryption (3DES) for SSH</a>	X	X	X	X	X
<b>Note</b> <ul style="list-style-type: none"> <li>The SSH k9 images support SSH 3DES access in software on the MSFC.</li> <li>The k9 images in Release 12.2(17d)SXB and later releases support both SSHv2 server and SSHv2 client features.</li> <li>The k9 images in releases earlier than Release 12.2(17d)SXB support only SSHv2 server features.</li> </ul>					
PIMv1, PIMv2 (Search for “PIM” in the <a href="#">“New Features” section on page 135</a> for information about supported PIM features.)	X	X	X	X	X
<a href="#">RIPv1, RIPv2</a>	X	X	X	X	X

## Feature Sets in Release 12.2(18)SXF

These sections describe the feature sets in Release 12.2(18)SXF:

- [Supervisor Engine 720 Images in Release 12.2\(18\)SXF and Rebuilds, page 109](#)
- [Supervisor Engine 32 Images in Release 12.2\(18\)SXF and Rebuilds, page 112](#)
- [Supervisor Engine 2 Images in Release 12.2\(18\)SXF Rebuilds, page 115](#)

## Supervisor Engine 720 Images in Release 12.2(18)SXF and Rebuilds

These sections describe the Supervisor Engine 720 images:

- [Supervisor Engine 720 Advanced Enterprise Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 110](#)
- [Supervisor Engine 720 Enterprise Services for Release 12.2\(18\)SXF and Rebuilds, page 110](#)
- [Supervisor Engine 720 Advanced IP Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 111](#)
- [Supervisor Engine 720 IP Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 111](#)



### Note

Release 12.2(18)SXF and later releases support the [CompactFlash adapter and 512 MB CompactFlash card \(WS-CF-UPG=\)](#), which replaces the 64 MB bootflash device.

## Supervisor Engine 720 Advanced Enterprise Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-adventerprisek9_wan-vz.122-18.SXF6 (88,393,360)	<a href="#">ADVANCED ENTERPRISE SERVICES SSH (MODULAR)</a> CAT6000-SUP720/MSFC3: S733AEK9M-12218SXF
s72033-adventerprisek9_wan-vz.122-18.SXF5 (88,334,992)	
s72033-adventerprisek9_wan-vz.122-18.SXF4 (78,965,904)	
<b>Note</b> This is a limited-access strong encryption image.	
s72033-adventerprisek9_wan-mz.122-18.SXF6 (82,484,292)	<a href="#">ADVANCED ENTERPRISE SERVICES SSH</a> CAT6000-SUP720/MSFC3: S733AEK9-12218SXF 7600-SUP720/MSFC3: S763AEK9-12218SXF
s72033-adventerprisek9_wan-mz.122-18.SXF5 (82,433,604)	
s72033-adventerprisek9_wan-mz.122-18.SXF4 (76,971,076)	
s72033-adventerprisek9_wan-mz.122-18.SXF3 (76,945,476)	
s72033-adventerprisek9_wan-mz.122-18.SXF2 (76,913,220)	
s72033-adventerprisek9_wan-mz.122-18.SXF1 (76,603,972)	
s72033-adventerprisek9_wan-mz.122-18.SXF (76,597,828)	
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 720 Enterprise Services for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-entservicesk9_wan-vz.122-18.SXF6 (88,388,240)	<a href="#">ENTERPRISE SERVICES SSH (MODULAR)</a> CAT6000-SUP720/MSFC3: S733ESK9M-12218SXF
s72033-entservicesk9_wan-vz.122-18.SXF5 (88,324,240)	
s72033-entservicesk9_wan-vz.122-18.SXF4 (78,956,176)	
<b>Note</b> This is a limited-access strong encryption image.	
s72033-entservicesk9_wan-mz.122-18.SXF6 (81,727,524)	<a href="#">ENTERPRISE SERVICES SSH</a> CAT6000-SUP720/MSFC3: S733ESK9-12218SXF
s72033-entservicesk9_wan-mz.122-18.SXF5 (81,680,932)	
s72033-entservicesk9_wan-mz.122-18.SXF4 (76,220,452)	
s72033-entservicesk9_wan-mz.122-18.SXF3 (76,190,756)	
s72033-entservicesk9_wan-mz.122-18.SXF2 (76,159,524)	
s72033-entservicesk9_wan-mz.122-18.SXF1 (75,852,836)	
s72033-entservicesk9_wan-mz.122-18.SXF (75,846,692)	
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 720 Advanced IP Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-advipervicesk9_wan-vz.122-18.SXF6 (88,394,384) s72033-advipervicesk9_wan-vz.122-18.SXF5 (88,334,480) s72033-advipervicesk9_wan-vz.122-18.SXF4 (78,958,736) <b>Note</b> This is a limited-access strong encryption image.	<b>IP SERVICES SSH (MODULAR)</b> CAT6000-SUP720/MSFC3: S733AIK9M-12218SXF
s72033-advipervicesk9_wan-mz.122-18.SXF6 (82,484,772) s72033-advipervicesk9_wan-mz.122-18.SXF5 (82,434,084) s72033-advipervicesk9_wan-mz.122-18.SXF4 (76,975,140) s72033-advipervicesk9_wan-mz.122-18.SXF3 (76,943,908) s72033-advipervicesk9_wan-mz.122-18.SXF2 (76,912,676) s72033-advipervicesk9_wan-mz.122-18.SXF1 (76,603,428) s72033-advipervicesk9_wan-mz.122-18.SXF (76,599,844) <b>Note</b> This is a limited-access strong encryption image.	<b>ADVANCED IP SERVICES SSH</b> CAT6000-SUP720/MSFC3: S733AIK9-12218SXF 7600-SUP720/MSFC3: S763AIK9-12218SXF

## Supervisor Engine 720 IP Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-ipervicesk9_wan-vz.122-18.SXF6 (88,393,360) s72033-ipervicesk9_wan-vz.122-18.SXF5 (88,326,800) s72033-ipervicesk9_wan-vz.122-18.SXF4 (78,955,664) <b>Note</b> This is a limited-access strong encryption image.	<b>IP SERVICES SSH (MODULAR)</b> CAT6000-SUP720/MSFC3: S733ISK9M-12218SXF
s72033-ipervicesk9_wan-mz.122-18.SXF6 (81,728,516) s72033-ipervicesk9_wan-mz.122-18.SXF5 (81,681,412) s72033-ipervicesk9_wan-mz.122-18.SXF4 (76,219,396) s72033-ipervicesk9_wan-mz.122-18.SXF3 (76,192,772) s72033-ipervicesk9_wan-mz.122-18.SXF2 (76,158,468) s72033-ipervicesk9_wan-mz.122-18.SXF1 (75,851,780) s72033-ipervicesk9_wan-mz.122-18.SXF (75,847,684) <b>Note</b> This is a limited-access strong encryption image.	<b>IP SERVICES SSH</b> CAT6000-SUP720/MSFC3: S733ISK9-12218SXF 7600-SUP720/MSFC3: S763ISK9-12218SXF
s72033-ipervicesk9-vz.122-18.SXF6 (78,260,368) s72033-ipervicesk9-vz.122-18.SXF5 (78,206,096) s72033-ipervicesk9-vz.122-18.SXF4 (69,208,720) <b>Note</b> This is a limited-access strong encryption image.	<b>IP SERVICES SSH LAN ONLY (MODULAR)</b> CAT6000-SUP720/MSFC3: S733ISK9N-12218SXF
s72033-ipervicesk9-mz.122-18.SXF6 (41,887,236) s72033-ipervicesk9-mz.122-18.SXF5 (41,860,100) s72033-ipervicesk9-mz.122-18.SXF4 (40,674,820) s72033-ipervicesk9-mz.122-18.SXF3 (40,649,220) s72033-ipervicesk9-mz.122-18.SXF2 (40,620,548) s72033-ipervicesk9-mz.122-18.SXF1 (40,436,740) s72033-ipervicesk9-mz.122-18.SXF (40,432,132) <b>Note</b> This is a limited-access strong encryption image.	<b>IP SERVICES SSH LAN ONLY</b> CAT6000-SUP720/MSFC3: S733ISK9L-12218SXF

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-ip-services_wan-vz.122-18.SXF6 (86,215,312)	<a href="#">IP SERVICES (MODULAR)</a> CAT6000-SUP720/MSFC3: S733ISM-12218SXF
s72033-ip-services_wan-vz.122-18.SXF5 (86,173,840)	
s72033-ip-services_wan-vz.122-18.SXF4 (76,898,448)	
s72033-ip-services_wan-mz.122-18.SXF6 (80,394,756)	<a href="#">IP SERVICES</a> CAT6000-SUP720/MSFC3: S733IS-12218SXF 7600-SUP720/MSFC3: S763IS-12218SXF
s72033-ip-services_wan-mz.122-18.SXF5 (80,350,724)	
s72033-ip-services_wan-mz.122-18.SXF4 (74,889,732)	
s72033-ip-services_wan-mz.122-18.SXF3 (74,859,524)	
s72033-ip-services_wan-mz.122-18.SXF2 (74,826,244)	
s72033-ip-services_wan-mz.122-18.SXF1 (74,525,188)	
s72033-ip-services_wan-mz.122-18.SXF (74,519,556)	

## Supervisor Engine 32 Images in Release 12.2(18)SXF and Rebuilds

These sections describe the Supervisor Engine 32 images:

- [Supervisor Engine 32 Advanced Enterprise Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 112](#)
- [Supervisor Engine 32 Enterprise Services for Release 12.2\(18\)SXF and Rebuilds, page 113](#)
- [Supervisor Engine 32 Advanced IP Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 113](#)
- [Supervisor Engine 32 IP Services Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 113](#)
- [Supervisor Engine 32 IP Base Feature Set for Release 12.2\(18\)SXF and Rebuilds, page 114](#)

### Supervisor Engine 32 Advanced Enterprise Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-adventerprisek9_wan-vz.122-18.SXF6 (54,961,808)	<a href="#">ADVANCED ENTERPRISE SERVICES SSH (MODULAR)</a> CAT6000-SUP32/MSFC2A: S323AEK9M-12218SXF
s3223-adventerprisek9_wan-vz.122-18.SXF5 (54,924,944)	
<b>Note</b> This is a limited-access strong encryption image.	
s3223-adventerprisek9_wan-mz.122-18.SXF6 (50,575,940)	<a href="#">ADVANCED ENTERPRISE SERVICES SSH</a> CAT6000-SUP32/MSFC2A: S323AEK9-12218SXF 7600-SUP32/MSFC2A: S7632AEK9-12218SXF
s3223-adventerprisek9_wan-mz.122-18.SXF5 (50,550,852)	
s3223-adventerprisek9_wan-mz.122-18.SXF4 (47,386,180)	
s3223-adventerprisek9_wan-mz.122-18.SXF3 (47,369,284)	
s3223-adventerprisek9_wan-mz.122-18.SXF2 (47,351,876)	
s3223-adventerprisek9_wan-mz.122-18.SXF (47,114,308)	
<b>Note</b> This is a limited-access strong encryption image.	



## Supervisor Engine 32 Enterprise Services for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-entservicesk9_wan-vz.122-18.SXF6 (54,963,344) s3223-entservicesk9_wan-vz.122-18.SXF5 (54,924,432) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">ENTERPRISE SERVICES SSH (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323ESK9M-12218SXF
s3223-entservicesk9_wan-mz.122-18.SXF6 (49,818,148) s3223-entservicesk9_wan-mz.122-18.SXF5 (49,797,156) s3223-entservicesk9_wan-mz.122-18.SXF4 (46,632,996) s3223-entservicesk9_wan-mz.122-18.SXF3 (46,615,076) s3223-entservicesk9_wan-mz.122-18.SXF2 (46,597,156) s3223-entservicesk9_wan-mz.122-18.SXF (46,363,172) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">ENTERPRISE SERVICES SSH</a> CAT6000-SUP32/MSFC2A:S323ESK9-12218SXF

## Supervisor Engine 32 Advanced IP Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-advipservicesk9_wan-vz.122-18.SXF6 (54,966,416) s3223-advipservicesk9_wan-vz.122-18.SXF5 (54,924,432) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP SERVICES SSH (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323AIK9M-12218SXF
s3223-advipservicesk9_wan-mz.122-18.SXF6 (50,575,396) s3223-advipservicesk9_wan-mz.122-18.SXF5 (50,549,284) s3223-advipservicesk9_wan-mz.122-18.SXF4 (47,386,148) s3223-advipservicesk9_wan-mz.122-18.SXF3 (47,367,716) s3223-advipservicesk9_wan-mz.122-18.SXF2 (47,351,844) s3223-advipservicesk9_wan-mz.122-18.SXF (47,115,812) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">ADVANCED IP SERVICES SSH</a> CAT6000-SUP32/MSFC2A:S323AIK9-12218SXF 7600-SUP32/MSFC2A:S7632AIK9-12218SXF

## Supervisor Engine 32 IP Services Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-ip-servicesk9_wan-vz.122-18.SXF6 (54,962,832) s3223-ip-servicesk9_wan-vz.122-18.SXF5 (54,925,968) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP SERVICES SSH (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323ISK9M-12218SXF
s3223-ip-servicesk9_wan-mz.122-18.SXF6 (49,819,140) s3223-ip-servicesk9_wan-mz.122-18.SXF5 (49,796,612) s3223-ip-servicesk9_wan-mz.122-18.SXF4 (46,631,940) s3223-ip-servicesk9_wan-mz.122-18.SXF3 (46,615,556) s3223-ip-servicesk9_wan-mz.122-18.SXF2 (46,596,100) s3223-ip-servicesk9_wan-mz.122-18.SXF (46,363,140) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP SERVICES SSH</a> CAT6000-SUP32/MSFC2A:S323ISK9-12218SXF 7600-SUP32/MSFC2A:S7632ISK9-12218SXF

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-ipservices_wan-vz.122-18.SXF6 (52,808,336) s3223-ipservices_wan-vz.122-18.SXF5 (52,780,176)	<a href="#">IP SERVICES (MODULAR)</a> 7600-SUP32/MSFC2A:S323ISM-12218SXF
s3223-ipservices_wan-mz.122-18.SXF6 (48,487,940) s3223-ipservices_wan-mz.122-18.SXF5 (48,463,876) s3223-ipservices_wan-mz.122-18.SXF4 (45,302,276) s3223-ipservices_wan-mz.122-18.SXF3 (45,279,236) s3223-ipservices_wan-mz.122-18.SXF2 (45,266,436) s3223-ipservices_wan-mz.122-18.SXF (45,033,476)	<a href="#">IP SERVICES</a> 7600-SUP32/MSFC2A:S7632IS-12218SXF

### Supervisor Engine 32 IP Base Feature Set for Release 12.2(18)SXF and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s3223-ipbasek9_wan-vz.122-18.SXF6 (54,962,832) s3223-ipbasek9_wan-vz.122-18.SXF5 (54,920,848) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP BASE SSH (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323IBK9M-12218SXF
s3223-ipbasek9_wan-mz.122-18.SXF6 (49,819,588) s3223-ipbasek9_wan-mz.122-18.SXF5 (49,795,524) s3223-ipbasek9_wan-mz.122-18.SXF4 (46,632,388) s3223-ipbasek9_wan-mz.122-18.SXF3 (46,613,956) s3223-ipbasek9_wan-mz.122-18.SXF2 (46,599,620) s3223-ipbasek9_wan-mz.122-18.SXF (46,362,564) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP BASE SSH</a> CAT6000-SUP32/MSFC2A:S323IBK9-12218SXF
s3223-ipbasek9-vz.122-18.SXF6 (49,030,800) s3223-ipbasek9-vz.122-18.SXF5 (48,991,888) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP BASE SSH LAN ONLY (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323IBK9LM-12218SXF
s3223-ipbasek9-mz.122-18.SXF6 (27,966,916) s3223-ipbasek9-mz.122-18.SXF5 (27,957,700) s3223-ipbasek9-mz.122-18.SXF4 (27,463,108) s3223-ipbasek9-mz.122-18.SXF3 (27,448,260) s3223-ipbasek9-mz.122-18.SXF2 (27,433,412) s3223-ipbasek9-mz.122-18.SXF (27,267,012) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP BASE SSH LAN ONLY</a> CAT6000-SUP32/MSFC2A:S323IBK9L-12218SXF
s3223-ipbase_wan-vz.122-18.SXF6 (52,809,360) s3223-ipbase_wan-vz.122-18.SXF5 (52,788,880)	<a href="#">IP BASE (MODULAR)</a> CAT6000-SUP32/MSFC2A:S323IBM-12218SXF
s3223-ipbase_wan-mz.122-18.SXF6 (48,487,364) s3223-ipbase_wan-mz.122-18.SXF5 (48,461,764) s3223-ipbase_wan-mz.122-18.SXF4 (45,302,724) s3223-ipbase_wan-mz.122-18.SXF3 (45,278,660) s3223-ipbase_wan-mz.122-18.SXF2 (45,266,372) s3223-ipbase_wan-mz.122-18.SXF (45,032,388)	<a href="#">IP BASE</a> CAT6000-SUP32/MSFC2A:S323IB-12218SXF

## Supervisor Engine 2 Images in Release 12.2(18)SXF Rebuilds

These sections describe the Supervisor Engine 2 images:

- [Supervisor Engine 2 Advanced Enterprise Services Feature Set for Release 12.2\(18\)SXF Rebuilds, page 115](#)
- [Supervisor Engine 2 Enterprise Services for Release 12.2\(18\)SXF Rebuilds, page 115](#)
- [Supervisor Engine 2 Advanced IP Services Feature Set for Release 12.2\(18\)SXF Rebuilds, page 115](#)
- [Supervisor Engine 2 IP Services Feature Set for Release 12.2\(18\)SXF Rebuilds, page 116](#)

### Supervisor Engine 2 Advanced Enterprise Services Feature Set for Release 12.2(18)SXF Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s222-adventerprisek9_wan-mz.122-18.SXF6 (52,478,532)	<a href="#">ADVANCED ENTERPRISE SERVICES</a> SSH CAT6000-SUP2/MSFC2:S222AEK9-12218SXF 7600-SUP2/MSFC2S76AEK9-12218SXF
s222-adventerprisek9_wan-mz.122-18.SXF5 (52,448,836)	
s222-adventerprisek9_wan-mz.122-18.SXF4 (49,592,900)	
s222-adventerprisek9_wan-mz.122-18.SXF3 (49,581,124)	
s222-adventerprisek9_wan-mz.122-18.SXF2 (49,567,300)	
<b>Note</b> This is a limited-access strong encryption image.	

### Supervisor Engine 2 Enterprise Services for Release 12.2(18)SXF Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s222-entservicesk9_wan-mz.122-18.SXF6 (51,720,740)	<a href="#">ENTERPRISE SERVICES</a> SSH CAT6000-SUP2/MSFC2:S222ESK9-12218SXF
s222-entservicesk9_wan-mz.122-18.SXF5 (51,696,164)	
s222-entservicesk9_wan-mz.122-18.SXF4 (48,838,692)	
s222-entservicesk9_wan-mz.122-18.SXF3 (48,828,452)	
s222-entservicesk9_wan-mz.122-18.SXF2 (48,813,604)	
<b>Note</b> This is a limited-access strong encryption image.	

### Supervisor Engine 2 Advanced IP Services Feature Set for Release 12.2(18)SXF Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s222-advipservicesk9_wan-mz.122-18.SXF6 (52,478,500)	<a href="#">ADVANCED IP SERVICES</a> SSH CAT6000-SUP2/MSFC2:S222AIK9-12218SXF 7600-SUP2/MSFC2S76AIK9-12218SXF
s222-advipservicesk9_wan-mz.122-18.SXF5 (52,448,804)	
s222-advipservicesk9_wan-mz.122-18.SXF4 (49,592,356)	
s222-advipservicesk9_wan-mz.122-18.SXF3 (49,581,604)	
s222-advipservicesk9_wan-mz.122-18.SXF2 (49,566,756)	
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 2 IP Services Feature Set for Release 12.2(18)SXF Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s222-ip-servicesk9-mz.122-18.SXF6 (32,651,748) s222-ip-servicesk9-mz.122-18.SXF5 (32,636,900) s222-ip-servicesk9-mz.122-18.SXF4 (31,973,348) s222-ip-servicesk9-mz.122-18.SXF3 (31,961,572) s222-ip-servicesk9-mz.122-18.SXF2 (31,949,284) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP SERVICES</a> SSH LAN ONLY CAT6000-SUP2/MSFC2:S222ISK9L-12218SXF
s222-ip-servicesk9_wan-mz.122-18.SXF6 (51,720,708) s222-ip-servicesk9_wan-mz.122-18.SXF5 (51,696,132) s222-ip-servicesk9_wan-mz.122-18.SXF4 (48,837,124) s222-ip-servicesk9_wan-mz.122-18.SXF3 (48,828,420) s222-ip-servicesk9_wan-mz.122-18.SXF2 (48,814,596) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">IP SERVICES</a> SSH CAT6000-SUP2/MSFC2:S222ISK9-12218SXF 7600-SUP2/MSFC2S76ISK9-12218SXF
s222-ip-services_wan-mz.122-18.SXF6 (50,411,524) s222-ip-services_wan-mz.122-18.SXF5 (50,390,020) s222-ip-services_wan-mz.122-18.SXF4 (47,528,452) s222-ip-services_wan-mz.122-18.SXF3 (47,516,676) s222-ip-services_wan-mz.122-18.SXF2 (47,498,244)	<a href="#">IP SERVICES</a> CAT6000-SUP2/MSFC2:S222IS-12218SXF 7600-SUP2/MSFC2S76IS-12218SXF

## Feature Sets in Release 12.2(18)SXE and Rebuilds

These sections describe the feature sets in Release 12.2(18)SXE and rebuilds:

- [Advanced Enterprise Services SSH Feature Set for Release 12.2\(18\)SXE and Rebuilds, page 116](#)
- [Enterprise Services SSH for Release 12.2\(18\)SXE and Rebuilds, page 117](#)
- [Advanced IP Services SSH Feature Set for Release 12.2\(18\)SXE and Rebuilds, page 117](#)
- [IP Services SSH Feature Set for Release 12.2\(18\)SXE and Rebuilds, page 117](#)
- [FPD Image Packages, page 80](#)

## Advanced Enterprise Services SSH Feature Set for Release 12.2(18)SXE and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-adventerprisek9_wan-mz.122-18.SXE6a (75,344,356) s72033-adventerprisek9_wan-mz.122-18.SXE6 (75,339,748) s72033-adventerprisek9_wan-mz.122-18.SXE5 (75,309,540) s72033-adventerprisek9_wan-mz.122-18.SXE4 (74,349,540) s72033-adventerprisek9_wan-mz.122-18.SXE3 (74,272,228) s72033-adventerprisek9_wan-mz.122-18.SXE2 (74,259,428) s72033-adventerprisek9_wan-mz.122-18.SXE1 (73,019,364) s72033-adventerprisek9_wan-mz.122-18.SXE (deferred) <b>Note</b> This is a limited-access strong encryption image.	<a href="#">ADVANCED ENTERPRISE SERVICES</a> SSH CAT6000-SUP720/MSFC3: S733AESK9-12218SXE 7600-SUP720/MSFC3: S763AESK9-12218SXE

## Enterprise Services SSH for Release 12.2(18)SXE and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-entservicesk9_wan-mz.122-18.SXE6a (75,344,868) s72033-entservicesk9_wan-mz.122-18.SXE6 (75,339,236) s72033-entservicesk9_wan-mz.122-18.SXE5 (75,309,028) s72033-entservicesk9_wan-mz.122-18.SXE4 (74,351,076) s72033-entservicesk9_wan-mz.122-18.SXE3 (74,273,252) s72033-entservicesk9_wan-mz.122-18.SXE2 (74,259,428) s72033-entservicesk9_wan-mz.122-18.SXE1 (73,019,364)	<a href="#">ENTERPRISE SERVICES SSH</a> CAT6000-SUP720/MSFC3: S733ESK9-12218SXE
<b>Note</b> This is a limited-access strong encryption image.	

## Advanced IP Services SSH Feature Set for Release 12.2(18)SXE and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-advipservicesk9_wan-mz.122-18.SXE6a (75,344,356) s72033-advipservicesk9_wan-mz.122-18.SXE6 (75,339,748) s72033-advipservicesk9_wan-mz.122-18.SXE5 (75,309,540) s72033-advipservicesk9_wan-mz.122-18.SXE4 (74,349,028) s72033-advipservicesk9_wan-mz.122-18.SXE3 (74,272,228) s72033-advipservicesk9_wan-mz.122-18.SXE2 (74,259,428) s72033-advipservicesk9_wan-mz.122-18.SXE1 (73,019,364) s72033-advipservicesk9_wan-mz.122-18.SXE (deferred)	<a href="#">ADVANCED IP SERVICES SSH</a> CAT6000-SUP720/MSFC3:S733AISK9-12218SXE 7600-SUP720/MSFC3:S763AISK9-12218SXE
<b>Note</b> This is a limited-access strong encryption image.	

## IP Services SSH Feature Set for Release 12.2(18)SXE and Rebuilds

Image Filename and Size in Bytes	Description, Platform, and Product ID
s72033-ipservicesk9_wan-mz.122-18.SXE6a (75,344,868) s72033-ipservicesk9_wan-mz.122-18.SXE6 (75,339,236) s72033-ipservicesk9_wan-mz.122-18.SXE5 (75,309,028) s72033-ipservicesk9_wan-mz.122-18.SXE4 (74,350,564) s72033-ipservicesk9_wan-mz.122-18.SXE3 (74,273,252) s72033-ipservicesk9_wan-mz.122-18.SXE2 (74,259,428) s72033-ipservicesk9_wan-mz.122-18.SXE1 (73,019,364)	<a href="#">IP SERVICES SSH</a> CAT6000-SUP720/MSFC3:S733IPSK9-12218SXE 7600-SUP720/MSFC3:S763IPSK9-12218SXE
<b>Note</b> This is a limited-access strong encryption image.	
s72033-ipservicesk9-mz.122-18.SXE6a (40,611,812) s72033-ipservicesk9-mz.122-18.SXE6 (40,607,204) s72033-ipservicesk9-mz.122-18.SXE5 (40,583,140) s72033-ipservicesk9-mz.122-18.SXE4 (40,456,676) s72033-ipservicesk9-mz.122-18.SXE3 (40,399,844) s72033-ipservicesk9-mz.122-18.SXE2 (40,394,212) s72033-ipservicesk9-mz.122-18.SXE1 (40,379,844)	<a href="#">IP SERVICES SSH LAN ONLY</a> CAT6000-SUP720/MSFC3:S733IPLK9-12218SXE
<b>Note</b> This is a limited-access strong encryption image.	

## Feature Sets in Release 12.2(18)SXD and Rebuilds

These sections describe the feature sets in Release 12.2(18)SXD and rebuilds:

- [Enterprise Firewall MPLS and IPv6 Feature Set for Release 12.2\(18\)SXD and Rebuilds, page 118](#)
- [Enterprise IPv6 Feature Set for Release 12.2\(18\)SXD and Rebuilds, page 119](#)
- [IP MPLS, IPv6, and BGP Feature Set for Release 12.2\(18\)SXD and Rebuilds, page 121](#)
- [IP Feature Set for Release 12.2\(18\)SXD and Rebuilds, page 122](#)

## Enterprise Firewall MPLS and IPv6 Feature Set for Release 12.2(18)SXD and Rebuilds

- [Features, page 118](#)
- [Supervisor Engine 720 Images, page 118](#)
- [Supervisor Engine 2 Images, page 119](#)

### Features

- MPLS
- IPv6
- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)
- IPX routing in software on the MSFC
- AppleTalk Phase 1 and 2, and DECnet Phase IV routing in software on the MSFC
- DECnet Phase V and CLNS/OSI routing in software on the MSFC

### Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, firewall, SSHv2, and 3DES: s72033-jk9o3sv-mz.122-18.SXD7a (48,419,116) s72033-jk9o3sv-mz.122-18.SXD7 (48,411,760) s72033-jk9o3sv-mz.122-18.SXD6 (48,415,152) s72033-jk9o3sv-mz.122-18.SXD5 (48,414,964) s72033-jk9o3sv-mz.122-18.SXD4 (48,382,272) s72033-jk9o3sv-mz.122-18.SXD3 (deferred) s72033-jk9o3sv-mz.122-18.SXD2 (deferred) s72033-jk9o3sv-mz.122-18.SXD1 (deferred) s72033-jk9o3sv-mz.122-18.SXD (deferred)	ENT FW W/MPLS/IPV6/SSH/3DES: S733AK9H-12218SXD (Catalyst 6500 series) S763AK9H-12218SXD (Cisco 7600 series)
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, firewall, SSHv2, and 3DES: c6k222-jk9o3sv-mz.122-18.SXD7a (40,939,416) c6k222-jk9o3sv-mz.122-18.SXD7 (40,937,356) c6k222-jk9o3sv-mz.122-18.SXD6 (40,939,140) c6k222-jk9o3sv-mz.122-18.SXD5 (40,939,152) c6k222-jk9o3sv-mz.122-18.SXD4 (40,913,596) c6k222-jk9o3sv-mz.122-18.SXD3 (deferred) c6k222-jk9o3sv-mz.122-18.SXD2 (deferred) c6k222-jk9o3sv-mz.122-18.SXD1 (deferred) c6k222-jk9o3sv-mz.122-18.SXD (deferred) <b>Note</b> This is a limited-access strong encryption image.	ENT FW W/MPLS/IPV6/SSH/3DES: S222AK9H-12218SXD (Catalyst 6500 series) S762AK9H-12218SXD (Cisco 7600 series)
Supports SSHv2 and 3DES: c6k222-jk9s-mz.122-18.SXD7a (28,963,704) c6k222-jk9s-mz.122-18.SXD7 (28,967,260) c6k222-jk9s-mz.122-18.SXD6 (28,965,304) c6k222-jk9s-mz.122-18.SXD5 (28,964,572) c6k222-jk9s-mz.122-18.SXD4 (28,937,964) c6k222-jk9s-mz.122-18.SXD3 (deferred) c6k222-jk9s-mz.122-18.SXD2 (deferred) c6k222-jk9s-mz.122-18.SXD1 (deferred) c6k222-jk9s-mz.122-18.SXD (deferred) <b>Note</b> This is a limited-access strong encryption image.	ENT W/IPV6/SSH/3DES LAN ONLY: S222ALK9-12218SXD (Catalyst 6500 series)
Supports OSM, FlexWAN, and firewall: c6k222-jo3sv-mz.122-18.SXD7a (39,757,056) c6k222-jo3sv-mz.122-18.SXD7 (39,756,956) c6k222-jo3sv-mz.122-18.SXD6 (39,756,624) c6k222-jo3sv-mz.122-18.SXD5 (39,756,980) c6k222-jo3sv-mz.122-18.SXD4 (39,731,780) c6k222-jo3sv-mz.122-18.SXD3 (deferred) c6k222-jo3sv-mz.122-18.SXD2 (deferred) c6k222-jo3sv-mz.122-18.SXD1 (deferred) c6k222-jo3sv-mz.122-18.SXD (deferred) <b>Note</b> This is a limited-access strong encryption image.	ENT FW W/MPLS/IPV6: S222AH-12218SXD (Catalyst 6500 series)

## Enterprise IPv6 Feature Set for Release 12.2(18)SXD and Rebuilds

- [Features, page 119](#)
- [Supervisor Engine 720 Images, page 120](#)
- [Supervisor Engine 2 Images, page 121](#)

### Features

- IPv6
- Wire speed Layer 2 switching (bridging)

- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)
- IPX routing in software on the MSFC
- AppleTalk Phase 1 and 2, and DECnet Phase IV routing in software on the MSFC
- DECnet Phase V and CLNS/OSI routing in software on the MSFC

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: s72033-jk9sv-mz.122-18.SXD7a (48,224,032) s72033-jk9sv-mz.122-18.SXD7 (48,213,556) s72033-jk9sv-mz.122-18.SXD6 (48,215,464) s72033-jk9sv-mz.122-18.SXD5 (48,215,488) s72033-jk9sv-mz.122-18.SXD4 (48,191,764) s72033-jk9sv-mz.122-18.SXD3 (deferred) s72033-jk9sv-mz.122-18.SXD2 (deferred) s72033-jk9sv-mz.122-18.SXD1 (deferred) s72033-jk9sv-mz.122-18.SXD (deferred)	ENTERPRISE W/IPV6 W/SSH: S733AK9-12218SXD (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	
Supports SSHv2 and 3DES: s72033-jk9s-mz.122-18.SXD7a (36,442,456) s72033-jk9s-mz.122-18.SXD7 (36,437,352) s72033-jk9s-mz.122-18.SXD6 (36,434,492) s72033-jk9s-mz.122-18.SXD5 (36,433,680) s72033-jk9s-mz.122-18.SXD4 (36,408,484) s72033-jk9s-mz.122-18.SXD3 (deferred) s72033-jk9s-mz.122-18.SXD2 (deferred) s72033-jk9s-mz.122-18.SXD1 (deferred) s72033-jk9s-mz.122-18.SXD (deferred)	ENT. W/IPV6 W/SSH LAN ONLY: S733ALK9-12218SXD (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	



## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: c6k222-jk9sv-mz.122-18.SXD7a (40,744,288) c6k222-jk9sv-mz.122-18.SXD7 (40,744,876) c6k222-jk9sv-mz.122-18.SXD6 (40,746,196) c6k222-jk9sv-mz.122-18.SXD5 (40,744,076) c6k222-jk9sv-mz.122-18.SXD4 (40,718,164) c6k222-jk9sv-mz.122-18.SXD3 (deferred) c6k222-jk9sv-mz.122-18.SXD2 (deferred) c6k222-jk9sv-mz.122-18.SXD1 (deferred) c6k222-jk9sv-mz.122-18.SXD (deferred)	ENT W/IPV6/SSH/3DES: S222AK9-12218SXD (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	
Supports OSM and FlexWAN: c6k222-jsv-mz.122-18.SXD7a (39,567,132) c6k222-jsv-mz.122-18.SXD7 (39,563,340) c6k222-jsv-mz.122-18.SXD6 (39,563,796) c6k222-jsv-mz.122-18.SXD5 (39,564,244) c6k222-jsv-mz.122-18.SXD4 (39,539,568) c6k222-jsv-mz.122-18.SXD3 (deferred) c6k222-jsv-mz.122-18.SXD2 (deferred) c6k222-jsv-mz.122-18.SXD1 (deferred) c6k222-jsv-mz.122-18.SXD (deferred)	ENT W/IPV6: S222A-12218SXD (Catalyst 6500 series)

## IP MPLS, IPv6, and BGP Feature Set for Release 12.2(18)SXD and Rebuilds

- [Features, page 121](#)
- [Supervisor Engine 720 Images, page 122](#)
- [Supervisor Engine 2 Images, page 122](#)

### Features

- MPLS
- IPv6
- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: s72033-pk9sv-mz.122-18.SXD7a (46,665,796) s72033-pk9sv-mz.122-18.SXD7 (46,660,652) s72033-pk9sv-mz.122-18.SXD6 (46,658,960) s72033-pk9sv-mz.122-18.SXD5 (46,656,764) s72033-pk9sv-mz.122-18.SXD4 (46,633,792) s72033-pk9sv-mz.122-18.SXD3 (deferred) s72033-pk9sv-mz.122-18.SXD2 (deferred) s72033-pk9sv-mz.122-18.SXD1 (deferred) s72033-pk9sv-mz.122-18.SXD (deferred)	ADV IP W/MPLS/IPV6/SSH/3DES + BGP: S733ZK9M-12218SXD (Catalyst 6500 series) S763ZK9M-12218SXD (Cisco 7600 series)
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: c6k222-pk9sv-mz.122-18.SXD7a (39,458,172) c6k222-pk9sv-mz.122-18.SXD7 (39,455,296) c6k222-pk9sv-mz.122-18.SXD6 (39,457,416) c6k222-pk9sv-mz.122-18.SXD5 (39,457,356) c6k222-pk9sv-mz.122-18.SXD4 (39,433,116) c6k222-pk9sv-mz.122-18.SXD3 (deferred) c6k222-pk9sv-mz.122-18.SXD2 (deferred) c6k222-pk9sv-mz.122-18.SXD1 (deferred) c6k222-pk9sv-mz.122-18.SXD (deferred)	ADV IP W/MPLS/IPV6/SSH/3DES + BGP: S222ZK9M-12218SXD (Catalyst 6500 series) S762ZK9M-12218SXD (Cisco 7600 series)
<b>Note</b> This is a limited-access strong encryption image.	

## IP Feature Set for Release 12.2(18)SXD and Rebuilds

- [Features, page 122](#)
- [Supervisor Engine 720 Images, page 123](#)
- [Supervisor Engine 2 Images, page 124](#)

### Features

- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: s72033-pk9sv-mz.122-18.SXD7a (46,665,796) s72033-pk9sv-mz.122-18.SXD7 (46,660,652) s72033-pk9sv-mz.122-18.SXD6 (46,658,960) s72033-pk9sv-mz.122-18.SXD5 (46,656,764) s72033-pk9sv-mz.122-18.SXD4 (46,633,792) s72033-pk9sv-mz.122-18.SXD3 (deferred) s72033-pk9sv-mz.122-18.SXD2 (deferred) s72033-pk9sv-mz.122-18.SXD1 (deferred) s72033-pk9sv-mz.122-18.SXD (deferred)  <b>Note</b> This is a limited-access strong encryption image.	IP W/SSH/3DES: S733ZK9-12218SXD (Catalyst 6500 series) S763ZK9-12218SXD (Cisco 7600 series)
Supports SSHv2 and 3DES: s72033-pk9s-mz.122-18.SXD7a (34,884,504) s72033-pk9s-mz.122-18.SXD7 (34,883,700) s72033-pk9s-mz.122-18.SXD6 (34,878,116) s72033-pk9s-mz.122-18.SXD5 (34,876,048) s72033-pk9s-mz.122-18.SXD4 (34,853,900) s72033-pk9s-mz.122-18.SXD3 (deferred) s72033-pk9s-mz.122-18.SXD2 (deferred) s72033-pk9s-mz.122-18.SXD1 (deferred) s72033-pk9s-mz.122-18.SXD (deferred)  <b>Note</b> This is a limited-access strong encryption image.	IP W/SSH/3DES LAN ONLY: S733ZLK9-12218SXD (Catalyst 6500 series)
Supports OSM and FlexWAN: s72033-psv-mz.122-18.SXD7a (45,472,068) s72033-psv-mz.122-18.SXD7 (45,463,592) s72033-psv-mz.122-18.SXD6 (45,465,840) s72033-psv-mz.122-18.SXD5 (45,465,300) s72033-psv-mz.122-18.SXD4 (45,443,036) s72033-psv-mz.122-18.SXD3 (deferred) s72033-psv-mz.122-18.SXD2 (deferred) s72033-psv-mz.122-18.SXD1 (deferred) s72033-psv-mz.122-18.SXD (deferred)	IP: S733Z-12218SXD (Catalyst 6500 series) S763Z-12218SXD (Cisco 7600 series)
s72033-ps-mz.122-18.SXD7a (33,961,820) s72033-ps-mz.122-18.SXD7 (33,956,572) s72033-ps-mz.122-18.SXD6 (33,956,684) s72033-ps-mz.122-18.SXD5 (33,953,304) s72033-ps-mz.122-18.SXD4 (33,927,520) s72033-ps-mz.122-18.SXD3 (deferred) s72033-ps-mz.122-18.SXD2 (deferred) s72033-ps-mz.122-18.SXD1 (deferred) s72033-ps-mz.122-18.SXD (deferred)	IP LAN ONLY: S733ZL-12218SXD (Catalyst 6500 series)

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Platform, and Product ID (Installed; append “=” for spare on shippable media.)
Supports OSM, FlexWAN, SSHv2, and 3DES: c6k222-pk9sv-mz.122-18.SXD7a (39,458,172) c6k222-pk9sv-mz.122-18.SXD7 (39,455,296) c6k222-pk9sv-mz.122-18.SXD6 (39,457,416) c6k222-pk9sv-mz.122-18.SXD5 (39,457,356) c6k222-pk9sv-mz.122-18.SXD4 (39,433,116) c6k222-pk9sv-mz.122-18.SXD3 (deferred) c6k222-pk9sv-mz.122-18.SXD2 (deferred) c6k222-pk9sv-mz.122-18.SXD1 (deferred) c6k222-pk9sv-mz.122-18.SXD (deferred)  <b>Note</b> This is a limited-access strong encryption image.	IP W/SSH/3DES: S222ZK9-12218SXD (Catalyst 6500 series) S762ZK9-12218SXD (Cisco 7600 series)
Supports SSHv2 and 3DES: c6k222-pk9s-mz.122-18.SXD7a (27,674,212) c6k222-pk9s-mz.122-18.SXD7 (27,676,528) c6k222-pk9s-mz.122-18.SXD6 (27,674,272) c6k222-pk9s-mz.122-18.SXD5 (27,674,940) c6k222-pk9s-mz.122-18.SXD4 (27,650,864) c6k222-pk9s-mz.122-18.SXD3 (deferred) c6k222-pk9s-mz.122-18.SXD2 (deferred) c6k222-pk9s-mz.122-18.SXD1 (deferred) c6k222-pk9s-mz.122-18.SXD (deferred)  <b>Note</b> This is a limited-access strong encryption image.	IP W/SSH/3DES LAN ONLY: S222ZLK9-12218SXD (Catalyst 6500 series)
Supports OSM and FlexWAN: c6k222-psv-mz.122-18.SXD7a (38,281,420) c6k222-psv-mz.122-18.SXD7 (38,277,828) c6k222-psv-mz.122-18.SXD6 (38,278,260) c6k222-psv-mz.122-18.SXD5 (38,278,572) c6k222-psv-mz.122-18.SXD4 (38,254,300) c6k222-psv-mz.122-18.SXD3 (deferred) c6k222-psv-mz.122-18.SXD2 (deferred) c6k222-psv-mz.122-18.SXD1 (deferred) c6k222-psv-mz.122-18.SXD (deferred)	IP: S222Z-12218SXD (Catalyst 6500 series) S762Z-12218SXD (Cisco 7600 series)
c6k222-ps-mz.122-18.SXD7a (26,498,860) c6k222-ps-mz.122-18.SXD7 (26,498,168) c6k222-ps-mz.122-18.SXD6 (26,498,412) c6k222-ps-mz.122-18.SXD5 (26,496,384) c6k222-ps-mz.122-18.SXD4 (26,471,648) c6k222-ps-mz.122-18.SXD3 (deferred) c6k222-ps-mz.122-18.SXD2 (deferred) c6k222-ps-mz.122-18.SXD1 (deferred) c6k222-ps-mz.122-18.SXD (deferred)	IP LAN ONLY: S222ZL-12218SXD (Catalyst 6500 series)

## Feature Sets in Release 12.2(17d)SXB and Rebuilds

These sections describe the feature sets in Release 12.2(17d)SXB and rebuilds:

- [Enterprise Firewall MPLS and IPv6 Feature Set for Release 12.2\(17d\)SXB and Rebuilds, page 125](#)
- [Enterprise IPv6 Feature Set for Release 12.2\(17d\)SXB and Rebuilds, page 127](#)
- [IP MPLS, IPv6, and BGP Feature Set for Release 12.2\(17d\)SXB and Rebuilds, page 129](#)
- [IP Feature Set for Release 12.2\(17d\)SXB and Rebuilds, page 130](#)

## Enterprise Firewall MPLS and IPv6 Feature Set for Release 12.2(17d)SXB and Rebuilds

- [Features, page 125](#)
- [Supervisor Engine 720 Images, page 125](#)
- [Supervisor Engine 2 Images, page 126](#)

### Features

- MPLS
- IPv6
- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)
- IPX routing in software on the MSFC
- AppleTalk Phase 1 and 2, DECnet Phase IV, and VINES routing in software on the MSFC
- DECnet Phase V and CLNS/OSI routing in software on the MSFC

### Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
s72033-jk9o3sv-mz.122-17d.SXB11a (43,880,568)	ENT FW W/MPLS/IPV6/SSH/3DES: S733AK9H-12217SXB (Catalyst 6500 series) S763AK9H-12217SXB (Cisco 7600 series)
s72033-jk9o3sv-mz.122-17d.SXB11 (43,810,240)	
s72033-jk9o3sv-mz.122-17d.SXB10 (43,818,816)	
s72033-jk9o3sv-mz.122-17d.SXB9 (43,799,804)	
s72033-jk9o3sv-mz.122-17d.SXB8 (43,760,344)	
s72033-jk9o3sv-mz.122-17d.SXB7 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB6 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB5 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB4 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB3 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB2 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB1 (deferred)	
s72033-jk9o3sv-mz.122-17d.SXB (deferred)	
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
c6k222-jk9o3sv-mz.122-17d.SXB11a (37,685,844) c6k222-jk9o3sv-mz.122-17d.SXB11 (37,673,212) c6k222-jk9o3sv-mz.122-17d.SXB10 (37,681,184) c6k222-jk9o3sv-mz.122-17d.SXB9 (37,664,684) c6k222-jk9o3sv-mz.122-17d.SXB8 (37,640,496) c6k222-jk9o3sv-mz.122-17d.SXB7 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB6 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB5 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB4 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB3 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB2 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB1 (deferred) c6k222-jk9o3sv-mz.122-17d.SXB (deferred)	ENT FW W/MPLS/IPV6/SSH/3DES: S222AK9H-12217SXB (Catalyst 6500 series) S762AK9H-12217SXB (Cisco 7600 series)
<b>Note</b> This is a limited-access strong encryption image.	ENT W/IPV6/SSH/3DES LAN ONLY: S222ALK9-12217SXB (Catalyst 6500 series)
c6k222-jk9s-mz.122-17d.SXB11a (26,891,604) c6k222-jk9s-mz.122-17d.SXB11 (26,881,824) c6k222-jk9s-mz.122-17d.SXB10 (26,891,068) c6k222-jk9s-mz.122-17d.SXB9 (26,877,532) c6k222-jk9s-mz.122-17d.SXB8 (26,851,208) c6k222-jk9s-mz.122-17d.SXB7 (deferred) c6k222-jk9s-mz.122-17d.SXB6 (deferred) c6k222-jk9s-mz.122-17d.SXB5 (deferred) c6k222-jk9s-mz.122-17d.SXB4 (deferred) c6k222-jk9s-mz.122-17d.SXB3 (deferred) c6k222-jk9s-mz.122-17d.SXB2 (deferred) c6k222-jk9s-mz.122-17d.SXB1 (deferred) c6k222-jk9s-mz.122-17d.SXB (deferred)	ENT W/IPV6/SSH/3DES LAN ONLY: S222ALK9-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	ENT FW W/MPLS/IPV6: S222AH-12217SXB (Catalyst 6500 series)
c6k222-jo3sv-mz.122-17d.SXB11a (36,415,936) c6k222-jo3sv-mz.122-17d.SXB11 (36,403,784) c6k222-jo3sv-mz.122-17d.SXB10 (36,409,760) c6k222-jo3sv-mz.122-17d.SXB9 (36,395,956) c6k222-jo3sv-mz.122-17d.SXB8 (36,368,352) c6k222-jo3sv-mz.122-17d.SXB7 (deferred) c6k222-jo3sv-mz.122-17d.SXB6 (deferred) c6k222-jo3sv-mz.122-17d.SXB5 (deferred) c6k222-jo3sv-mz.122-17d.SXB4 (deferred) c6k222-jo3sv-mz.122-17d.SXB3 (deferred) c6k222-jo3sv-mz.122-17d.SXB2 (deferred) c6k222-jo3sv-mz.122-17d.SXB1 (deferred) c6k222-jo3sv-mz.122-17d.SXB (deferred)	ENT FW W/MPLS/IPV6: S222AH-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	

## Enterprise IPv6 Feature Set for Release 12.2(17d)SXB and Rebuilds

- [Features, page 127](#)
- [Supervisor Engine 720 Images, page 128](#)
- [Supervisor Engine 2 Images, page 129](#)

### Features

- IPv6
- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)
- IPX routing in software on the MSFC
- AppleTalk Phase 1 and 2, DECnet Phase IV, and VINES routing in software on the MSFC
- DECnet Phase V and CLNS/OSI routing in software on the MSFC

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
s72033-jk9sv-mz.122-17d.SXB11a (43,690,324) s72033-jk9sv-mz.122-17d.SXB11 (43,619,424) s72033-jk9sv-mz.122-17d.SXB10 (43,626,788) s72033-jk9sv-mz.122-17d.SXB9 (43,610,624) s72033-jk9sv-mz.122-17d.SXB8 (43,569,316) s72033-jk9sv-mz.122-17d.SXB7 (deferred) s72033-jk9sv-mz.122-17d.SXB6 (deferred) s72033-jk9sv-mz.122-17d.SXB5 (deferred) s72033-jk9sv-mz.122-17d.SXB4 (deferred) s72033-jk9sv-mz.122-17d.SXB3 (deferred) s72033-jk9sv-mz.122-17d.SXB2 (deferred) s72033-jk9sv-mz.122-17d.SXB1 (deferred) s72033-jk9sv-mz.122-17d.SXB (deferred)	ENTERPRISE W/IPV6 W/SSH: S733AK9-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	
s72033-jk9s-mz.122-17d.SXB11a (33,088,544) s72033-jk9s-mz.122-17d.SXB11 (33,016,328) s72033-jk9s-mz.122-17d.SXB10 (33,025,852) s72033-jk9s-mz.122-17d.SXB9 (33,011,016) s72033-jk9s-mz.122-17d.SXB8 (32,970,964) s72033-jk9s-mz.122-17d.SXB7 (deferred) s72033-jk9s-mz.122-17d.SXB6 (deferred) s72033-jk9s-mz.122-17d.SXB5 (deferred) s72033-jk9s-mz.122-17d.SXB4 (deferred) s72033-jk9s-mz.122-17d.SXB3 (deferred) s72033-jk9s-mz.122-17d.SXB2 (deferred) s72033-jk9s-mz.122-17d.SXB1 (deferred) s72033-jk9s-mz.122-17d.SXB (deferred)	ENT. W/IPV6 W/SSH LAN ONLY: S733ALK9-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	



## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
c6k222-jk9sv-mz.122-17d.SXB11a (37,493,056) c6k222-jk9sv-mz.122-17d.SXB11 (37,483,068) c6k222-jk9sv-mz.122-17d.SXB10 (37,489,204) c6k222-jk9sv-mz.122-17d.SXB9 (37,475,792) c6k222-jk9sv-mz.122-17d.SXB8 (37,447,880) c6k222-jk9sv-mz.122-17d.SXB7 (deferred) c6k222-jk9sv-mz.122-17d.SXB6 (deferred) c6k222-jk9sv-mz.122-17d.SXB5 (deferred) c6k222-jk9sv-mz.122-17d.SXB4 (deferred) c6k222-jk9sv-mz.122-17d.SXB3 (deferred) c6k222-jk9sv-mz.122-17d.SXB2 (deferred) c6k222-jk9sv-mz.122-17d.SXB1 (deferred) c6k222-jk9sv-mz.122-17d.SXB (deferred)	ENT W/IPV6/SSH/3DES: S222AK9-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.  c6k222-jsv-mz.122-17d.SXB11a (36,222,792) c6k222-jsv-mz.122-17d.SXB11 (36,211,152) c6k222-jsv-mz.122-17d.SXB10 (36,222,496) c6k222-jsv-mz.122-17d.SXB9 (36,204,308) c6k222-jsv-mz.122-17d.SXB8 (36,180,896) c6k222-jsv-mz.122-17d.SXB7 (deferred) c6k222-jsv-mz.122-17d.SXB6 (deferred) c6k222-jsv-mz.122-17d.SXB5 (deferred) c6k222-jsv-mz.122-17d.SXB4 (deferred) c6k222-jsv-mz.122-17d.SXB3 (deferred) c6k222-jsv-mz.122-17d.SXB2 (deferred) c6k222-jsv-mz.122-17d.SXB1 (deferred) c6k222-jsv-mz.122-17d.SXB (deferred)	ENT W/IPV6: S222A-12217SXB (Catalyst 6500 series)

## IP MPLS, IPv6, and BGP Feature Set for Release 12.2(17d)SXB and Rebuilds

- [Features, page 129](#)
- [Supervisor Engine 720 Images, page 130](#)
- [Supervisor Engine 2 Images, page 130](#)

### Features

- Includes FR-IRC6
- MPLS
- IPv6
- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
s72033-pk9sv-mz.122-17d.SXB11a (42,131,936)	ADV IP W/MPLS/IPV6/SSH/3DES + BGP: S733ZK9M-12217SXB (Catalyst 6500 series) S763ZK9M-12217SXB (Cisco 7600 series)
s72033-pk9sv-mz.122-17d.SXB11 (42,061,544)	
s72033-pk9sv-mz.122-17d.SXB10 (42,066,736)	
s72033-pk9sv-mz.122-17d.SXB9 (42,050,492)	
s72033-pk9sv-mz.122-17d.SXB8 (42,007,568)	
s72033-pk9sv-mz.122-17d.SXB7 (deferred)	
s72033-pk9sv-mz.122-17d.SXB6 (deferred)	
s72033-pk9sv-mz.122-17d.SXB5 (deferred)	
s72033-pk9sv-mz.122-17d.SXB4 (deferred)	
s72033-pk9sv-mz.122-17d.SXB3 (deferred)	
s72033-pk9sv-mz.122-17d.SXB2 (deferred)	
s72033-pk9sv-mz.122-17d.SXB1 (deferred)	
s72033-pk9sv-mz.122-17d.SXB (deferred)	
<b>Note</b> This is a limited-access strong encryption image.	

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
c6k222-pk9sv-mz.122-17d.SXB11a (36,201,004)	ADV IP W/MPLS/IPV6/SSH/3DES + BGP: S222ZK9M-12217SXB (Catalyst 6500 series) S762ZK9M-12217SXB (Cisco 7600 series)
c6k222-pk9sv-mz.122-17d.SXB11 (36,192,332)	
c6k222-pk9sv-mz.122-17d.SXB10 (36,199,852)	
c6k222-pk9sv-mz.122-17d.SXB9 (36,183,184)	
c6k222-pk9sv-mz.122-17d.SXB8 (36,158,288)	
c6k222-pk9sv-mz.122-17d.SXB7 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB6 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB5 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB4 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB3 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB2 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB1 (deferred)	
c6k222-pk9sv-mz.122-17d.SXB (deferred)	
<b>Note</b> This is a limited-access strong encryption image.	

## IP Feature Set for Release 12.2(17d)SXB and Rebuilds

- [Features, page 131](#)
- [Supervisor Engine 720 Images, page 131](#)
- [Supervisor Engine 2 Images, page 133](#)

## Features

- Wire speed Layer 2 switching (bridging)
- Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP and MSDP, IGMP, and RGMP)

## Supervisor Engine 720 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
s72033-pk9sv-mz.122-17d.SXB11a (42,131,936) s72033-pk9sv-mz.122-17d.SXB11 (42,061,544) s72033-pk9sv-mz.122-17d.SXB10 (42,066,736) s72033-pk9sv-mz.122-17d.SXB9 (42,050,492) s72033-pk9sv-mz.122-17d.SXB8 (42,007,568) s72033-pk9sv-mz.122-17d.SXB7 (deferred) s72033-pk9sv-mz.122-17d.SXB6 (deferred) s72033-pk9sv-mz.122-17d.SXB5 (deferred) s72033-pk9sv-mz.122-17d.SXB4 (deferred) s72033-pk9sv-mz.122-17d.SXB3 (deferred) s72033-pk9sv-mz.122-17d.SXB2 (deferred) s72033-pk9sv-mz.122-17d.SXB1 (deferred) s72033-pk9sv-mz.122-17d.SXB (deferred)	IP W/SSH/3DES: S733ZK9-12217SXB (Catalyst 6500 series) S763ZK9-12217SXB (Cisco 7600 series)
<b>Note</b> This is a limited-access strong encryption image.  s72033-pk9s-mz.122-17d.SXB11a (31,530,692) s72033-pk9s-mz.122-17d.SXB11 (31,460,688) s72033-pk9s-mz.122-17d.SXB10 (31,467,692) s72033-pk9s-mz.122-17d.SXB9 (31,451,440) s72033-pk9s-mz.122-17d.SXB8 (31,409,268) s72033-pk9s-mz.122-17d.SXB7 (deferred) s72033-pk9s-mz.122-17d.SXB6 (deferred) s72033-pk9s-mz.122-17d.SXB5 (deferred) s72033-pk9s-mz.122-17d.SXB4 (deferred) s72033-pk9s-mz.122-17d.SXB3 (deferred) s72033-pk9s-mz.122-17d.SXB2 (deferred) s72033-pk9s-mz.122-17d.SXB1 (deferred) s72033-pk9s-mz.122-17d.SXB (deferred)	IP W/SSH/3DES LAN ONLY: S733ZLK9-12217SXB (Catalyst 6500 series)
<b>Note</b> This is a limited-access strong encryption image.	

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
s72033-psv-mz.122-17d.SXB11a (41,123,924) s72033-psv-mz.122-17d.SXB11 (41,050,516) s72033-psv-mz.122-17d.SXB10 (41,056,568) s72033-psv-mz.122-17d.SXB9 (41,043,144) s72033-psv-mz.122-17d.SXB8 (41,002,792) s72033-psv-mz.122-17d.SXB7 (deferred) s72033-psv-mz.122-17d.SXB6 (deferred) s72033-psv-mz.122-17d.SXB5 (deferred) s72033-psv-mz.122-17d.SXB4 (deferred) s72033-psv-mz.122-17d.SXB3 (deferred) s72033-psv-mz.122-17d.SXB2 (deferred) s72033-psv-mz.122-17d.SXB1 (deferred) s72033-psv-mz.122-17d.SXB (deferred)	IP: S733Z-12217SXB (Catalyst 6500 series) S763Z-12217SXB (Cisco 7600 series)
s72033-ps-mz.122-17d.SXB11a (30,785,656) s72033-ps-mz.122-17d.SXB11 (30,713,804) s72033-ps-mz.122-17d.SXB10 (30,725,328) s72033-ps-mz.122-17d.SXB9 (30,709,512) s72033-ps-mz.122-17d.SXB8 (30,670,748) s72033-ps-mz.122-17d.SXB7 (deferred) s72033-ps-mz.122-17d.SXB6 (deferred) s72033-ps-mz.122-17d.SXB5 (deferred) s72033-ps-mz.122-17d.SXB4 (deferred) s72033-ps-mz.122-17d.SXB3 (deferred) s72033-ps-mz.122-17d.SXB2 (deferred) s72033-ps-mz.122-17d.SXB1 (deferred) s72033-ps-mz.122-17d.SXB (deferred)	IP LAN ONLY: S733ZL-12217SXB (Catalyst 6500 series)

## Supervisor Engine 2 Images

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
<p>Supports OSM, FlexWAN, SSHv2, and 3DES:</p> <p>c6k222-pk9sv-mz.122-17d.SXB11a (36,201,004)</p> <p>c6k222-pk9sv-mz.122-17d.SXB11 (36,192,332)</p> <p>c6k222-pk9sv-mz.122-17d.SXB10 (36,199,852)</p> <p>c6k222-pk9sv-mz.122-17d.SXB9 (36,183,184)</p> <p>c6k222-pk9sv-mz.122-17d.SXB8 (36,158,288)</p> <p>c6k222-pk9sv-mz.122-17d.SXB7 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB6 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB5 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB4 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB3 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB2 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB1 (deferred)</p> <p>c6k222-pk9sv-mz.122-17d.SXB (deferred)</p>	<p>IP W/SSH/3DES:</p> <p>S222ZK9-12217SXB (Catalyst 6500 series)</p> <p>S762ZK9-12217SXB (Cisco 7600 series)</p>
<p><b>Note</b> This is a limited-access strong encryption image.</p>	<p>IP W/SSH/3DES LAN ONLY:</p> <p>S222ZLK9-12217SXB (Catalyst 6500 series)</p>
<p>Supports SSHv2 and 3DES:</p> <p>c6k222-pk9s-mz.122-17d.SXB11a (25,603,104)</p> <p>c6k222-pk9s-mz.122-17d.SXB11 (25,593,288)</p> <p>c6k222-pk9s-mz.122-17d.SXB10 (25,599,148)</p> <p>c6k222-pk9s-mz.122-17d.SXB9 (25,584,404)</p> <p>c6k222-pk9s-mz.122-17d.SXB8 (25,562,768)</p> <p>c6k222-pk9s-mz.122-17d.SXB7 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB6 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB5 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB4 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB3 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB2 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB1 (deferred)</p> <p>c6k222-pk9s-mz.122-17d.SXB (deferred)</p>	<p><b>Note</b> This is a limited-access strong encryption image.</p>

Image Filename and Size in Bytes	Description, Product ID, and Platform (Installed; append “=” for spare on shippable media.)
Supports OSM and FlexWAN: c6k222-psv-mz.122-17d.SXB11a (34,935,488) c6k222-psv-mz.122-17d.SXB11 (34,924,732) c6k222-psv-mz.122-17d.SXB10 (34,933,412) c6k222-psv-mz.122-17d.SXB9 (34,914,412) c6k222-psv-mz.122-17d.SXB8 (34,890,524) c6k222-psv-mz.122-17d.SXB7 (deferred) c6k222-psv-mz.122-17d.SXB5 (deferred) c6k222-psv-mz.122-17d.SXB4 (deferred) c6k222-psv-mz.122-17d.SXB3 (deferred) c6k222-psv-mz.122-17d.SXB2 (deferred) c6k222-psv-mz.122-17d.SXB1 (deferred) c6k222-psv-mz.122-17d.SXB (deferred)	IP: S222Z-12217SXB (Catalyst 6500 series) S762Z-12217SXB (Cisco 7600 series)
c6k222-ps-mz.122-17d.SXB11a (24,333,568) c6k222-ps-mz.122-17d.SXB11 (24,322,684) c6k222-ps-mz.122-17d.SXB9 (24,317,120) c6k222-ps-mz.122-17d.SXB8 (24,292,916) c6k222-ps-mz.122-17d.SXB7 (deferred) c6k222-ps-mz.122-17d.SXB6 (deferred) c6k222-ps-mz.122-17d.SXB5 (deferred) c6k222-ps-mz.122-17d.SXB4 (deferred) c6k222-ps-mz.122-17d.SXB3 (deferred) c6k222-ps-mz.122-17d.SXB2 (deferred) c6k222-ps-mz.122-17d.SXB1 (deferred) c6k222-ps-mz.122-17d.SXB (deferred)	IP LAN ONLY: S222ZL-12217SXB (Catalyst 6500 series)

## Feature Sets in Release 12.2(17b)SXA and Rebuilds (Deferred)

Release 12.2(17b)SXA and rebuilds are deferred.

## Feature Sets in Release 12.2(17a)SX and Rebuilds (Deferred)

Release 12.2(17a)SX and rebuilds are deferred.

## Feature Sets in Release 12.2(14)SX and Rebuilds (Deferred)

Release 12.2(14)SX and rebuilds are deferred.

# New Features



## Note

See the “Feature Sets” section on page 106 for information about which releases are deferred.

- [New Features in Release 12.2\(18\)SXF6, page 136](#)
- [New Features in Release 12.2\(18\)SXF5, page 137](#)
- [New Features in Release 12.2\(18\)SXF4, page 138](#)
- [New Features in Release 12.2\(18\)SXF3, page 138](#)
- [New Features in Release 12.2\(18\)SXF2, page 139](#)
- [New Features in Release 12.2\(18\)SXF1, page 143](#)
- [New Features in Release 12.2\(18\)SXF, page 143](#)
- [New Features in Release 12.2\(18\)SXE6a, page 146](#)
- [New Features in Release 12.2\(18\)SXE6, page 147](#)
- [New Features in Release 12.2\(18\)SXE5, page 147](#)
- [New Features in Release 12.2\(18\)SXE4, page 148](#)
- [New Features in Release 12.2\(18\)SXE3, page 148](#)
- [New Features in Release 12.2\(18\)SXE2, page 148](#)
- [New Features in Release 12.2\(18\)SXE1, page 149](#)
- [New Features in Release 12.2\(18\)SXE, page 149](#)
- [New Features in Release 12.2\(18\)SXD7a, page 159](#)
- [New Features in Release 12.2\(18\)SXD7, page 159](#)
- [New Features in Release 12.2\(18\)SXD6, page 159](#)
- [New Features in Release 12.2\(18\)SXD5, page 160](#)
- [New Features in Release 12.2\(18\)SXD4, page 160](#)
- [New Features in Release 12.2\(18\)SXD3, page 160](#)
- [New Features in Release 12.2\(18\)SXD2, page 161](#)
- [New Features in Release 12.2\(18\)SXD1, page 161](#)
- [New Features in Release 12.2\(18\)SXD, page 163](#)
- [New Features in Release 12.2\(17d\)SXB11a, page 170](#)
- [New Features in Release 12.2\(17d\)SXB11, page 171](#)
- [New Features in Release 12.2\(17d\)SXB10, page 171](#)
- [New Features in Release 12.2\(17d\)SXB9, page 171](#)
- [New Features in Release 12.2\(17d\)SXB9, page 171](#)
- [New Features in Release 12.2\(17d\)SXB7, page 172](#)
- [New Features in Release 12.2\(17d\)SXB6, page 172](#)
- [New Features in Release 12.2\(17d\)SXB5, page 173](#)
- [New Features in Release 12.2\(17d\)SXB4, page 173](#)

- [New Features in Release 12.2\(17d\)SXB3, page 173](#)
- [New Features in Release 12.2\(17d\)SXB2, page 174](#)
- [New Features in Release 12.2\(17d\)SXB1, page 174](#)
- [New Features in Release 12.2\(17d\)SXB, page 175](#)
- [New Features in Release 12.2\(17b\)SXA2, page 179](#)
- [New Features in Release 12.2\(17b\)SXA, page 179](#)
- [New Features in Release 12.2\(17a\)SX4, page 184](#)
- [New Features in Release 12.2\(17a\)SX3, page 185](#)
- [New Features in Release 12.2\(17a\)SX2, page 185](#)
- [New Features in Release 12.2\(17a\)SX1, page 185](#)
- [New Features in Release 12.2\(17a\)SX, page 187](#)
- [New Features in Release 12.2\(14\)SX1, page 190](#)
- [New Features in Release 12.2\(14\)SX, page 192](#)
- [Software Features from Earlier Releases, page 196](#)

**Note**

- 
- See the following site for information about MIBs:  
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
  - Features in the Cisco IOS 12.2SX releases that are also supported in the Cisco IOS 12.2 mainline, 12.2T and 12.2S releases are documented in the publications for these releases. When applicable, this section refers to these publications for platform-independent features supported in the Cisco IOS 12.2SX releases.
- 

## New Features in Release 12.2(18)SXF6

These sections describe the new features in Release 12.2(18)SXF6, 22 Sep 2006:

- [New Hardware Features in Release 12.2\(18\)SXF6, page 136](#)
- [New Software Features in Release 12.2\(18\)SXF6, page 136](#)

### New Hardware Features in Release 12.2(18)SXF6

None.

### New Software Features in Release 12.2(18)SXF6

- IPSec Anti-Replay Window: Expanding and Disabling—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_14/gt\\_iarwe.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_iarwe.htm)



## New Features in Release 12.2(18)SXF5

These sections describe the new features in Release 12.2(18)SXF5, 10 Jul 2006:

- [New Hardware Features in Release 12.2\(18\)SXF5, page 137](#)
- [New Software Features in Release 12.2\(18\)SXF5, page 137](#)

### New Hardware Features in Release 12.2(18)SXF5

- 8-port 10-Gigabit Ethernet X2switching module ([WS-X6708-10GE](#))
- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 32:
  - [WS-SVC-MWAM-1](#)
  - [Also supported with Supervisor Engine 720](#)
  - [Also supported with Supervisor Engine 2](#)
  - See these publications for more information:
    - [http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/servmod/esa\\_mwam.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/servmod/esa_mwam.htm)
    - <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/mwam/index.htm>

### New Software Features in Release 12.2(18)SXF5

- Autostate - Firewall Capability for the Firewall service module—See this publication:
  - [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/fwsm/index.htm)
- With [Cisco IOS software modularity](#) images:
  - [Support for Supervisor Engine 32](#)
  - [Multi-VRF \(VRF Lite\)](#)
- With Cisco IOS software images, Embedded Event Manager (EEM) 2.1 (previously supported with Cisco IOS software modularity images)—See this publication:
  - [http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/evnt\\_mgr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/evnt_mgr/index.htm)
- DSCP-based Queue Mapping—See this publication:
  - <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- IGMP Static Group Range Support—See this publication:
  - <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/stgrpsxf.htm>
- QoS - Ignore Port Trust—See this publication:
  - <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- RSVP Interface-based Receiver Proxy—See this publication:
  - <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/rsvpprox.htm>
- RSVP Refresh Reduction and Reliable Messaging—See this publication:
  - <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsrelmsg.htm>

- RSVP Scalability Enhancements—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/rsvpscal.htm>
- SRR (Shaped Round Robin)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- WCCP L2 Return—With Supervisor Engine 2, you can configure WCCP to use the Layer 2 return WCCP feature.

## New Features in Release 12.2(18)SXF4

These sections describe the new features in Release 12.2(18)SXF4, 27 Mar 2006:

- [New Hardware Features in Release 12.2\(18\)SXF4, page 138](#)
- [New Software Features in Release 12.2\(18\)SXF4, page 138](#)

### New Hardware Features in Release 12.2(18)SXF4

- Application Control Engine (ACE) module ([ACE10-6500-K9](#))

### New Software Features in Release 12.2(18)SXF4

- IPS Inline VLAN Pairing for [WS-SVC-IDS-M2-K9](#)—See this publication for more information:  
<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids12/cliguide/index.htm>
- Cisco IOS Software Modularity support with Supervisor Engine 720—See these sections for information about Cisco IOS Software Modularity:
  - [Cisco IOS Software Modularity Images, page 105](#)
  - [Cisco IOS Software Modularity Documentation, page 105](#)
  - [Cisco IOS Software Modularity Unsupported Features, page 105](#)

## New Features in Release 12.2(18)SXF3

These sections describe the new features in Release 12.2(18)SXF3, 16 Feb 2006:

- [New Hardware Features in Release 12.2\(18\)SXF3, page 138](#)
- [New Software Features in Release 12.2\(18\)SXF3, page 139](#)

### New Hardware Features in Release 12.2(18)SXF3

- 96-port 10/100TX RJ-45 switching module ([WS-X6148X2-RJ-45](#), [WS-X6148X2-45AF](#))
- 96-port 10/100TX RJ-21 switching module ([WS-X6196-RJ-21](#), [WS-X6196-21AF](#))
- IEEE 802.3af PoE daughtercard for [WS-X6148X2-RJ-45](#) and [WS-X6196-RJ-21](#) ([WS-F6K-FE48X2-AF](#))

## New Software Features in Release 12.2(18)SXF3

None.

## New Features in Release 12.2(18)SXF2

These sections describe the new features in Release 12.2(18)SXF2, 20 Jan 2006:

- [New Hardware Features in Release 12.2\(18\)SXF2, page 139](#)
- [New Software Features in Release 12.2\(18\)SXF2, page 140](#)

## New Hardware Features in Release 12.2(18)SXF2

- Wireless Services Module (WiSM; [WS-SVC-WISM-1-K9](#))
- 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1 ([SPA-OC192POS-VSR](#)):
  - Supported only with [7600-SIP-600](#)
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 100BASE SFPs for use with [WS-X6148-FE-SFP](#):
  - 100BASE-BX10-U SFP ([GLC-FE-100BX-U](#))
  - 100BASE-BX10-D SFP ([GLC-FE-100BX-D](#))
- Support with Supervisor Engine 32 for these modules:
  - Services SPA Carrier (SSC; [7600-SSC-400](#))

---

**Note** 7600-SSC-400 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.

---

  - IPsec SPA ([SPA-IPSEC-2G](#))
  - [Also supported with Supervisor Engine 720](#)
  - SPA-IPSEC-2G supports the features that were previously supported with [WS-SVC-IPSEC-1](#).
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- Support with Supervisor Engine 2 for these modules:
  - 48-port 10/100TX RJ-45 switching module ([WS-X6148A-RJ-45](#), [WS-X6148A-45AF](#))
  - 48-port 10/100/1000 Mbps switching module ([WS-X6148A-GE-TX](#), [WS-X6148A-GE-45AF](#))

- 48-port 100BASE-FX switching module ([WS-X6148-FE-SFP](#)), with these SFPs:
  - 100BASE-BX10-U SFP ([GLC-FE-100BX-U](#))
  - 100BASE-BX10-D SFP ([GLC-FE-100BX-D](#))
  - 100BASEEX SFP ([GLC-FE-100EX](#))
  - 100BASEZX SFP ([GLC-FE-100ZX](#))
  - 100BASEFX SFP ([GLC-FE-100FX](#))
  - 100BASELX SFP ([GLC-FE-100LX](#))
- Fast Ethernet port adapters ([PA-2FE](#), [PA-1FE](#))—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- 1-port Packet over SONET OC3c/STM1 port adapter ([PA-POS-1OC3](#))—See this publication: [http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514\\_1oc/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514_1oc/index.htm)
- Receive-only coarse or dense Wavelength Division Multiplexing (WDM) GBIC ([WDM-GBIC-REC](#))

## New Software Features in Release 12.2(18)SXF2

- NAC - L2 IP; Network Admission Control (NAC) Layer 2 Layer 2 IP validation (not supported with Supervisor Engine 2)—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nac.htm>
- Encrypted Multicast over GRE (supported on [SPA-IPSEC-2G](#))—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- Control Plane DSCP Support for RSVP—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dscprsvp.htm>
- RSVP Scalability Enhancements—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/rsvpscal.htm>
- Dot1q Transparency for EoMPLS on WAN ports—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mpls.htm>
- RFC 1483 Spanning-Tree Interoperability Enhancements on WAN ports—See these publications: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/atm.htm> <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>
- Support with Supervisor Engine 32 for:
  - [NetFlow v9 Export Format](#), including [NetFlow Export of BGP Nexthop Information](#)
  - [NetFlow multicast support](#)
  - [PIM snooping DR flooding enhancement](#)
- Support with Supervisor Engine 2 for these features, which are already supported with other Supervisor Engines:
  - [Any transport over MPLS \(AToM\): HDLC over MPLS \(HDLCoMPLS\)](#)
  - [Any transport over MPLS \(AToM\): PPP over MPLS \(PPPoMPLS\)](#)
  - [ATM OAM ping](#)

- ATM VC access trunk emulation
- Bandwidth command for HQoS parent class support
- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN
- BGP support for TTL security check
- Bidirectional forwarding detection (BFD) standard implementation
- Bridge control protocol (BCP)
- Bridging using RFC1483 routed encapsulation (BRE)
- Clear hardware interface counters
- CNS interactive CLI
- Configurable per VLAN MAC learning (PVL)
- CSG: content services gateway release 6
- DE/CLP and EXP mapping on FR/ATMoMPLS VC
- Digital optical monitoring (DOM)
- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces
- Dynamic multipoint VPN (DMVPN) phase 2
- EIGRP MPLS VPN PE-CE Site of Origin (SoO)
- Embedded network management improvements
- EtherChannel enhancement - 128 EtherChannels support
- EtherChannel Min-Links
- Ethernet over MPLS (EoMPLS) per VLAN QoS
- Flex Links
- Frame Relay Virtual Circuit (VC) bundling
- Hardware capacity monitoring
- HQoS support for Ethernet over MPLS (EoMPLS) VC
- H-VPLS with MPLS edge
- IDSM-2 EtherChannel load balancing
- IEEE 802.1s - Multiple Spanning Tree (MST) standard compliance
- Integrated IS-IS global default metric
- Integrated IS-IS protocol shutdown support maintaining configuration parameters
- Integrated IS-IS support for BFD over IPv4
- Invalid Special Parameter Index (SPI) recovery
- IP routing of RFC1483 ATM Bridge Encapsulation (RBE)
- IP unnumbered for VLAN-SVI interfaces
- IS-IS caching of redistributed routes
- IS-IS support for priority-driven IP prefix RIB installation
- Key rollover for certificate renewal
- Layer 2 traceroute
- MPLS LDP - inbound label binding filtering

- MPLS LSP ping/traceroute and AToM VCCV
- MQC: distribution of remaining bandwidth
- Multicast-VPN: multicast support for MPLS VPN
- Multipoint Bridging (MPB)
- NetFlow - bridged flow statistics
- OSPF link state database overload protection
- OSPF Link-Local Signaling (LLS) per interface basis
- OSPF MIB support of RFC 1850 and latest extensions
- OSPF support for BFD over IPv4
- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels
- OSPF support for unlimited software VRFs per Provider Edge (PE) router
- Packet classification based on layer3 packet-length (supported on WAN ports)
- Per interface sticky ARP
- Per port MAC limiting
- Per VLAN load balancing for advanced QinQ service mapping
- PIM snooping DR flooding enhancement
- PKI AAA authorization using the entire subject name
- Port security on 802.1Q tunnel ports
- Port security on private VLAN ports
- Port security on trunk ports
- Port security with 4096 secure MAC addresses
- Port security with sticky MAC addresses
- Protected private key storage
- QoS: aggregated DSCP / precedence values for WRED
- QoS: ingress shaping on FlexWAN module interfaces
- QoS: match VLAN on OSMs
- QoS: percentage based policing on WAN ports
- Query mode definition per trustpoint
- Query multiple servers during certificate revocation check
- RADIUS Load Balancing (RLB) IMSI sticky
- Re-enroll using existing certificate
- RFC-1490 bridging on FlexWAN interfaces
- SafeNet IPsec VPN client support
- SCP health monitoring for enhanced-FlexWAN
- Show diagnostic sanity
- Show Top-N
- SLB: interface-aware
- SLB: stateful failover within single chassis

- SPAN destination port permit list
- Strict priority low latency queueing (LLQ)
- Sub interface features - phase 1
- Unicast flood blocking (UFB)
- Uni-Directional Link Routing (UDLR)
- **verify certificate chain** command
- VLANs over IP unnumbered sub-interfaces

## New Features in Release 12.2(18)SXF1

These sections describe the new features in Release 12.2(18)SXF1, 22 Dec 2005:

- [New Hardware Features in Release 12.2\(18\)SXF1, page 143](#)
- [New Software Features in Release 12.2\(18\)SXF1, page 143](#)

## New Hardware Features in Release 12.2(18)SXF1

None.

## New Software Features in Release 12.2(18)SXF1

- DHCP Option 82 on Untrusted Port—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snoodhcp.htm>

## New Features in Release 12.2(18)SXF

These sections describe the new features in Release 12.2(18)SXF, 12 Sep 2005:

- [New Hardware Features in Release 12.2\(18\)SXF, page 143](#)
- [New Software Features in Release 12.2\(18\)SXF, page 145](#)

## New Hardware Features in Release 12.2(18)SXF



Note

Initial support for these modules is now in Release 12.2(18)SXF3:

- 96-port 10/100TX RJ-45 switching module ([WS-X6148X2-RJ-45](#), [WS-X6148X2-45AF](#))
- 96-port 10/100TX RJ-21 switching module ([WS-X6196-RJ-21](#), [WS-X6196-21AF](#))
- IEEE 802.3af PoE daughtercard for [WS-X6148X2-RJ-45](#) and [WS-X6196-RJ-21](#) ([WS-F6K-FE48X2-AF](#))

(CSCsd16853)

- Compact Flash Adapter in Bootflash Slot (WS-CF-UPG=):
  - CompactFlash adapter with 512 MB CompactFlash card that replaces the bootflash device.
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_17277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_17277.htm)
- Supervisor Engine 32 (WS-SUP32-10GE-3B, WS-SUP32-GE-3B)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/supe\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/supe_gd/index.htm)




---

**Note** See the “Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)” section on page 15 for the list of features not supported with Supervisor Engine 32.

---

- 48-port 10/100/1000 Mbps switching module (WS-X6148A-GE-TX, WS-X6148A-GE-45AF)
- 48-port 100BASE-FX switching module (WS-X6148-FE-SFP), with these SFPs:
  - 100BASEFX SFP (GLC-FE-100FX)
  - 100BASELX SFP (GLC-FE-100LX)
- 48-port 10/100TX RJ-45 switching module (WS-X6148A-RJ-45, WS-X6148A-45AF)
- SPA Interface Processor-600 (7600-SIP-600)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics (SPA-1XTENGE-XFP), with this XFP module: 10-Gigabit Ethernet LR (10 km; XFP-10GLR-OC192LR)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 10-port Gigabit Ethernet SPA, SFP Optics (SPA-10X1GE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 5-port Gigabit Ethernet SPA, SFP Optics (SPA-5X1GE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 2-port Gigabit Ethernet SPA, SFP Optics (SPA-2X1GE), with these SFPs:
  - Extended Temperature SX SFP (SFP-GE-S)
  - Extended Temperature LX/LH SFP (SFP-GE-L)
  - Extended Temperature ZX SFP (SFP-GE-Z)

See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>

- 1-port OC-192c/STM-64 POS/RPR SPA, SM-LR (SPA-OC192POS-LR)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- 1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics (SPA-OC192POS-XFP), with these XFP modules:
  - Single-Mode (SM) Short Reach (SR; XFP-10GLR-OC192SR)
  - Single-Mode (SM) Intermediate Reach (IR-2; XFP-10GER-OC192IR)

See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>



- 1 port OC-48c/STM-16 ATM SPA ([SPA-1XOC48-ATM](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm))—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- Firewall Services module support with Supervisor Engine 32:
  - [WS-SVC-FWM-1-K9](#)
  - Also supported with Supervisor Engine 720.
  - Also supported with Supervisor Engine 2.
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm)
- Network Analysis Module support with Supervisor Engine 32:
  - [WS-SVC-NAM-1](#) and [WS-SVC-NAM-2](#)
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/reInotes/78\\_15353.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/reInotes/78_15353.htm)
- Intrusion Detection System Module 2 support with Supervisor Engine 32:
  - [WS-SVC-IDSM2-K9](#)
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029\\_02.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029_02.htm)
- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 32:
  - [WS-SVC-SSL-1](#)
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/reInotes/ol\\_5277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/reInotes/ol_5277.htm)

## New Software Features in Release 12.2(18)SXF



### Note

See the “[Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A\)](#)” section on [page 15](#) for the list of features not supported with Supervisor Engine 32.

- H-VPLS with MPLS Edge—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mpls.htm>
- 'match cos' classification on 7600-SIP-400—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- EtherChannel Min-Links—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/channel.htm>

- Flex Links—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/flexlink.htm>
- Hardware Capacity Monitoring—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/pwr\\_envr.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/pwr_envr.htm)
- IEEE 802.1s - Multiple Spanning Tree (MST) Standard Compliance—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mst.htm>
- IP Unnumbered for VLAN-SVI interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/layer3.htm>
- L3 MPLS VPN over GRE (7600-SIP-400)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- Mapping a subinterface to an EoMPLS VC (7600-SIP-400)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>
- Multicast enhancement - egress replication performance improvement—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm>
- Multicast Enhancement - Replication Mode Detection—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm>
- NetFlow v9 Export Format, including NetFlow Export of BGP Nexthop Information—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123\\_1/nfv9expf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/nfv9expf.htm)
- NetFlow multicast support:
  - Supported only with NetFlow v9 export format.
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123\\_1/nfmultic.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/nfmultic.htm)
  - The NetFlow Multicast Support document contains a prerequisite that does not apply when configuring NetFlow multicast support with Release 12.2(18)SXF and later 12.2SX releases:  
You do not need to configure multicast fast switching or multicast distributed fast switching (MDFS); multicast CEF switching is supported with Release 12.2(18)SXF and later 12.2SX releases.
- Per Interface Sticky ARP—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dos.htm>
- PIM snooping DR flooding enhancement—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snooppim.htm>

## New Features in Release 12.2(18)SXE6a

These sections describe the new features in Release 12.2(18)SXE6a, 18 Sep 2006:

- [New Hardware Features in Release 12.2\(18\)SXE6a, page 147](#)
- [New Software Features in Release 12.2\(18\)SXE6a, page 147](#)

## New Hardware Features in Release 12.2(18)SXE6a

None.

## New Software Features in Release 12.2(18)SXE6a

None.

## New Features in Release 12.2(18)SXE6

These sections describe the new features in Release 12.2(18)SXE6, 08 Jun 2006:

- [New Hardware Features in Release 12.2\(18\)SXE6, page 147](#)
- [New Software Features in Release 12.2\(18\)SXE6, page 147](#)

## New Hardware Features in Release 12.2(18)SXE6

None.

## New Software Features in Release 12.2(18)SXE6

None.

## New Features in Release 12.2(18)SXE5

These sections describe the new features in Release 12.2(18)SXE5, 13 Feb 2006:

- [New Hardware Features in Release 12.2\(18\)SXE5, page 147](#)
- [New Software Features in Release 12.2\(18\)SXE5, page 147](#)

## New Hardware Features in Release 12.2(18)SXE5

- Compact Flash Adapter in Bootflash Slot (WS-CF-UPG=):
  - CompactFlash adapter with 512 MB CompactFlash card that replaces the bootflash device.
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_17277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_17277.htm)

## New Software Features in Release 12.2(18)SXE5

- UDI - Unique Device Identifier—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtpepudi.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpepudi.htm)

## New Features in Release 12.2(18)SXE4

These sections describe the new features in Release 12.2(18)SXE4, 10 Oct 2005:

- [New Hardware Features in Release 12.2\(18\)SXE4, page 148](#)
- [New Software Features in Release 12.2\(18\)SXE4, page 148](#)

### New Hardware Features in Release 12.2(18)SXE4

None.

### New Software Features in Release 12.2(18)SXE4

None.

## New Features in Release 12.2(18)SXE3

These sections describe the new features in Release 12.2(18)SXE3, 22 Aug 2005:

- [New Hardware Features in Release 12.2\(18\)SXE3, page 148](#)
- [New Software Features in Release 12.2\(18\)SXE3, page 148](#)

### New Hardware Features in Release 12.2(18)SXE3

None.

### New Software Features in Release 12.2(18)SXE3

None.

## New Features in Release 12.2(18)SXE2

These sections describe the new features in Release 12.2(18)SXE2, 23 Jun 2005:

- [New Hardware Features in Release 12.2\(18\)SXE2, page 148](#)
- [New Software Features in Release 12.2\(18\)SXE2, page 149](#)

### New Hardware Features in Release 12.2(18)SXE2

Support with Supervisor Engine 720 for these modules:

- Services SPA Carrier (SSC; [7600-SSC-400](#))



**Note**

7600-SSC-400 does not maintain state when an [NSF with SSO](#) redundancy mode switchover occurs.

- IPsec SPA ([SPA-IPSEC-2G](#)):
- [Also supported with Supervisor Engine 32](#)
- SPA-IPSEC-2G supports the features that were previously supported with [WS-SVC-IPSEC-1](#).
- See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/index.htm>

## New Software Features in Release 12.2(18)SXE2

None.

## New Features in Release 12.2(18)SXE1

These sections describe the new features in Release 12.2(18)SXE1, 18 Apr 2005:

- [New Hardware Features in Release 12.2\(18\)SXE1, page 149](#)
- [New Software Features in Release 12.2\(18\)SXE1, page 149](#)

## New Hardware Features in Release 12.2(18)SXE1

- Application-Oriented Networking (AON) Module ([WS-SVC-AON-1-K9](#)) support with Supervisor Engine 720—See these publications:  
<http://www.cisco.com/univercd/cc/td/doc/product/aon/index.htm>
- WebVPN Services Module ([WS-SVC-WEBVPN-K9](#); not supported with Supervisor Engine 2)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_7761.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_7761.htm)

## New Software Features in Release 12.2(18)SXE1

None.

## New Features in Release 12.2(18)SXE

These sections describe the new features in Release 12.2(18)SXE, 11 Apr 2005:

- [New Hardware Features in Release 12.2\(18\)SXE, page 149](#)
- [New Software Features in Release 12.2\(18\)SXE, page 151](#)

## New Hardware Features in Release 12.2(18)SXE

- Anomaly Guard Module ([WS-SVC-AGM-1-K9](#))—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/jaffa/jaffaagd.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/jaffa/jaffaagd.htm)
- Traffic Anomaly Detector Module ([WS-SVC-ADM-1-K9](#))—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/jaffa/jaffatad.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/jaffa/jaffatad.htm)

- 2700 W AC power supply for CISCO7606 chassis (PWR-2700-AC)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis\\_76xx/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis_76xx/index.htm)
- 2700 W DC power supply for CISCO7606 chassis (PWR-2700-DC)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis\\_76xx/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis_76xx/index.htm)
- 2700 W DC power supply for 4-slot chassis (PWR-2700-DC/4)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis\\_76xx/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis_76xx/index.htm)
- Catalyst 6500 series switch 4-slot chassis (WS-C6504-E)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/6500\\_ins/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/6500_ins/index.htm)
- Cisco 7600 series router 4-slot chassis (CISCO7604)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis\\_76xx/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/cis_76xx/index.htm)
- Cisco 7600 Series SPA Interface Processor-200 (7600-SIP-200)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco 7600 Series SPA Interface Processor-400 (7600-SIP-400)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco 1-Port OC-12c/STM-4c ATM Shared Port Adapter (SPA-1XOC12-ATM)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco 1-Port OC-12c/STM-4c POS Shared Port Adapter (SPA-1XOC12-POS)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco Channelized T3 to DS0 Shared Port Adapter (SPA-2XCT3/DS0, SPA-4XCT3/DS0)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3, SPA-4XT3/E3)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco OC-3c/STM-1c ATM Shared Port Adapter (SPA-2XOC3-ATM, SPA-4XOC3-ATM)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Cisco OC-3c/STM-1c POS Shared Port Adapter (SPA-2XOC3-POS, SPA-4XOC3-POS)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipsipa/index.htm>
- Fast Ethernet port adapters (PA-2FE, PA-1FE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- 1-port Packet over SONET OC3c/STM1 port adapter (PA-POS-1OC3)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514\\_1oc/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/7301/73pa/73-son/6514_1oc/index.htm)
- Content Switching Module with SSL (CSM-S; WS-X6066-SLB-S-K9)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78\\_16597.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_16597.htm)
- 10GBASE-LW XENPAK Module with WAN PHY for SMF (XENPAK-10GB-LW)

- 10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid ([DWDM-XENPAK](#))
- 10GBASE receive-only wavelength division multiplexing (WDM; [WDM-XENPAK-REC](#))
- 1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength ([GLC-BX-D](#))
- 1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength ([GLC-BX-U](#))
- Receive-only coarse or dense Wavelength Division Multiplexing (WDM) GBIC ([WDM-GBIC-REC](#))

## New Software Features in Release 12.2(18)SXE

- Any Transport over MPLS (AToM): HDLC over MPLS (HDLCoverMPLS):
  - Supported on WAN ports.
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- Any Transport over MPLS (AToM): PPP over MPLS (PPPoMPLS):
  - Supported on WAN ports.
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- ATM VC access trunk emulation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fsxeibmp.htm>



**Note** With the BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN feature configured, do not attach output service policies to VRF interfaces. (CSCsb25509)

For nonMPLS environments, see the [Interior Border Gateway Protocol \(iBGP\) Multipath Load Sharing](#) feature.

- BGP support for TTL security check—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fsxebtsh.htm>

- Bidirectional Forwarding Detection (BFD) standard implementation—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs\\_bfd.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs_bfd.htm)



**Note** Catalyst 6500 switches and Cisco 7600 routers support BFD only on Ethernet, Fast Ethernet (except PA-2FE and PA-1FE), Gigabit Ethernet, Gigabit Ethernet WAN (GE-WAN), and 10-Gigabit Ethernet ports, including Ethernet SPAs. The Catalyst 6500 switches and Cisco 7600 routers do not support BFD on PA-2FE or PA-1FE Ethernet LAN ports, or on POS, ATM, or serial WAN ports.

Also see “[Integrated IS-IS support for BFD over IPv4](#)” and “[OSPF support for BFD over IPv4](#).”

- Bridge Control Protocol (BCP)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>
- Bridging using RFC1483 Routed Encapsulation (BRE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- Clear hardware interface counters—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>
- CNS Interactive CLI—Network management applications can use the Cisco Networking Services (CNS) agents to manage network routers. The CNS agent provides the capability to send commands to a router from a programmable source. The CNS Interactive CLI feature introduces a new XML interface that allows you to send interactive commands to a router, such as commands that generate prompts for user input. A benefit of this feature is that interactive commands can be aborted before they have been fully processed. For example, for commands that generate a significant amount of output, the XML interface can be customized to limit the size of the output or the length of time allowed for the output to accumulate. The capability to use a programmable interface to abort a command before its normal termination (similar to manually aborting a command) can greatly increase the efficiency of diagnostic applications that might use this functionality. The new XML interface also allows for multiple commands to be processed in a single session. The response for each command is packaged together and sent in a single response event.
- Configurable Per VLAN MAC Learning (PVL)—See the **mac-address-table learning** command in this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>
- CSG: Content Services Gateway Release 6—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/csg/index.htm>
- DE/CLP and EXP mapping on FR/ATMoMPLS VC—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mps.htm>
- DHCP Snooping (supported only with PFC3)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snoodhcp.htm>
- Digital Optical Monitoring (DOM)—See the **show interfaces transceiver** command in this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>



**Note** See this publication for additional information about DOM:

[http://www.cisco.com/univercd/cc/td/doc/product/gbic\\_sfp/gbic\\_doc/ol\\_8031.htm](http://www.cisco.com/univercd/cc/td/doc/product/gbic_sfp/gbic_doc/ol_8031.htm)



- Dynamic ARP Inspection (DAI; supported only with PFC3)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dynarp.htm>
- Dynamic Multipoint VPN (DMVPN) Phase 2
  - In Release 12.2(18)SXE2 and later releases, supported with [SPA-IPSEC-2G](#).
  - In Release 12.2(18)SXE and later releases, supported with [WS-SVC-IPSEC-1](#).
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftgreips.htm>
- Egress ACL support for remarked DSCP (supported only with PFC3)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- EIGRP MPLS VPN PE-CE site of origin (SoO)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/s\\_mvsesoo.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/s_mvsesoo.htm)
- Embedded network management improvements—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/7600mibs/index.htm>
- Encapsulated Remote SPAN (ERSPAN)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm>
- EtherChannel Enhancement - 128 EtherChannels Support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/channel.htm>
- Ethernet over MPLS (EoMPLS) per VLAN QoS—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mpls.htm>
- Field-programmable device upgrade tool—The Cisco SPA field-programmable device (FPD) upgrade tool provides customers and field engineers a consistent way across platforms to upgrade firmware or images for the programmable devices (for example, FPGAs, PLDs, ROMMON). The customer can get proper images from Cisco.com, and use this tool to automatically download (with a flash card or TFTP) to the FPD tool, or manually if needed. The FPD tool provides a convenient and safe way for customer to upgrade an FPD for related bug fixes and feature enhancement with minimum system impact. The FPD tool significantly improves customer satisfaction and product reliability.
- Frame Relay virtual circuit (VC) bundling—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- HQoS support for Ethernet over MPLS (EoMPLS) VC—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- IDSM-2 EtherChannel load balancing—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids11/cliguide/index.htm>
- Integrated IS-IS global default metric—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtisglob.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtisglob.htm)
- Integrated IS-IS protocol shutdown support maintaining configuration parameters—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtisprot.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtisprot.htm)

- Integrated IS-IS support for BFD over IPv4—See this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs\\_bfd.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs_bfd.htm)



**Note** Also see “[Bidirectional Forwarding Detection \(BFD\) standard implementation.](#)”

- Invalid Special Parameter Index (SPI) Recovery—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gt\\_ispir.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_ispir.htm)
- IP routing of RFC1483 ATM bridge encapsulation (RBE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- PFC3 hardware support for IPv4 multicast over point-to-point GRE tunnels—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter\\_c/icflogin.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflogin.htm)



**Note** Releases earlier than Release 12.2(18)SXE supported IPv4 multicast over point-to-point GRE tunnels in software on the MSFC. The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

- IPv6 access services: DHCPv6 prefix delegation—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6\\_vgf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm)
- IPv6 hardware: multicast assist—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv6.htm>
- IPv6 multicast RPR/RPR+ support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/redund.htm>
- IPv6 multicast: Bootstrap Router (BSR)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6\\_c/sa\\_mcast.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm)
- IPv6 Multicast: HW assisted egress replication—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv6.htm>
- IPv6 QoS: (quality of service)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- IS-IS caching of redistributed routes—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/isredrib.htm>
- IS-IS support for priority-driven IP prefix RIB installation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fslocrib.htm>
- Key rollover for certificate renewal—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_7/gtkyroll.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtkyroll.htm)

- Lawful Intercept with CSG Module (CSG-LI; [WS-SVC-CSG-1](#)) on Supervisor Engine 720:
  - Also supported on Supervisor Engine 2.
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/csg/csg4/csgnrl4.htm>
- Layer 2 traceroute—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/l2trace.htm>
- MLD snooping—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snoopmld.htm>
- MPLS LDP - Inbound Label Binding Filtering—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsinbd4.htm>
- MPLS LSP ping/traceroute and AToM VCCV—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/sx\\_lspt.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/sx_lspt.htm)
- MQC: distribution of remaining bandwidth (supported only on WAN ports)—You configure QoS features on an interface using the modular QoS CLI (MQC). Using MQC, you create service policies for traffic classes and attach the policies to an interface. You can use MQC to specify how the remaining bandwidth is distributed among the interface or subinterface output queues. The remaining bandwidth is the available bandwidth left on an interface or subinterface after all guaranteed traffic is accounted for. The amount of remaining bandwidth available for use is determined by the excess information rate (EIR) configured for the queue.

The **bandwidth remaining percent** command allows you to configure the remaining bandwidth for output queues. The aggregate of all user-configured EIR bandwidth percentages cannot exceed 100 percent. If the aggregate of all remaining bandwidth is less than 100 percent, the remainder is evenly split among user queues (including the default queue) that do not have a remaining bandwidth percentage configured. The minimum EIR value of each output queue is 1.

This example shows how to use the **bandwidth remaining percent** command to distribute percentages of remaining bandwidth to various traffic classes in a policy map:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map myPolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# class prec1
Router(config-pmap-c)# bandwidth remaining percent 30
Router(config-pmap-c)# class prec2
Router(config-pmap-c)# bandwidth remaining percent 10
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router# show policy-map myPolicy
  Policy Map myPolicy
    Class prec1
      bandwidth remaining percent 30
    Class prec2
      bandwidth percent 50
      bandwidth remaining percent 10
    Class class-default
      bandwidth remaining percent 20
Router#
```

- Multicast-VPN: Multicast Support for MPLS VPN—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mvvpn.htm>



**Note**

Support for MVPN also includes support for multicast VRF (MVRF). MVRF is also known as multicast over VRF-lite. MVPN and MVRF are supported in PFC3B or PDC3BXL mode.

- Multipoint bridging (MPB)—See these publications:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/pos.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/atm.htm>

- NetFlow - Bridged Flow Statistics—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm>

- Netflow Multiple Export Destinations:

- In Release 12.2(18)SXF and later releases, supported with Supervisor Engine 32
- In Release 12.2(18)SXE and later releases, supported with Supervisor Engine 720
- In Release 12.2(18)SXD and later releases, supported with Supervisor Engine 2
- Allows entry of a second **ip flow-export destination** command
- See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm>

- OSPF link state database overload protection—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/ospfopro.htm>

- OSPF link-local signaling (LLS) per interface basis—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/ospflls.htm>

- OSPF MIB support of RFC 1850 and latest extensions—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/7600mibs/index.htm>

- OSPF support for BFD over IPv4—See this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs\\_bfd.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/fs_bfd.htm)



**Note**

Also see “[Bidirectional Forwarding Detection \(BFD\) standard implementation.](#)”

- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/ospffa.htm>

- OSPF support for unlimited software VRFs per provider edge (PE) router—See this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtospfvf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtospfvf.htm)

- Packet classification based on layer3 packet-length (supported on WAN ports)—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmchpkt.htm>

- Per port MAC limiting—See the **mac-address-table limit** command in this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>
- Per VLAN load balancing for advanced QinQ service mapping—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- PKI AAA authorization using the entire subject name—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_11/gt\\_dnall.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gt_dnall.htm)
- Port security on 802.1Q tunnel ports, port security on private VLAN ports, port security on trunk ports, port security with 4096 secure MAC addresses, and port security with sticky MAC addresses—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/port\\_sec.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/port_sec.htm)
- Protected private key storage—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_7/gt\\_ppkey.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_ppkey.htm)
- QoS: Aggregated DSCP / Precedence Values for WRED—Aggregates multiple DSCP or IP Precedence values for a single minimum or maximum threshold and marks probability when specifying WRED parameters for **7600-SIP-400** ATM SPAs.
- QoS: ingress shaping on FlexWAN module interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- QoS: match VLAN on OSMs—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- QoS: percentage based policing on WAN ports—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12s\\_pctpg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12s_pctpg.htm)
- Query mode definition per trustpoint—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_7/gt\\_qerym.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_qerym.htm)
- Query multiple servers during certificate revocation check—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_7/gtcertrc.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtcertrc.htm)
- Re-enroll using existing certificate—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zh13/gthttpca.htm>
- Redundant Supervisor Engine 720 system high availability enhancement:
  - When a module is inserted or removed (OIR), a data integrity mechanism engages to ensure that no corrupt data is transferred on the backplane bus. This mechanism can cause a minimal amount of packet loss during OIR in a non-DFC-based system. For a DFC-based system, this mechanism does not have an effect on any traffic during OIR.

This feature causes the redundant supervisor engine to operate as a DFC-based module (the redundant supervisor engine operates as a non-DFC-based module by default), which protects the redundant supervisor engine from any packet loss during module OIR because it is disconnected from the backplane bus.

This feature only applies to a system with redundant supervisor engines and DFCs on all the modules. The supervisor engine uplink ports (on both standby and active) cannot be used with this configuration.

- See the **fabric switching-mode allow dcef-only** command in this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>
- RFC-1490 bridging on FlexWAN interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm>
- RADIUS Load Balancing (RLB) IMSI sticky—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/slbsxe1.htm>
- SafeNet IPsec VPN client support—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_14/gt\\_scse.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_scse.htm)
- SCP health monitoring for enhanced-Flex WAN—The SCP health monitor feature provides improved debugging capabilities for problems that cause WAN module resets because of SCP keepalive failures.
- Show diagnostic sanity—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm>
- Show Top-N—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/topn.htm>
- SLB: stateful failover within single chassis—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/slbsxe1.htm>
- SLB: interface-aware—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/slbsxe1.htm>
- SPAN destination port permit list—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm>
- SSM mapping for IPv6—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6\\_vgf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm)
- Strict priority low latency queueing (LLQ) on WAN ports—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- Sub interface features - phase 1—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/layer3.htm>
- Bandwidth Command for HQoS Parent Class Support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/index.htm>
- Uni-Directional Link Routing (UDLR)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/ude\\_udlr.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/ude_udlr.htm)
- Unicast flood blocking (UFB)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/blocking.htm>
- **verify certificate chain** command—Allows the use of the Layer 2 overhead specification for shaping.
- VLANs over IP unnumbered sub-interfaces—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtunvlan.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtunvlan.htm)

- ATM OAM ping—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/12a/tmpng.htm>

## New Features in Release 12.2(18)SXD7a

These sections describe the new features in Release 12.2(18)SXD7a, 15 Sep 2006

- [New Hardware Features in Release 12.2\(18\)SXD7a, page 159](#)
- [New Software Features in Release 12.2\(18\)SXD7a, page 159](#)

### New Hardware Features in Release 12.2(18)SXD7a

None.

### New Software Features in Release 12.2(18)SXD7a

None.

## New Features in Release 12.2(18)SXD7

These sections describe the new features in Release 12.2(18)SXD7, 15 Dec 2005:

- [New Hardware Features in Release 12.2\(18\)SXD7, page 159](#)
- [New Software Features in Release 12.2\(18\)SXD7, page 159](#)

### New Hardware Features in Release 12.2(18)SXD7

None.

### New Software Features in Release 12.2(18)SXD7

None.

## New Features in Release 12.2(18)SXD6

These sections describe the new features in Release 12.2(18)SXD6, 22 Aug 2005:

- [New Hardware Features in Release 12.2\(18\)SXD6, page 159](#)
- [New Software Features in Release 12.2\(18\)SXD6, page 160](#)

### New Hardware Features in Release 12.2(18)SXD6

None.

## New Software Features in Release 12.2(18)SXD6

None.

## New Features in Release 12.2(18)SXD5

These sections describe the new features in Release 12.2(18)SXD5, 16 May 2005:

- [New Hardware Features in Release 12.2\(18\)SXD5, page 160](#)
- [New Software Features in Release 12.2\(18\)SXD5, page 160](#)

## New Hardware Features in Release 12.2(18)SXD5

None.

## New Software Features in Release 12.2(18)SXD5

None.

## New Features in Release 12.2(18)SXD4

These sections describe the new features in Release 12.2(18)SXD4, 24 Mar 2005:

- [New Hardware Features in Release 12.2\(18\)SXD4, page 160](#)
- [New Software Features in Release 12.2\(18\)SXD4, page 160](#)

## New Hardware Features in Release 12.2(18)SXD4

None.

## New Software Features in Release 12.2(18)SXD4

None.

## New Features in Release 12.2(18)SXD3

These sections describe the new features in Release 12.2(18)SXD3, 13 Dec 2004:

- [New Hardware Features in Release 12.2\(18\)SXD3, page 161](#)
- [New Software Features in Release 12.2\(18\)SXD3, page 161](#)



## New Hardware Features in Release 12.2(18)SXD3

- Distributed Forwarding Card 3BXL (DFC3BXL; [WS-F6K-DFC3BXL](#)) for use on dCEF256 and CEF256 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22.
- Distributed Forwarding Card 3B (DFC3B; [WS-F6K-DFC3B](#)) for use on dCEF256 and CEF256 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22.
- Anomaly Guard Module ([WS-SVC-AGM-1-K9](#))—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/jaffa/jaffaagd.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/jaffa/jaffaagd.htm)
- Traffic Anomaly Detector Module ([WS-SVC-ADM-1-K9](#))—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/secure/ad\\_g/jaffa/jaffatad.htm](http://www.cisco.com/univercd/cc/td/doc/product/secure/ad_g/jaffa/jaffatad.htm)

## New Software Features in Release 12.2(18)SXD3

- Source Specific Multicast (SSM) Mapping:
  - Do not configure SSM mapping in a VLAN that supports IGMPv3 multicast receivers.
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gtssmma.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm)

## New Features in Release 12.2(18)SXD2

These sections describe the new features in Release 12.2(18)SXD2, 22 Oct 2004:

- [New Hardware Features in Release 12.2\(18\)SXD2, page 161](#)
- [New Software Features in Release 12.2\(18\)SXD2, page 161](#)

## New Hardware Features in Release 12.2(18)SXD2

None.

## New Software Features in Release 12.2(18)SXD2

None.

## New Features in Release 12.2(18)SXD1

These sections describe the new features in Release 12.2(18)SXD1, 30 Sep 2004:

- [New Hardware Features in Release 12.2\(18\)SXD1, page 162](#)
- [New Software Features in Release 12.2\(18\)SXD1, page 162](#)

## New Hardware Features in Release 12.2(18)SXD1



### Note

In Release 12.2(18)SXD1, all service modules have been tested with OSMs, the FlexWAN module, and the Enhanced FlexWAN module.

- Persistent Storage Device (PSD; [WS-SVC-PSD-1](#)) support with Supervisor Engine 720:
  - [Also supported with Supervisor Engine 2](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_4781.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_4781.htm)
- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 720:
  - [WS-SVC-MWAM-1](#)
  - [Also supported with Supervisor Engine 32](#)
  - [Also supported with Supervisor Engine 2](#)
  - See these publications for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/servmod/esa\\_mwam.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/servmod/esa_mwam.htm)  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/mwam/index.htm>



### Note

With Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an [NSF with SSO](#) redundancy mode switchover occurs. With Release 12.2(18)SXD, WS-SVC-MWAM-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.

- Content Services Gateway (CSG) support with Supervisor Engine 720
  - [WS-SVC-CSG-1](#)
  - [Also supported with Supervisor Engine 2](#)
  - See this publication for more information:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/csg/index.htm>

## New Software Features in Release 12.2(18)SXD1

- MPLS Traffic Engineering (TE) Fast Reroute (FRR) Link and Node Protection—See these publications:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/fsfrr24.htm>



### Note

Also see [MPLS Traffic Engineering DiffServ Aware \(DS-TE\)](#).  
MPLS TE FRR Link and Node Protection is not supported on these interface types:

- Port channel interfaces
- Switch virtual interfaces (SVIs)
- Multiple link point-to-point protocol (MLPPP) interfaces
- Multilink Frame Relay (MLFR or MFR)

- VRF Aware IPsec:
  - In Release 12.2(18)SXE2 and later releases, supported with [SPA-IPSEC-2G](#).
  - In Release 12.2(18)SXD1 and later releases, supported with Supervisor Engine 720 and [WS-SVC-IPSEC-1](#).
  - Not supported with Supervisor Engine 2 and WS-SVC-IPSEC-1.
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_14459.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14459.htm)
- Hardware Control Plane Interface for Control Plane Policing (CoPP):
  - With Cisco IOS 12.2SX releases, only the PFC3 supports CoPP.
  - The PFC3 does not support CoPP output rate limiting (policing).
  - The PFC3 does not support the CoPP silent operation mode.
  - The PFC3 does not support the **match protocol arp** command.
  - The PFC3 automatically installs the CoPP service policy on all DFC-equipped switching modules.
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dos.htm>
- Web Cache Control Protocol (WCCP) support with Supervisor Engine 720—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/wccp.htm>
- The **fabric switching-mode allow dcef-only** command support with [Supervisor Engine 2](#) (CSCec05612):
  - By default, the two Gigabit Ethernet ports on a redundant Supervisor Engine 2 rely on the PFC on the active supervisor engine for all forwarding decisions.
  - The **fabric switching-mode allow dcef-only** command disables the Gigabit Ethernet ports on the redundant Supervisor Engine 2 to ensure that all modules are operating in dCEF mode.
  - Module OIR is nondisruptive when all active switching modules are dCEF-enabled.

## New Features in Release 12.2(18)SXD

These sections describe the new features in Release 12.2(18)SXD, 26 Jul 2004:

- [New Hardware Features in Release 12.2\(18\)SXD, page 163](#)
- [New Software Features in Release 12.2\(18\)SXD, page 165](#)

## New Hardware Features in Release 12.2(18)SXD



### Note

With Release 12.2(18)SXD and later releases, OSMs require a minimum of 128 MB of dynamic random-access memory (SDRAM)—See this publication for memory upgrade procedures:

[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/osmodule/app\\_upgr.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/osmodule/app_upgr.htm)

- [WS-F6700-DFC3BXL](#) Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22
- Distributed Forwarding Card 3B (DFC3B; [WS-F6700-DFC3B](#)) for use on CEF720 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22
- Wireless LAN service module ([WS-SVC-WLAN-1-K9](#)) support with Supervisor Engine 720—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_6097.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_6097.htm)
- [WS-X6066-SLB-S-K9](#) Content Switching Module with SSL (CSM-S) with Supervisor Engine 2:
  - Also supported with Supervisor Engine 720
  - See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78\\_16597.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_16597.htm)
- 6000 W AC power supply ([WS-CAC-6000W](#))

## New Software Features in Release 12.2(18)SXD

- Cisco Nonstop Forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy on Supervisor Engine 720 and Supervisor Engine 2—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nsfsso.htm>



### Note

- Release 12.2(18)SXD and later releases do not support the SRM with SSO redundancy mode (see the “New Software Features in Release 12.2(17b)SXA” section on page 180).
- With PFC3, NSF with SSO supports multicast traffic.
- NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, or MPLS.
- These protocols can coexist with NSF with SSO redundancy mode, but there is no stateful support for them:
  - MPLS and LDP
  - GLBP
  - HSRP
  - VRRP

Following an NSF with SSO switchover, traffic loss occurs on the links where the protocols are configured until the protocols converge.

- The following modules do not maintain state when an NSF with SSO redundancy mode switchover occurs:
  - IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)).
  - [WS-X6066-SLB-APC](#) (CSM; with Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-APC maintains state when an NSF with SSO redundancy mode switchover occurs).
  - [WS-SVC-FWM-1-K9](#) firewall services module (with Release 12.2(18)SXD3 and later Cisco IOS releases and with Firewall Services Module Software Release 2.3(1), WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs).
  - [WS-SVC-SSL-1](#) secure sockets layer (SSL) services module.
  - [WS-SVC-MWAM-1](#) (with Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an NSF with SSO redundancy mode switchover occurs).
  - [WS-SVC-PSD-1](#) (with Release 12.2(18)SXD1 and later releases, WS-SVC-PSD-1 maintains state when an NSF with SSO redundancy mode switchover occurs).

- ARP ACLs for QoS Filtering (supported only with PFC3)—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>



### Note

Supervisor Engine 2 applies IP ACLs to ARP traffic.

- Protocol-Independent MAC ACL Filtering (supported only in PFC3BXL or PFC3B mode)—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>

- Netflow Multiple Export Destinations:
  - In Release 12.2(18)SXE and later releases, supported with Supervisor Engine 720
  - In Release 12.2(18)SXD and later releases, supported with Supervisor Engine 2
  - Allows entry of a second **ip flow-export destination** command
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm>
- Lawful Intercept with CSG Module (CSG-LI; **WS-SVC-CSG-1**) on Supervisor Engine 2:
  - Also supported on Supervisor Engine 720.
  - See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/csg/csg4/csgnrl4.htm>



**Note** In releases earlier than Release 12.2(18)SXD1, the Lawful Intercept feature on the **WS-SVC-CSG-1** has not been tested with OSMs or the FlexWAN module or the Enhanced FlexWAN module.

- For the IPsec VPN Acceleration services module (**WS-SVC-IPSEC-1**):



**Note** In Release 12.2(18)SXE2 and later releases, these features are also supported with **SPA-IPSEC-2G**.

- Easy VPN Server features—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunit y.htm>
- Distinguished Name-Based Crypto Maps—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdna cl.htm>
- IKE: Initiate Aggressive Mode—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft\\_ike ag.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ike ag.htm)
- Real-Time Resolution for IPsec Tunnel Peer—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtrlr es.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtrlr es.htm)
- IPsec VPN Accounting—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft\\_e vpna.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_e vpna.htm)
- Trusted Root Certification Authority—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtrust rt.htm>
- Certificate Security Attribute-Based Access Control—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcrt acl.htm>

- Trustpoint CLI—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm>
- Multiple RSA Key Pair Support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm>
- Manual Certificate Enrollment (TFTP and Cut-and-Paste)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancert.htm>
- Source Interface Selection for Outgoing Traffic with Certificate Authority—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft\\_asissh.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_asissh.htm)
- IP Security VPN Monitoring—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gt\\_ipsvm.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ipsvm.htm)
- Encrypted Preshared Key—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gt\\_e\\_psk.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_e_psk.htm)
- Crypto Conditional Debug Support—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gt\\_dbcry.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_dbcry.htm)
- Certificate Autoenrollment—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftautoen.htm>
- Metro Ethernet Advanced QinQ Service Mapping—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/pwan.htm>
- Cisco IOS server load balancing (Cisco IOS SLB):
  - Initial support on Supervisor Engine 720 including GGSN-SLB Messaging (previously supported on Supervisor Engine 2)
  - Initial support for Home Agent Loadbalancing on Supervisor Engine 720 and Supervisor Engine 2

See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxd/slbsxd1.htm>



**Note** Web Cache Control Protocol (WCCP) Layer 2 PFC redirection is supported with Cisco IOS SLB. Other WCCP configurations are not compatible with Cisco IOS SLB.

- Cisco IOS Secure Copy (SCP)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftscp.htm>

- Cisco IOS IP Event Dampening—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftipevdp.htm>
- BGP Configuration Using Peer Templates—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s\\_bgpct.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s_bgpct.htm)
- BGP Cost Community—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s\\_bgpcc.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s_bgpcc.htm)
- BGP Dynamic Update Peer-Groups—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s\\_bgpdpg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s_bgpdpg.htm)
- BGP Route-Map Continue—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gt\\_brmcs.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_brmcs.htm)
- BGP Route-Map Policy List Support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbgrprpl.htm>
- BGP Restart Session After Max-Prefix Limit—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbrsmp.htm>
- BGP Increased Support of Numbered AS-path Access Lists to 500—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftiaaspa.htm>
- IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fsisiadv.htm>
- IS-IS Incremental SPF—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/isisispf.htm>
- IS-IS Support for Route Tags—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gtisitag.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtisitag.htm)
- IS-IS Limit on Number of Redistributed Routes—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsiredis.htm>
- OSPF Support for Fast Hellos—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fasthelo.htm>
- OSPF Forwarding Address Suppression in Translated Type-5 LSAs—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftoadsup.htm>
- OSPF Incremental Shortest Path First (i-SPF)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/ospfispf.htm>



- OSPF Limit on Number of Redistributed Routes—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsoredis.htm>
- OSPF Support for Link State Advertisement (LSA) Throttling—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsolsath.htm>
- OSPF Inbound Filtering Using Route Maps with a Distribute List—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/routmap.htm>
- On LAN ports, Multi-VRF for CE Routers (VRF Lite) with IPv4 forwarding between VRFs interfaces, IPv4 ACLs, and IPv4 HSRP—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mps.htm>



**Note** Multi-VRF for CE Routers (VRF Lite) with the PFC3 supports multi-VRF CE functionality with [EIGRP](#), OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported. Also supported on [WAN ports](#).

- MPLS Traffic Engineering DiffServ Aware (DS-TE)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fdserv3.htm>



**Note** Also see [MPLS Traffic Engineering \(TE\) Fast Reroute \(FRR\) Link and Node Protection](#). MPLS DS-TE is not supported on these interface types:

- Port channel interfaces
- Switch virtual interfaces (SVIs)
- Multiple link point-to-point protocol (MLPPP) interfaces
- Multilink Frame Relay (MLFR or MFR)

- MPLS Traffic Engineering Forwarding Adjacency—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa\\_3.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa_3.htm)
- MPLS Traffic Engineering (TE) Interarea Tunnels—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsiarea3.htm>
- MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) —See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fseipece.htm>



**Note** The MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) feature also provides EIGRP support for VRF Lite.

- You can use the **set ip dscp** and **set ip precedence** policy map class commands on non-IP traffic to mark the internal DSCP value, which is the basis of the egress Layer 2 CoS value. (CSCec34212)

- Support for the **mls netflow maximum-flows** command. (CSCee28200)
- Support for the allowed VLAN list to filter the traffic transmitted from a SPAN destination trunk port. (CSCeb01318)
- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch 1.1 (CVDM-C6500)  
Resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module 1.1 (CVDM-SSLSM)  
Enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for the Cisco Content Switching Module 1.1 (CVDM-CSM)  
Enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.
  - CiscoView Device Manager for the Cisco IPsec VPN Acceleration services module (**WS-SVC-IPSEC-1**) 1.1 (CVDM-VPNSM)  
Allows users to manage VLANs, create and configure VPNs, and configure settings such as IPsec rules on their VPN module. It is a task-based tool that allows users to control the versatility of their Cisco VPN module by offering configuration wizards based on recommended practices in tasks such as creating Site-to-Site VPNs and configuring GRE tunnels.

To access all CiscoView Device Manager documentation, go to this URL:

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

## New Features in Release 12.2(17d)SXB11a

These sections describe the new features in Release 12.2(17d)SXB11a, 17 Apr 2006:

- [New Hardware Features in Release 12.2\(17d\)SXB11a, page 170](#)
- [New Software Features in Release 12.2\(17d\)SXB11a, page 170](#)

### New Hardware Features in Release 12.2(17d)SXB11a

None.

### New Software Features in Release 12.2(17d)SXB11a

None.

## New Features in Release 12.2(17d)SXB11

These sections describe the new features in Release 12.2(17d)SXB11, 17 Nov 2005:

- [New Hardware Features in Release 12.2\(17d\)SXB11, page 171](#)
- [New Software Features in Release 12.2\(17d\)SXB11, page 171](#)

### New Hardware Features in Release 12.2(17d)SXB11

None.

### New Software Features in Release 12.2(17d)SXB11

None.

## New Features in Release 12.2(17d)SXB10

These sections describe the new features in Release 12.2(17d)SXB10, 16 Aug 2005:

- [New Hardware Features in Release 12.2\(17d\)SXB10, page 171](#)
- [New Software Features in Release 12.2\(17d\)SXB10, page 171](#)

### New Hardware Features in Release 12.2(17d)SXB10

None.

### New Software Features in Release 12.2(17d)SXB10

None.

## New Features in Release 12.2(17d)SXB9

These sections describe the new features in Release 12.2(17d)SXB8, 21 Jul 2005:

- [New Hardware Features in Release 12.2\(17d\)SXB9, page 171](#)
- [New Software Features in Release 12.2\(17d\)SXB9, page 171](#)

### New Hardware Features in Release 12.2(17d)SXB9

None.

### New Software Features in Release 12.2(17d)SXB9

None.

## New Features in Release 12.2(17d)SXB8

These sections describe the new features in Release 12.2(17d)SXB8, 02 May 2005:

- [New Hardware Features in Release 12.2\(17d\)SXB8, page 172](#)
- [New Software Features in Release 12.2\(17d\)SXB8, page 172](#)

### New Hardware Features in Release 12.2(17d)SXB8

None.

### New Software Features in Release 12.2(17d)SXB8

None.

## New Features in Release 12.2(17d)SXB7

These sections describe the new features in Release 12.2(17d)SXB7, 01 Mar 2005:

- [New Hardware Features in Release 12.2\(17d\)SXB7, page 172](#)
- [New Software Features in Release 12.2\(17d\)SXB7, page 172](#)

### New Hardware Features in Release 12.2(17d)SXB7

- WebVPN Services Module ([WS-SVC-WEBVPN-K9](#); not supported with Supervisor Engine 2)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_7761.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_7761.htm)

### New Software Features in Release 12.2(17d)SXB7

None.

## New Features in Release 12.2(17d)SXB6

These sections describe the new features in Release 12.2(17d)SXB6, 21 Dec 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB6, page 173](#)
- [New Software Features in Release 12.2\(17d\)SXB6, page 173](#)

## New Hardware Features in Release 12.2(17d)SXB6

- Distributed Forwarding Card 3BXL (DFC3BXL; [WS-F6700-DFC3BXL](#)) for use on CEF720 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22.
- Distributed Forwarding Card 3B (DFC3B; [WS-F6700-DFC3B](#)) for use on CEF720 modules—See the “[Distributed and Centralized Forwarding Cards](#)” section on page 22.

## New Software Features in Release 12.2(17d)SXB6

None.

## New Features in Release 12.2(17d)SXB5

These sections describe the new features in Release 12.2(17d)SXB5, 01 Nov 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB5, page 173](#)
- [New Software Features in Release 12.2\(17d\)SXB5, page 173](#)

## New Hardware Features in Release 12.2(17d)SXB5

None.

## New Software Features in Release 12.2(17d)SXB5

None.

## New Features in Release 12.2(17d)SXB4

These sections describe the new features in Release 12.2(17d)SXB4, 07 Sep 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB4, page 173](#)
- [New Software Features in Release 12.2\(17d\)SXB4, page 173](#)

## New Hardware Features in Release 12.2(17d)SXB4

None.

## New Software Features in Release 12.2(17d)SXB4

None.

## New Features in Release 12.2(17d)SXB3

These sections describe the new features in Release 12.2(17d)SXB3, 17 Aug 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB3, page 174](#)
- [New Software Features in Release 12.2\(17d\)SXB3, page 174](#)

## New Hardware Features in Release 12.2(17d)SXB3

None.

## New Software Features in Release 12.2(17d)SXB3

- You can use the **set ip dscp** and **set ip precedence** policy map class commands on non-IP traffic to mark the internal DSCP value, which is the basis of the egress Layer 2 CoS value. (CSCee56918)

## New Features in Release 12.2(17d)SXB2

These sections describe the new features in Release 12.2(17d)SXB2, 21 Jul 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB2, page 174](#)
- [New Software Features in Release 12.2\(17d\)SXB2, page 174](#)

## New Hardware Features in Release 12.2(17d)SXB2

None.

## New Software Features in Release 12.2(17d)SXB2

- Initial support for the **mls rate-limit multicast non-rpf** command. (CSCee95301)
- Initial support for the **mls ip cef load-sharing [full] [simple | optimized]** command. (CSCed74512)

## New Features in Release 12.2(17d)SXB1

These sections describe the new features in Release 12.2(17d)SXB1, 01 Jun 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB1, page 174](#)
- [New Software Features in Release 12.2\(17d\)SXB1, page 175](#)

## New Hardware Features in Release 12.2(17d)SXB1



### Note

Release 12.2(17d)SXB1 and later releases do not support **XENPAK-10GB-ER** units with part number 800-24557-01, as described in this external field notice (CSCee47030):

<http://www.cisco.com/warp/public/770/fn29736.shtml>

- **WS-SUP720-3B** Supervisor Engine 720 with Policy Feature Card 3B (PFC3B)—See the “Supervisor Engines” section on page 11
- **WS-F6K-PFC3B**= Policy Feature Card 3BXL (PFC3B)—See the “Policy Feature Cards” section on page 18
- 1000BASE-ZX GBIC (**GLC-ZX-SM**)
- 10GBASE-CX4 XENPAK Module for CX4 (copper) cable (**XENPAK-10GB-CX4**)

## New Software Features in Release 12.2(17d)SXB1

- GGSN-SLB Messaging (supported only with Supervisor Engine 2)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12217sxb/slbsxb2.htm>
- Initial support for the **mls netflow usage notify** global configuration mode command to configure NetFlow table usage monitoring. (CSCdz64998)
- Initial support in the **show mls statistics** command for display of the approximate Layer 2 switching rate in packets-per-second. (CSCee28215; see resolved caveat CSCee92338)
- Distributed LFI (dLFI) and distributed QoS (dQoS) over Leased Lines on FlexWAN module interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdlfi2.htm>

## New Features in Release 12.2(17d)SXB

These sections describe the new features in Release 12.2(17d)SXB, 05 Mar 2004:

- [New Hardware Features in Release 12.2\(17d\)SXB, page 175](#)
- [New Software Features in Release 12.2\(17d\)SXB, page 177](#)

## New Hardware Features in Release 12.2(17d)SXB

- 48-port Gigabit Ethernet SFP switching module ([WS-X6748-SFP](#); supported only with Supervisor Engine 720)
- IEEE 802.3af PoE daughtercard for [WS-X6148-RJ-45](#) and [WS-X6148-RJ-21](#) ([WS-F6K-FE48-AF](#))
- IEEE 802.3af PoE daughtercard for [WS-X6548-GE-TX](#) and [WS-X6148-GE-TX](#) ([WS-F6K-GE48-AF](#))
- [Supervisor Engine 2](#), PFC2, and MSFC2
  - [WS-X6K-S2U-MSFC2](#)
  - [WS-X6K-S2-MSFC2](#) with upgraded memory

See the [“Supported Hardware”](#) section on [page 10](#) for information about the hardware supported with Supervisor Engine 2.

- Distributed Forwarding Card (DFC; [WS-F6K-DFC](#)); requires Switch Fabric Module; supported only with Supervisor Engine 2
- The Switch Fabric Module (SFM; [WS-C6500-SFM](#)); does not support [13-slot chassis](#); supported only with Supervisor Engine 2
- [WS-X6500-SFM 2](#) Switch Fabric Module version 2 (SFM2); supports all chassis; supported only with Supervisor Engine 2
- Persistent Storage Device (PSD) support with Supervisor Engine 2:
  - [WS-SVC-PSD-1](#)
  - Also supported with Supervisor Engine 720
  - See this publication for more information:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_4781.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_4781.htm)

- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 2:
  - [WS-SVC-MWAM-1](#)
  - [Also supported with Supervisor Engine 720](#)
  - [Also supported with Supervisor Engine 32](#)
  - See this publication for more information:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/mwam/index.htm>
- Content Services Gateway (CSG) support with Supervisor Engine 2:
  - [WS-SVC-CSG-1](#)
  - [Also supported with Supervisor Engine 720](#)
  - See this publication for more information:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/csg/index.htm>
- Firewall Services module support with Supervisor Engine 2:
  - [WS-SVC-FWM-1-K9](#)
  - [Also supported with Supervisor Engine 720](#)
  - [Also supported with Supervisor Engine 32](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm)
- Network Analysis Module support with Supervisor Engine 2:
  - [WS-SVC-NAM-1](#) and [WS-SVC-NAM-2](#)
  - [Also supported with Supervisor Engine 720](#)
  - [Also supported with Supervisor Engine 32](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78\\_15353.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_15353.htm)
- Intrusion Detection System Module 2 support with Supervisor Engine 2:
  - [WS-SVC-IDSM2-K9](#)
  - [Also supported with Supervisor Engine 720](#)
  - [Also supported with Supervisor Engine 32](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029\\_02.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029_02.htm)
- Content Switching Module (CSM) support with Supervisor Engine 2:
  - [WS-X6066-SLB-APC](#)
  - [Also supported with Supervisor Engine 720](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/csm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/index.htm)



- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 2:
  - [WS-SVC-SSL-1](#)
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_5277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_5277.htm)

## New Software Features in Release 12.2(17d)SXB

- Secure Shell SSH Version 2 Client Support—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gt\\_ssh2.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ssh2.htm)
- Generic Online Diagnostics (GOLD) for Supervisor Engine 2—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm>
- Enhanced support for interface link status messages (CSCeb06765). See the following publication for more information:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/i1.htm>
- Support for the **mls qos trust [dscp | ip-precedence | cos]** command on [WS-X6148-RJ-45](#), [WS-X6148-RJ-45V](#), [WS-X6148-RJ-21](#), and [WS-X6148-RJ-21V](#) switching modules. (CSCec30649)
- VACL capture on LAN and WAN ports—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm>




---

**Note** VACL capture is not supported on [WS-X6708-10GE](#) ports.

---

- Hardware-supported counters for hardware-supported ACLs, displayed by the **show tcam interface** command (supported only in PFC3BXL or PFC3B mode). See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/show4.htm>
- Optimized ACL logging (supported only with PFC3)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/acl.htm>
- Release 12.2(17d)SXB provides initial Release 12.2SX support for Supervisor Engine 2. Support for Supervisor Engine 2 in Release 12.2SX has all the Supervisor Engine 2 features supported by Release 12.1(20)E, including these:
  - Web Cache Control Protocol (WCCP) support with Supervisor Engine 2—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/wccp.htm>
  - Cisco IOS server load balancing (SLB) support with Supervisor Engine 2—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12217sxb/slb17sxb.htm>




---

**Note** Web Cache Control Protocol (WCCP) Layer 2 PFC redirection is supported with Cisco IOS SLB. Other WCCP configurations are not compatible with Cisco IOS SLB.

---

- Network-Based Application Recognition (NBAR) for LAN ports; supported only with Supervisor Engine 2—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm>
- Unknown unicast flood protection (UUF); supported only with Supervisor Engine 2—See the **mac-address-table unicast-flood** command at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/i1.htm1>
- Release 12.2(17d)SXB provides initial support with Supervisor Engine 2 for these features in software. These features are already supported with Supervisor Engine 720 in hardware:
  - IPv6 unicast traffic on LAN and WAN interfaces—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6\\_vgf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm)
  - Bidirectional Protocol Independent Multicast (PIM)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm>
- Release 12.2(17d)SXB provides initial support with Supervisor Engine 2 for these features. These features are already supported with Supervisor Engine 720:
  - Gateway Load Balancing Protocol (GLBP)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f\\_s\\_glb2.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f_s_glb2.htm)
  - Interior Border Gateway Protocol (IBGP) multipath—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f\\_sbgpls.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f_sbgpls.htm)
  - Virtual Router Redundancy Protocol (VRRP)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st\\_vrrpx.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st_vrrpx.htm)
  - Distributed Multilink Frame Relay (FRF.16)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/dmfr.htm>
  - MPLS VPN—Inter-AS—IPv4 BGP Label Distribution—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f\\_siaslbl.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/f_siaslbl.htm)
  - Virtual Private LAN Services (VPLS) on the Optical Services Modules—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mppls.htm>
  - Any Transport over MPLS (AToM) features:
    - Supported on WAN ports
    - Ethernet over MPLS (EoMPLS)
    - Frame Relay over MPLS (FRoMPLS)
    - ATM Single Cell Relay over MPLS-VC Mode (CRoMPLS)
    - ATM AAL5 over MPLS (AAL5oMPLS)
 See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mppls.htm>

- TDR cable diagnostics—See “TDR cable diagnostics” in the “New Software Features in Release 12.2(17a)SX” section on page 188.
- ATM Cell Loss Priority (CLP) Setting on FlexWAN module ATM interfaces—See this publication: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>
- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.1 (CVDM-C6500)  
CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.1 (CVDM-SSLSM)  
CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.1 (CVDM-CSM)  
CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

To access all CiscoView Device Manager documentation, go to this URL:

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

## New Features in Release 12.2(17b)SXA2

These sections describe the new features in Release 12.2(17b)SXA2, 22 Apr 2004:

- [New Hardware Features in Release 12.2\(17b\)SXA2, page 179](#)
- [New Software Features in Release 12.2\(17b\)SXA2, page 179](#)

### New Hardware Features in Release 12.2(17b)SXA2

None.

### New Software Features in Release 12.2(17b)SXA2

None.

## New Features in Release 12.2(17b)SXA

These sections describe the new features in Release 12.2(17b)SXA, 31 Dec 2003:

- [New Hardware Features in Release 12.2\(17b\)SXA, page 180](#)
- [New Software Features in Release 12.2\(17b\)SXA, page 180](#)

## New Hardware Features in Release 12.2(17b)SXA

- [WS-SUP720-3BXL](#) Supervisor Engine 720-3BXL—see the “[Supervisor Engines](#)” section on page 11
- [WS-F6K-PFC3BXL](#) Policy Feature Card 3BXL (PFC3BXL)—See the “[Policy Feature Cards](#)” section on page 18
- Optical Service Modules (OSMs; see the “[Optical Services Modules \(OSMs\)](#)” section on page 48)
- WS-X6582-2PA Enhanced FlexWAN module—See the “[FlexWAN and Enhanced FlexWAN Modules](#)” section on page 57
- 2-port Packet-over-SONET OC-3c/STM-1 Port Adapter ([PA-POS-2OC3](#))
- IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#))—See this publication: [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_14459.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14459.htm)
- To avoid reloads with software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases), do not configure the single router mode with stateful switchover ([SRM with SSO](#)) redundancy mode with a WS-SVC-IPSEC-1 module installed. In software releases where caveat CSCed17605 is not resolved, the WS-SVC-IPSEC-1 module supports only RPR and RPR+ redundancy modes.

## New Software Features in Release 12.2(17b)SXA



### Note

- With a PFC3BXL or PFC3B functioning in PFC3A mode, there is no support for features that require the PFC3BXL (see the “[Policy Feature Cards](#)” section on page 18).
- In a system with a PFC3BXL or PFC3B, DFC3A modules are not recognized if inserted while the system is online.
- In a system with a PFC3BXL or PFC3B, after a reboot, any DFC3A modules are active, but the system functions in PFC3A mode and does not support the PCF3BXL or PFC3B mode features.

- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)  
CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)  
CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)  
CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

To access all CiscoView Device Manager documentation, go to this URL:

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

- Cisco IP Phone support enhancements:
  - Support for a high-powered phone to negotiate a low-power mode (dimmed screen) when powered by a pre-standard Cisco PoE daughtercard.
  - Support for a high-powered phone to negotiate a high-power mode (full screen brightness) when powered by a IEEE 802.3af Cisco PoE daughtercard.
- TDR cable diagnostics—See “TDR cable diagnostics” in the “New Software Features in Release 12.2(17a)SX” section on page 188.
- Support for more than 1 Gbps of traffic per EtherChannel on the [WS-X6548-GE-TX](#) and [WS-X6548V-GE-TX](#) switching modules.
- Hardware support for Network Address Translation (NAT) and Port Address Translation (PAT) of UDP traffic (supported only in PFC3BXL or PFC3B mode).
- Support for PFC QoS features on tunnels (supported only in PFC3BXL or PFC3B mode).
- Support for per-VLAN and CoS-based QoS filtering in MAC ACLs (supported only in PFC3BXL or PFC3B mode).
- Population of the NDE Layer 4 source port field with the ICMP type and code values (supported only in PFC3BXL or PFC3B mode).
- Hardware switching for ICMP traffic when Cisco IOS reflexive ACLs are configured (supported only in PFC3BXL or PFC3B mode). (CSCeb20666)
- VLAN translation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vlans.htm>
- Received ToS byte preservation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- Ingress CoS mutation on IEEE 802.1Q tunnel ports—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>

- Single router mode with stateful switchover (SRM with SSO) redundancy mode for unicast traffic—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/srmsso.htm>



#### Note

- Release 12.2(18)SXD and later releases support non-stop forwarding (NSF) with stateful switchover (SSO) on Supervisor Engine 720 and Supervisor Engine 2 (see the “[New Software Features in Release 12.2\(18\)SXD](#)” section on page 165).
- Release 12.2(18)SXD and later releases do not support SRM with SSO.
- Release 12.2(17b)SXA, rebuilds of Release 12.2(17b)SXA, Release 12.2(17d)SXB, and rebuilds of Release 12.2(17d)SXB support SRM with SSO on Supervisor Engine 720.
- SRM with SSO is not supported on Supervisor Engine 2 in any release.
- SRM with SSO redundancy mode does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then recreated and reinstalled in the hardware by the newly active MSFC.
- SRM with SSO redundancy mode does not support MPLS. If you configure MPLS, use the RPR or RPR+ redundancy mode.
- SRM with SSO redundancy mode does not support the IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) in software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases).
- The following modules do not maintain state when an SRM with SSO redundancy mode switchover occurs:
  - IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#))
  - [WS-X6066-SLB-APC](#) (CSM)
  - [WS-SVC-FWM-1-K9](#) firewall services module
  - [WS-SVC-SSL-1](#) secure sockets layer (SSL) services module

- RFC-1483 Bridging on FlexWAN—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm\\_inst/atm.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/atm.htm)
- On WAN ports, VRF-lite with IPv4 forwarding between VRFs interfaces, IPv4 ACLs, and IPv4 HSRP—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mppls.htm>



#### Note

Multi-VRF for CE Routers (VRF Lite) with the PFC3 supports multi-VRF CE functionality with [EIGRP](#) (Release 12.2(18)SXD and later releases), OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported. Also supported on [LAN ports](#) (Release 12.2(18)SXD and later releases).

- Virtual Private LAN Services (VPLS) on the Optical Services Modules (supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mppls.htm>

**Note**

These redundancy modes support MultiProtocol Label Switching (MPLS):

- Route Processor Redundancy (RPR) with:
  - Release 12.2(17b)SXA and rebuilds
  - Release 12.2(17d)SXB and rebuilds
- RPR+ with Release 12.2(18)SXD and rebuilds
- In Release 12.2(18)SXD and rebuilds, MPLS can coexist with NSF with SSO redundancy, but there is no support for stateful MPLS switchover.

- MPLS Basic, including Provider (P) and Provider Edge (PE) functionality (MPLS; supported only in PFC3BXL or PFC3B mode)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm\\_inst/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm)
- MPLS Label Distribution Protocol (LDP; supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mpls.htm>
- MPLS Virtual Private Networks (MPLS VPN; supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsmvpns.htm>
- MPLS VPN Carrier Supporting Carrier (supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs2scsc.htm>  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fscsc lbl.htm>
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution (supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsiasl bl.htm>
- MPLS VPN ID (supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/vpnid2.htm>

- Any Transport over MPLS (AToM) Features:
  - Not supported with PFC3A
  - Supported on WAN ports
  - Ethernet over MPLS (EoMPLS)
  - Frame Relay over MPLS (FRoMPLS)
  - ATM Single Cell Relay over MPLS-VC Mode (CRoMPLS)
  - ATM AAL5 over MPLS (AAL5oMPLS)

See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/optical/122sx/mpls.htm>

- MPLS VPN—OSPF and Sham-Link Support (supported only in PFC3BXL or PFC3B mode)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/shamlink.htm>
- Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS (supported only in PFC3BXL or PFC3B mode)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6\\_c/sa\\_mpls6.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mpls6.htm)
- Distributed Multilink Frame Relay (FRF.16)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/dmfr.htm>
- Automatic Protection Switching (APS) 1+1—See this publication:  
[http://www.cisco.com/warp/public/127/aps\\_support\\_16140.pdf](http://www.cisco.com/warp/public/127/aps_support_16140.pdf)
- ATM Virtual Circuit (VC) Bundling—See these publications:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/fqcprt7/qcfipao v.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt7/qcfipao v.htm)  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsmu26s.htm>
- IPv6 Support on WAN Interfaces—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6\\_sol/ipv6dswp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.htm)
- OSPF Shortest Path First Throttling—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsspf trl.htm>
- Gateway Load Balancing Protocol—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs\\_gl bp2.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_gl bp2.htm)

## New Features in Release 12.2(17a)SX4

These sections describe the new features in Release 12.2(17a)SX4, 23 Apr 2004:

- [New Hardware Features in Release 12.2\(17a\)SX4, page 185](#)
- [New Software Features in Release 12.2\(17a\)SX4, page 185](#)



## New Hardware Features in Release 12.2(17a)SX4

None.

## New Software Features in Release 12.2(17a)SX4

None.

## New Features in Release 12.2(17a)SX3

These sections describe the new features in Release 12.2(17a)SX3, 05 Mar 2004:

- [New Hardware Features in Release 12.2\(17a\)SX3, page 185](#)
- [New Software Features in Release 12.2\(17a\)SX3, page 185](#)

## New Hardware Features in Release 12.2(17a)SX3

None.

## New Software Features in Release 12.2(17a)SX3

None.

## New Features in Release 12.2(17a)SX2

These sections describe the new features in Release 12.2(17a)SX2, 29 Jan 2004:

- [New Hardware Features in Release 12.2\(17a\)SX2, page 185](#)
- [New Software Features in Release 12.2\(17a\)SX2, page 185](#)

## New Hardware Features in Release 12.2(17a)SX2

None.

## New Software Features in Release 12.2(17a)SX2

None.

## New Features in Release 12.2(17a)SX1

These sections describe the new features in Release 12.2(17a)SX1, 30 Oct 2003:

- [New Hardware Features in Release 12.2\(17a\)SX1, page 186](#)
- [New Software Features in Release 12.2\(17a\)SX1, page 186](#)

## New Hardware Features in Release 12.2(17a)SX1

- 10GBASE-SR Serial 850-nm short-reach XENPAK (XENPAK-10GB-SR; see the “10-Gigabit Ethernet Switching Modules” section on page 30)
- 10GBASE-LX4 Serial 1310-nm multimode fiber (MMF) XENPAK (XENPAK-10GB-LX4; see the “10-Gigabit Ethernet Switching Modules” section on page 30)

## New Software Features in Release 12.2(17a)SX1

- Distributed network-based application recognition (dNBAR) on FlexWAN module interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm>
- Hardware support for these basic IPv6 functions:
  - IPv6 standard access control lists (ACLs)
  - IPv6 extended ACLs
  - Reflexive ACLs
  - Manually configured v6 tunnels
  - ISATAP (ISATAP with 6-to-4 prefix is not supported in hardware)
  - Automatically configured IPv4 compatible tunnels
  - 6-to-4 tunnel
  - IPv6 over IPV4 IP in IP tunnels
- Software support for these basic IPv6 functions:
  - IPv6 addressing architecture
  - ICMPv6
  - Neighbor Discovery
  - Static ND cache entry
  - IPv6 stateless autoconfiguration
  - ICMPv6 Redirect
  - MTU path Discovery for IPv6
  - IPv6 ICMP rate limiting
  - IPv6 over IPV4 GRE tunnels
- Software support for IPv6 routing:
  - Static routes within IPv6
  - RIPng
  - MP-BGP4
  - OSPFv3
  - ISIS
  - Configuring an IPv6 Multiprotocol BGP Peer using a link local address
  - IPv6 MP-BGP distance command

- Switching support for IPv6:
  - Process
  - CEFv6
  - Distributed CEFv6
- Software support for these IPv6 applications:
  - Ping
  - Traceroute
  - Telnet
  - TFTP (client only)
  - FTP
  - SSH over IPv6
  - DNS
  - HTTP server

For configuration information, refer to this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6\\_vgf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm)

For command reference information, refer to this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_r/index.htm)

## New Features in Release 12.2(17a)SX

These sections describe the new features in Release 12.2(17a)SX, 06 Oct 2003:

- [New Hardware Features in Release 12.2\(17a\)SX, page 187](#)
- [New Software Features in Release 12.2\(17a\)SX, page 188](#)

## New Hardware Features in Release 12.2(17a)SX

- 48-port 10/100/1000 Ethernet RJ-45 switching module ([WS-X6748-GE-TX](#))
- 24-port Gigabit Ethernet SFP switching module ([WS-X6724-SFP](#))
- 4-port 10-Gigabit Ethernet XENPAK switching module ([WS-X6704-10GE](#))
- XENPAK-10GB-LR 10GBASE-LR Serial 1310-nm long-reach XENPAK
- XENPAK-10GB-ER 10GBASE-ER Serial 1550-nm extended-reach XENPAK
- 1000BASE-DWDM GBIC ([DWDM-GBIC](#))
- 1000BASE-CWDM SFP ([CWDM-SFP](#))
- 1000BASE-LX/LH SFP ([GLC-LH-SM](#))
- 1000BASE-T SFP ([GLC-T](#))

- 48-port 10/100/1000 Mbps switching module ([WS-X6548-GE-TX](#) and [WS-X6548V-GE-TX](#); [WS-X6548V-GE-TX](#) has [WS-F6K-VPWR-GE](#)).




---

**Note** The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support the following:

- With Release 12.2(17a)SX and Release 12.2(17a)SX1, more than 1 Gbps of traffic per EtherChannel
- [WS-F6K-DFC3A](#)
- ISL trunking
- Jumbo frames
- 802.1Q tunneling
- Traffic storm control

---

- 48-port 10/100/1000 Mbps switching module ([WS-X6148-GE-TX](#) and [WS-X6148V-GE-TX](#); [WS-X6148V-GE-TX](#) has [WS-F6K-VPWR-GE](#)).




---

**Note** The WS-X6148-GE-TX and WS-X6148V-GE-TX do not support the following:

- More than 1 Gbps of traffic per EtherChannel
- [WS-F6K-DFC3A](#)
- ISL trunking
- Jumbo frames
- 802.1Q tunneling
- Traffic storm control

---

- PWR-1400-AC 1,400 W AC power supply

## New Software Features in Release 12.2(17a)SX

- TDR cable diagnostics—TDR is supported on these switching modules:
  - In Release 12.2(17a)SX and later releases:
    - [WS-X6148-GE-TX](#)
    - [WS-X6148V-GE-TX](#)
    - [WS-X6148-GE-45AF](#)
    - [WS-X6548-GE-TX](#)
    - [WS-X6548V-GE-TX](#)
    - [WS-X6548-GE-45AF](#)
  - In Release 12.2(18)SXE and later releases, [WS-X6748-GE-TX](#)
  - In Release 12.2(18)SXF and later releases:
    - [WS-X6148A-GE-TX](#)
    - [WS-X6148A-GE-45AF](#)
    - [WS-X6148A-RJ-45](#)
    - [WS-X6148A-45AF](#)




---

**Note** TDR can test cables up to a maximum length of 115 meters.

---

See these publications:

- The “Checking the Cable Status Using the TDR” section of the “Configuring Interfaces” chapter at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/intrface.htm>

- The **test cable-diagnostics** command in the command reference at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>

- Layer 2 protocol tunneling global threshold—See the **l2protocol-tunnel global drop-threshold** command in the command reference at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>

- Custom IEEE 802.1Q Ethertypes:

- Supported on these modules:

- Supervisor engines
- WS-X6516-GE-TX
- WS-X6748-GE-TX
- WS-X6748-SFP
- WS-X6724-SFP
- WS-X6704-10GE
- WS-X6816-GBIC
- WS-X6516A-GBIC
- WS-X6516-GBIC



**Note**

The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType field value to all ports supported by each port ASIC (1 through 8 and 9 through 16).

- See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/layer2.htm>

- PIM Snooping—See this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snooppim.htm>

- Secure Shell (SSH) Version 2 server support in k9 images—By default, the k9 images support both SSHv1 connections and SSHv2 connections. To restrict connections to either SSHv1 or SSHv2, enter the **ip ssh mode [v1 | v2]** global configuration mode command. Except for the **v1** and **v2** keywords for the **ip ssh mode** command, you configure SSHv2 in the same way as SSHv1. See this publication for more information:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/sshv1.htm>

For information about SSHv1 client support, refer to the following publication:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sshv1c.htm>

- Support for these CiscoView Device Managers:

- CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)

CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.

- CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)

CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.

- CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)  
CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

To access all CiscoView Device Manager documentation, go to this URL:

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

## New Features in Release 12.2(14)SX1

These sections describe the new features in Release 12.2(14)SX1, 28 May 2003:

- [New Hardware Features in Release 12.2\(14\)SX1, page 190](#)
- [New Software Features in Release 12.2\(14\)SX1, page 191](#)

## New Hardware Features in Release 12.2(14)SX1

- Content Switching Module (CSM) support with Supervisor Engine 720:
  - [WS-X6066-SLB-APC](#)
  - [Also supported with Supervisor Engine 2](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/csm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/index.htm)




---

**Note** Support with Supervisor Engine 720 requires CSM module software release 3.1(4) or later.

---

- Intrusion Detection System Module 2 support with Supervisor Engine 720:
  - [WS-SVC-IDSM2-K9](#)
  - [Also supported with Supervisor Engine 32](#)
  - [Also supported with Supervisor Engine 2](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029\\_02.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/4029_02.htm)
- Firewall Services module support with Supervisor Engine 720:
  - [WS-SVC-FWM-1-K9](#)
  - [Also supported with Supervisor Engine 32](#)
  - [Also supported with Supervisor Engine 2](#)
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_icn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm)

- Network Analysis Module support with Supervisor Engine 720:
  - [WS-SVC-NAM-1](#) and [WS-SVC-NAM-2](#)
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78\\_15353.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_15353.htm)
- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 720:
  - [WS-SVC-SSL-1](#)
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_5277.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_5277.htm)

## New Software Features in Release 12.2(14)SX1

- Half-Bridging on FlexWAN ATM interfaces (CSCin27157)
- RFC 1483 hardware bridging on FlexWAN (CSCea70308)
- [VACL capture](#) to support the [WS-SVC-IDS2-K9](#) Intrusion Detection System Module 2 and the [WS-SVC-NAM-2](#) and [WS-SVC-NAM-1](#) network analysis modules.




---

**Note** Caveat CSCec75140 prevents use of VACL capture on WAN ports in releases earlier than Release 12.2(17b)SXA. Caveat CSCec75140 is resolved in Release 12.2(17b)SXA.

---

- Support for embedded CiscoView—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/intro.htm>
- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)  
CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)  
CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)  
CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

To access all CiscoView Device Manager documentation, go to this URL:

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

## New Features in Release 12.2(14)SX

These sections describe the new features in Release 12.2(14)SX, 14 Apr 2003:

- [New Hardware Features in Release 12.2\(14\)SX, page 192](#)
- [New Software Features in Release 12.2\(14\)SX, page 192](#)

### New Hardware Features in Release 12.2(14)SX

- [WS-SUP720](#) Supervisor Engine 720—See the “Supervisor Engines” section on page 11
- Communication Media Module ([WS-SVC-CMM](#))—See these publications:
  - Release 12.2(13)ZP3:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_4847.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_4847.htm)
  - Release 12.2(2)YK1:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_3137.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3137.htm)
  - Release 12.2(13)ZC:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol\\_3732.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3732.htm)
- 1000BASE-SX SFP ([GLC-SX-MM](#))
- Distributed Forwarding Card 3A (DFC3A; [WS-F6K-DFC3A](#))—See the “Distributed and Centralized Forwarding Cards” section on page 22
- 16-port Gigabit Ethernet switching module ([WS-X6516A-GBIC](#))
- FlexWAN port adapters:
  - 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced ([PA-A6-OC3MM](#))
  - 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced ([PA-A6-OC3SMI](#))
  - 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced ([PA-A6-OC3SML](#))
  - 1-port ATM DS3 port adapter, enhanced ([PA-A6-T3](#))
  - 1-port ATM E3 port adapter, enhanced ([PA-A6-E3](#))
- 4000 W DC-power supply ([PWR-4000-DC](#))

### New Software Features in Release 12.2(14)SX

- Generic Online Diagnostics (GOLD)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm>
- Virtual Router Redundancy Protocol (VRRP)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st\\_vrrpx.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st_vrrpx.htm)
- Bidirectional Protocol Independent Multicast (PIM) in hardware—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm>
- Interior Border Gateway Protocol (iBGP) Multipath Load Sharing—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsbgpls.htm>





**Note** For MPLS support, see [BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN](#).

- Internet Group Management Protocol Version 3 (IGMPv3) snooping—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snooigmp.htm>
- User-based microflow policing—See the procedures in this publication for information about configuring microflow policing based on either source or destination addresses:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- Egress policing for LAN ports configured as Layer 3 interfaces and for VLAN interfaces—See the procedures in this publication for information about configuring the **service-policy output** command:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- Egress DSCP mutation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- DSCP transparency (also called “Preserving the Received ToS Byte”)—See the procedures in this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm>
- Hardware-assisted NetFlow Aggregation—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm>
- Hardware-assisted Multiple-path Unicast Reverse Path Forwarding (Unicast RPF)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/secure.htm>
- Hardware-assisted Network Address Translation (NAT) and Port Address Translation (PAT) for IPv4 unicast and multicast traffic—Note the following information about hardware-assisted NAT:
  - The PFC3A does not support NAT or PAT for UDP traffic.



**Note** PFC3B and PFC3BXL modes support NAT and PAT for UDP traffic.

- The PFC3 does not support NAT or PAT for multicast traffic.
- The PFC3 does not support NAT or PAT configured with a route-map that specifies length.
- The PFC3 does not support NAT or PAT configured with a route-map that specifies static translations.
- When you configure NAT or PAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)

To configure NAT or PAT, refer to the Cisco IOS IP Configuration Guide, Release 12.2, “IP Addressing and Services,” “Configuring IP Addressing,” “Configuring Network Address Translation,” at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcp1/1cfipadr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcp1/1cfipadr.htm)

For information about configuring NAT or PAT with route maps, refer to this publication:

[http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ionetn/prodlit/1195\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ionetn/prodlit/1195_pp.htm)

To prevent a significant volume of NAT or PAT traffic from being sent to the MSFC, due to either a DoS attack or a misconfiguration, enter the **mls rate-limit unicast acl {ingress | egress}** command described in this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/m1.htm>

(CSCea23296)

- Hardware-assisted IP-in-IP tunneling and generic routing encapsulation (GRE) tunneling—The PFC3 and DFC3s support the following tunnel commands:
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

Other supported types of tunneling run in software on the MSFC3. The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

The **tunnel ttl** command (default 255) sets the TTL of encapsulated packets.

The **tunnel tos** command, if present, sets the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is not enabled, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is enabled, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

To configure GRE Tunneling and IP in IP Tunneling, refer to these publications:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter\\_c/icflogin.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflogin.htm)

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter\\_r/irfshoip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/irfshoip.htm)

To configure the **tunnel tos** and **tunnel ttl** commands, refer to this publication:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s\\_tos.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s_tos.htm)

Note the following information about tunnels:

- Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. Use secondary addresses on loopback interfaces or create multiple loopback interfaces. (CSCdy72539)
- Each tunnel interface uses one internal VLAN.
- Each tunnel interface uses one additional router MAC address entry per router MAC address.
- The PFC3A does not support any PFC QoS features on tunnel interfaces.
- The PFC3B and PFC3BXL support PFC QoS features on tunnel interfaces.
- In releases earlier than Release 12.2(18)SXE, the PFC3 does not support GRE tunnel encapsulation and de-encapsulation of multicast traffic.
- The MSFC supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT and PAT (for inside to outside translation), TCP intercept, context-based access control (CBAC), and encryption.

- Hardware-assisted Cisco IOS Firewall Features—refer to this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/fw.htm>

**Note**

For a complete listing of hardware-assisted features, refer to this publication:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/intro.htm>

- FlexWAN features:
  - Support for 4000 ATM VCs per port adapter on the following ATM port adapters:  
[PA-A3-OC3MM](#)  
[PA-A3-OC3SMI](#)  
[PA-A3-OC3SML](#)  
[PA-A3-T3](#)  
[PA-A3-E3](#)  
[PA-A6-OC3MM](#)  
[PA-A6-OC3SMI](#)  
[PA-A6-OC3SML](#)  
[PA-A6-T3](#)  
[PA-A6-E3](#)
  - Low Latency Queueing (LLQ) and Class-based Weighted Fair Queueing (CBWFQ) on MLPPP links—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm)
  - Voice over Frame Relay (VoFR) FRF.11 and FRF.12—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvfax\\_c/vvfvofr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvfax_c/vvfvofr.htm)

**Note**

Because the Catalyst 6500 series switches and the Cisco 7600 series routers do not support voice modules, they can act only as a VoFR tandem switch when FRF.11 or FRF.12 is configured on the FlexWAN.

- Link Fragmentation and Interleaving (LFI) for Frame Relay and ATM Virtual Circuits—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdli2.htm>
- RFC 1889 Compressed Real-Time Protocol (cRTP)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/fqcprt6/qcfcrtp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt6/qcfcrtp.htm)

**Note**

cRTP is not supported on MLPPP bundled links.

## Software Features from Earlier Releases

- Hardware-assisted TCP intercept—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/secure.htm>
- Hardware-assisted policy-based routing (PBR) for route-map sequences that use the **match ip address**, **set ip next-hop**, and **set ip default next-hop** PBR keywords.  
 To configure PBR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, “Classification,” “Configuring Policy-Based Routing,” at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/fqcpbr1/qcfpbr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcpbr1/qcfpbr.htm)  
 When configuring PBR, follow these guidelines and restrictions:
  - The PFC provides hardware support for PBR configured on a tunnel interface.
  - The PFC does not provides hardware support for PBR configured with the **set ip next-hop** keywords if the next hop is a tunnel interface.
  - If the MSFC3 address falls within the range of a PBR ACL, traffic addressed to the MSFC3 is policy routed in hardware instead of being forwarded to the MSFC3. To prevent policy routing of traffic addressed to the MSFC3, configure PBR ACLs to deny traffic addressed to the MSFC3.
  - Any options in Cisco IOS ACLs that provide filtering in a PBR route-map that would cause flows to be sent to the MSFC3 to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in PBR route-maps.
  - PBR traffic through switching module ports where PBR is configured is routed in software if the switching module resets. (CSCee92191)
- Hardware support for directed broadcasts with the **mls ip directed-broadcast** command—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/m1.htm>
- Cisco IP Phone Support—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/voip.htm>
- IEEE 802.1X Port-Based Authentication—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dot1x.htm>
- Port Security—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/port\\_sec.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/port_sec.htm)
- Remote SPAN—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm>
- MAC address-based traffic blocking—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/secure.htm>
- SNMP ifindex persistence—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/ifindex.htm>
- Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/spantree.htm>
- NDE—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm>

- Route Processor Redundancy Plus (RPR+) redundancy—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/redund.htm>
- 4096 Layer 2 VLANs—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vlans.htm>



**Note** We recommend that you configure a combined total of no more than 2,000 Layer 3 VLAN interfaces and Layer 3 ports.

- IEEE 802.1Q tunneling—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dot1qtnl.htm>
- IEEE 802.1Q protocol tunneling—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dot1qtnl.htm>
- IEEE 802.1s, multiple spanning tree (MST)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/spantree.htm>
- IEEE 802.1w, rapid reconfiguration of spanning tree—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/spantree.htm>
- IEEE 802.3ad, link aggregation control protocol (LACP)—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/channel.htm>
- PortFast BPDU filtering—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/stp\\_enha.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/stp_enha.htm)
- Traffic storm control—Prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.
- Jumbo frames on all Ethernet ports except ports on the [WS-X6548-GE-TX](#), [WS-X6548V-GE-TX](#), [WS-X6148-GE-TX](#), and [WS-X6148V-GE-TX](#) switching modules.



**Caution**

The following switching modules support a maximum ingress frame size of 8092 bytes:

- [WS-X6516-GE-TX](#) when operating at 100 Mbps
- [WS-X6148-RJ-45](#), [WS-X6148-RJ-45V](#) and WS-X6148-RJ21, WS-X6148-RJ21V
- [WS-X6248-RJ-45](#) and [WS-X6248-TEL](#)
- WS-X6248A-RJ-45 and [WS-X6248A-TEL](#)
- [WS-X6348-RJ-45](#), WS-X6348-RJ45V and WS-X6348-RJ21V

When jumbo frame support is configured, these modules drop ingress frames larger than 8092 bytes.

- Private VLANs—“Configuring Private VLANs”
- QoS Data Export—“Configuring QoS”
- VLAN Access Control Lists (VACLs)—“Configuring VLAN ACLs (VACLs)”
- VACL Deny Logging—“Configuring Network Security”

- Router-Port Group Management Protocol (RGMP)—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/rgmp.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/rgmp.htm>
- Spanning tree PortFast, UplinkFast, and BackboneFast, and Root Guard Feature—See either of these publications:
  - For Catalyst 6500 series switches:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/stp\\_enha.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/stp_enha.htm)
  - For Cisco 7600 series routers:  
[http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/stp\\_enha.htm](http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/stp_enha.htm)
- UniDirectional Link Detection—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/udld.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/udld.htm>
- Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP), including support on Gigabit Ethernet ports for jumbo frames—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/layer2.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/layer2.htm>
- VLANs—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vlans.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/vlans.htm>
- VLAN Trunk Protocol (VTP) and VTP domains—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vtp.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/vtp.htm>
- EtherChannel—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/channel.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/channel.htm>

- Spanning Tree Protocol—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/spantree.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/spantree.htm>
- IGMP snooping and IGMP snooping querier—See either of these publications:
  - For Catalyst 6500 series switches:  
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/snooigmp.htm>
  - For Cisco 7600 series routers:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/snooigmp.htm>
- Mobile IP—See the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, “Configuring Mobile IP,” at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt1/1cdmobip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdmobip.htm)
- Local proxy ARP—See the *Catalyst 6500 Series Cisco IOS Command Reference* publication.



**Note** To use the local proxy ARP feature, you must enable the IP proxy ARP feature. The IP proxy ARP feature is enabled by default. See the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, “IP Addressing and Services,” “Configuring IP Addressing,” “Enabling Proxy ARP,” at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt1/1cdipadr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdipadr.htm)

- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3/1cfssm.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfssm.htm)
- Data-link switching plus (DLSw+)—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm\\_c/bcfpart2/bcfdlsw.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart2/bcfdlsw.htm)
- Standard Domain Naming System (DNS) support—See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt1/1cfipadr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt1/1cfipadr.htm)
- Dynamic Host Configuration Protocol (DHCP)— See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt1/1cfdhcp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt1/1cfdhcp.htm)
- Boot Protocol (BOOTP) relay— See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun\\_c/fcfrpt3/fc012.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfrpt3/fc012.htm)
- Multiple-Hot Standby Routing Protocol— See this publication:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt1/1cfip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt1/1cfip.htm)
- Cisco Discovery Protocol (CDP); (refer to the “Configuring CDP” chapter)
- NetFlow Data Export (refer to the “Configuring NDE” chapter)
- Access control using several supported authentication methods (refer to the “Configuring the Supervisor Engine” chapter)
- Switched Port Analyzer (SPAN); (refer to the “Configuring SPAN” chapter)

- Redundant supervisor engines (refer to the “Configuring the Supervisor Engine” chapter)
- Quality of Service (QoS); (refer to the “Configuring QoS” chapter)
- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>




---

**Note** cRTP is not supported on dMLPPP bundled links.

---

- Inverse Multiplexing over ATM (IMA) on FlexWAN module interfaces—See this publication:  
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/features.htm>

## Unsupported Features and Commands

- Hardware—See the “[Unsupported Hardware](#)” section on page 79.
- These QoS interface commands are not supported on SPA interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
  - **fair-queue**
  - **random-detect**
  - **rate-limit**
  - **tx-ring-limit**
  - **max-reserved-bandwidth**
- In Release 12.2(18)SXE and later releases, these QoS interface commands are no longer supported on FlexWAN and OSM interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
- In Release 12.2(18)SXE and later releases, these QoS interface commands are no longer supported on OSM interfaces, but they are still supported on FlexWAN interfaces:
  - **fair-queue**
  - **random-detect**
  - **rate-limit**
  - **tx-ring-limit**
  - **max-reserved-bandwidth**



- Random Sampled NetFlow (**flow-sampler** commands)
- These features are not supported in Release 12.2(18)SXD and later releases:
  - Apollo Domain
  - AppleTalk EIGRP
  - Banyan Vines
  - Exterior Gateway Protocol (EGP)
  - HP Probe
  - IEEE 802.10 VLANs
  - IGRP
  - LAN Extension
  - Netware Asynchronous Services Interface (NASI)
  - Next Hop Resolution Protocol (NHRP) for IPX
  - Novell Link-State Protocol (NLSP)
  - Simple Multicast Routing Protocol (SMRP) for Appletalk
  - Xerox Network Systems (XNS)
  - Xremote
- Generic routing encapsulation (GRE) tunnel IP source and destination VRF membership (the **tunnel vrf** command). (CSCee39138)
- Warm Reload (CSCef06158)
- ARP Optimization (CSCef30539)
- Exterior Border Gateway Protocol (eBGP) multihop over CSC-PE interfaces (CSCea83165)
- Ability to accept ingress traffic on SPAN destination ports (Cisco IOS software equivalent of **set span ... inpkts enable**).
- Automatic QoS
- With PFC3:
  - Unknown unicast flood protection
  - Network-based application recognition (NBAR) for LAN interfaces
- Commands to globally disable EtherChannel or trunking
- **write tech-support** command
- Cisco IOS software equivalent of the **set port host** command
- Disable port startup option
- Clear counters per port or clear QoS statistics
- System warning and error counter enhancements implemented in Catalyst software release 6.1(1)
- Option for no VTP support
- Command to display the port MAC address
- Port security timer enhancement
- System warnings on port counters
- VLAN Management Policy Server (VMPS) client or server

- Cisco IOS MAC-layer access control lists (ACLs)
- Accelerated server load balancing (ASLB)
- Hot Standby Router Protocol (HSRP) between redundant supervisor engines (the redundant supervisor engine and MSFC are in standby mode—HSRP to external routers is supported)
- Multi-Instance Spanning Tree Protocol (MISTP); IEEE 802.1s MST is supported
- Common Open Policy Server (COPS)
- Except to support tunnels, Resource ReSerVation Protocol (RSVP)
- GARP VLAN Registration Protocol (GVRP)
- GARP Multicast Registration Protocol (GMRP)
- Commands present in the CLI, but not supported:
  - ipv6 cef accounting
  - ip cef accounting
  - module provision

## Limitations and Restrictions

These sections list limitations and restrictions for the Cisco IOS for the Catalyst 6500 series switches and Cisco 7600 series routers:

- [Restrictions Removed by the PFC3, page 202](#)
- [General Limitations and Restrictions, page 203](#)
- [FlexWAN Limitations and Restrictions, page 211](#)
- [OSM Limitations and Restrictions, page 211](#)
- [Service Module Limitations and Restrictions, page 212](#)

## Restrictions Removed by the PFC3

The PFC3 removes these restrictions that were present with other policy feature cards:

- You can configure features to use up to 3 different flow masks.
- You can configure more than 1 Gateway Load Balancing Protocol (GLBP) group.
- You can configure up to 255 unique HSRP group numbers.
- You can configure a separate MAC address on each interface.
- You can configure Unicast RPF check without reducing the number of available CEF entries.
- You can configure VLAN-based QoS with DFC3s installed.
- You can configure port-based and VLAN-based QoS on a per-port basis on the [WS-X6548-RJ-45](#) and [WS-X6548-RJ-21](#) switching modules.
- You can configure QoS policy maps attached to an EtherChannel formed from interfaces on different DFC-equipped switching modules.

## General Limitations and Restrictions

This section describes general limitations and restrictions:

- When a redundant supervisor engine is in standby mode, the Ethernet ports on the redundant supervisor engine are always active.



**Note** With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on the redundant supervisor engine, which ensures that all modules are operating in dCEF mode. (CSCec05612)

- A supervisor engine that has one ROMMON version might boot at a different rate from a supervisor engine that has another ROMMON version. To ensure that redundant supervisor engines boot at the same rate, install the same ROMMON version on both supervisor engines. (CSCef29567)
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannel (maximum of eight interfaces) with no requirement that the ports be contiguous.
- All Ethernet ports on all modules support 802.1Q VLAN trunking.
- These modules do not support Inter-Switch Link (ISL) VLAN trunking:
  - [WS-X6502-10GE](#)
  - [WS-X6548-GE-TX](#)
  - [WS-X6148-GE-TX](#)

The ports on all other modules support ISL VLAN trunking.

- When you add a member port that does not support ISL trunking to an EtherChannel, Cisco IOS software automatically adds a **switchport trunk encapsulation dot1q** command to the port-channel interface to prevent configuration of the EtherChannel as an ISL trunk. The **switchport trunk encapsulation dot1q** command is inactive when the EtherChannel is not a trunk.
- The link state messages (“LINK-3-UPDOWN” and “LINEPROTO-5-UPDOWN”) are disabled by default. Release 12.2(17d)SXB and later releases have enhanced support for interface link status messages. See the following publication for more information:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/i1.htm>

(CSCeb06765)

- Do not configure [WS-X6708-10GE](#) switching module ports as VACL capture ports. (CSCsb59015)
- RSVP Traffic Engineering (TE) tunnels might stop forwarding traffic in hardware if Label Distribution Protocol (LDP) is not enabled globally. This problem occurs when a path change requires that ternary content addressable memory (TCAM) table entries be updated for all the prefixes routed over the TE tunnel. The TCAM entries are not updated correctly.

**Workaround:** If you enable LDP globally, a TE tunnel rewrite is created for each prefix. The hardware programming code receives an update for each prefix and will be able to program the TCAM entries correctly. (CSCee77417)

- The **show interface** command displays the giants field, which indicates the number of packets that are larger than 1518 octets. For Layer 2 trunk ports configured with an MTU size that supports jumbo frames on WS-X6704-10GE, WS-X6748-SFP, WS-X6724-SFP, and WS-X6748-GE-TX switching modules, the giants field always indicates zero. This is a display issue and does not impact the actual handling of jumbo frames on these ports.

**Workaround:** None. (CSCek23592)

- With the [BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN](#) feature configured, do not attach output service policies to VRF interfaces. (CSCsb25509)
- A distributed EtherChannel (DEC) is an EtherChannel with ports on more than one DFC-equipped module or, on a DFC-equipped dual-fabric connection module, with ports that use different fabric connections.
- In truncated mode, the Supervisor Engine 720 does not support Layer 2 denial-of-service (DoS) protection rate limiters. (CSCeb36155)
- To reduce CPU utilization during ACL configuration changes, use named ACLs instead of numbered ACLs whenever possible, because the ACL merge algorithm runs each time you change an ACE in a numbered ACL. With named ACLs, the ACL merge algorithm runs only when you exit the named ACL configuration mode.
- With bidirectional PIM configured, you cannot configure Bootstrap Router (BSR) rendezvous point (RP) candidates.

**Workaround:** Use AutoRP or static RP. (CSCeg29898)

- In rare situations, if you do an online insertion and removal (OIR) of a FlexWAN module, a [WS-X6516-GBIC](#) switching module that does not have a DFC installed might reset. (CSCec29255)
- For packet sizes beginning with 84 bytes, and at each 8-byte increment (92 bytes, 100 bytes, etc.), some packet loss occurs with line-rate traffic ingressing and egressing on a [WS-X6704-10GE](#) with a [WS-F6700-DFC3A](#). The loss for 84-byte packets is approximately 0.01 percent and increases up to 0.04 percent for larger traffic. (CSCee39455, CSCee94670)
- In releases where caveat CSCef78235 is resolved, with any Supervisor Engine 720 hardware revision, local SPAN and RSPAN source ports do not copy VACL-redirected traffic.

In releases where caveat CSCef78235 is not resolved:

- With [WS-SUP720](#), hardware revision 3.2 or higher, local SPAN source ports do not copy VACL-redirected traffic.
- With [WS-SUP720](#) hardware revisions lower than 3.2, local SPAN source ports copy VACL-redirected traffic.
- With any Supervisor Engine 720 hardware revision, RSPAN source ports copy VACL-redirected traffic.

Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision. For example:

```
Router# show module version | include WS-SUP720-BASE
7      2      WS-SUP720-BASE      SAD075301SZ Hw :3.2
```

- Unbalanced load-sharing between the two banks of the Layer 2 forwarding engine MAC table for non-statistical distributions of data-frame MAC Layer addresses causes a fractional performance degradation. (CSCec02266)
- With a PFC3, EoMPLS ports cannot be SPAN sources. (CSCed51245)
- IPsec in software on the MSFC is supported only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.

- With a PFC2 or a PFC3, you can either set DSCP in a packet or apply an MPLS tag to the packet, but cannot do both. You cannot set DSCP in a packet and then apply an MPLS tag to that packet. (CSCef19599)
- On a Supervisor Engine 2 with several hundred Layer 3 VLAN interfaces configured and with Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) configured, after a change in the Layer 2 topology (for example, a link coming up), there might be unacceptably high CPU utilization that prevents Rapid-PVST from sending BPDUs on time in all VLANs. (CSCed52310)
- There is no hardware support for fragmented multicast VPN traffic. (CSCef08631)
- The PFC2 supports a maximum of 1 Gateway Load Balancing Protocol (GLBP) group.
- The PFC2 supports a maximum of 16 unique Hot Standby Routing Protocol (HSRP) group numbers.
  - You can use the same HSRP group numbers in different VLANs (for example, use 1 as the first group number in each VLAN, use 2 for the second, etc.).
  - If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP group number.
- When a port becomes a member port of a Layer 2 EtherChannel, any service policy on that member port is displayed by the **show mls qos ip** command as being on the port-channel interface, but the service policy is not applied to the EtherChannel. (CSCec34784)
- In these releases:
  - 12.2(17a)SX and any later 12.2(17a)SX-based releases
  - 12.2(17b)SXA and any later 12.2(17b)SXA-based releases
  - 12.2(17d)SXB and any later 12.2(17d)SXB-based releases

When you enter the **crypto key generate rsa modulus** *modulus\_value* command the *modulus\_value* parameter is ignored and a prompt appears for entry of a modulus value. Pressing Enter generates a key with the default value (512).

**Workaround:** Reenter the modulus value at the prompt instead of accepting the default. (CSCed60483)

- With Release 12.2(17d)SXB6, to avoid a reload, enter the **no ip multicast vrf vrf\_name cache-headers** command before you enter the **no ip vrf vrf\_name** command for the same VRF. (CSCeg43304)
- The time taken to execute the **show spanning-tree** interface command is proportional to the number of VLANs configured. With many VLANs configured, there might be a noticeable delay in the output of the command while Cisco IOS scans the VLANs for spanning tree ports. (CSCec65860)
- If you set the MTU size on an LACP port-channel interface, the configured MTU size propagates to the member ports. If you change the MTU size on some of the member ports of an LACP EtherChannel, the change does not propagate to the port-channel interface. The ports configured with a different MTU size than the port-channel interface form a secondary LACP EtherChannel. The port-channel interface of a secondary LACP EtherChannel is not configurable. (CSCed18149)
- See this publication for information about the supported IPv6 address formats:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6\\_c/sa\\_bconn.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_bconn.htm)  
 (CSCed30692)
- The PFC3A and PFC3BXL incorrectly apply egress IP ACLs to MPLS-tagged traffic. (CSCed29392, CSCed16560)
- With an ingress policer, the PFC3BXL overpolicies tunnel-decapsulated packets because of the tunnel-packet length. (CSCec71389)

- In PFC3BXL mode, ToS rewrites for bridged multicast packets do not work when TTL-failure rate limiting is configured. (CSCed07399)
- With an EIGRP default network configured, if you remove the referencing network, the default route programming might remain.

**Workaround:** Use 0.0.0.0/0 as the default route or avoid entering the **ip default-network** command. Clear the EIGRP neighbors to recover. (CSCea70203)

- When a Supervisor Engine 720 bridges traffic between HSRP routers or Virtual Router Redundancy Protocol (VRRP) routers or GLBP routers that are providing redundancy to each other through switchports that are on different DFC-equipped modules or through switchports on both DFC-equipped modules and on non-DFC-equipped modules, HSRP or VRRP or GLBP switchover times for the routers might be proportional to the Layer 2 aging interval configured for the bridging VLAN on the Supervisor Engine 720.

**Workarounds:**

- Connect the HSRP or VRRP or GLBP routers to the Supervisor Engine 720 through switchports on the same DFC-equipped module.
- Connect the HSRP or VRRP or GLBP routers to the Supervisor Engine 720 through switchports on non-DFC-equipped modules.
- Reduce the Layer 2 aging time on the Supervisor Engine 720 VLAN to which the HSRP or VRRP or GLBP routers are connected.
- Configure HSRP or VRRP or GLBP routers to use the BIA (Burned-In MAC Address) instead of virtual MAC.

(CSCec27709)

- With a PFC3A, if there is an egress QoS policy on an interface, any ingress traffic on that interface that is dropped because of an RPF check failure or a FIB miss incorrectly increments the output policy QoS counters of that interface. (CSCeb01860)
- RPR and RPR+ do not synchronize configuration done through SNMP to the redundant supervisor engine. (CSCeb07866, CSCea72373)
- The PFC3A does not provide hardware-assisted NAT or PAT for hardware-switched traffic on interfaces where you have configured bidirectional PIM. (CSCea32737)
- If the MSFC3 address falls within the range of a PBR ACL, traffic addressed to the MSFC3 is policy routed in hardware instead of being forwarded to the MSFC3. To prevent policy routing of traffic addressed to the MSFC3, configure PBR ACLs to deny traffic addressed to the MSFC3.
- SPAN and RSPAN destination ports transmit VACL-redirected traffic. (CSCea57673)
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown. (CSCea23571)
- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.
- The PFC3 does not apply egress policing to traffic that is being bridged to the MSFC3.
- The PFC3 does not apply egress policing or egress DSCP mutation to multicast traffic from the MSFC3.
- With a PFC3, PFC QoS does not rewrite the ToS byte in bridged multicast traffic.
- The MSFC3 supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT (for inside to outside translation), TCP intercept, context-based access control (CBAC), and encryption.

- The PFC3A does not support any PFC QoS features on tunnel interfaces. The PFC3BXL supports PFC QoS features on tunnel interfaces.
- When you configure NAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)
- The PFC3BXL does not provide hardware switching for ICMP traffic if you configure NAT.
- The PFC3A does not provide hardware switching for ICMP traffic if you configure NAT or Cisco IOS reflexive ACLs.
- If you configure Unicast RPF check to filter with an ACL, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the MSFC for the Unicast RPF check. Packets permitted by the ACL are forwarded in hardware without a Unicast RPF check. (CSCdz35099)
- The PFC3 does not provide hardware supported Unicast RPF check for policy-based routing (PBR) traffic. (CSCea53554)
- If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.

- Enter the **copy running-config startup-config** command and the **redundancy reload peer** command to synchronize SNMP ifIndexes when RPR+ redundancy and SNMP ifIndex persistence are configured when all modules are online after any system boot or when you insert a module while the system is running. (CSCdy16763)
- RPR+ redundancy automatic startup configuration synchronization supports only the nvram:startup-config file. With RPR+ redundancy configured, if you enter a **boot config** command that does not specify nvram:startup-config as the startup configuration file, you must manually copy the startup configuration file to the redundant supervisor engine's device specified in the boot config command. (CSCdx25320)
- RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- Traffic flow and SNMP connectivity is interrupted briefly if you perform an online insertion and removal (OIR) that changes the number of fabric-enabled modules so that the switch must use a different fabric channel switching mode. (CSCdx39882)
- The Ethernet port ASICs drop frames that are invalid (for example, frames that are shorter than the minimum valid length). The Ethernet port ASICs do not keep a count of dropped frames. (CSCdx14209)
- Any options in Cisco IOS ACLs that provide filtering in a policy-map class that would cause flows to be sent to the MSFC to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in QoS policy-map classes.

The PFC does not provide QoS for flows that match an ACE in a Cisco IOS ACL configured with options that cause the flows to be sent to the MSFC to be switched in software, except when the Cisco IOS ACL provides filtering in a QoS policy-map class. For example, the PFC does not provide QoS for flows that match an ACE in a Cisco IOS ACL with logging configured. (CSCds72804)

- For multicast flows, the PFC does not provide Layer 3 switching on output interfaces with MTU sizes smaller than the flow's input interface MTU size.  
**Workaround:** Configure the same MTU size on both the input and output interfaces. (CSCds42685)
- Entering the **clear mls qos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded, which would otherwise be policed. (CSCdt40470)
- Catalyst 6500 series switches and Cisco 7600 series routers do not support:
  - Integrated routing and bridging (IRB)
  - Concurrent routing and bridging (CRB)
  - Remote source-route bridging (RSRB)
- Use bridge groups on VLAN interfaces, sometimes called fall-back bridging, to bridge nonrouted protocols. Bridge groups on VLAN interfaces are supported in software on the MSFC.
- Catalyst 6500 series switches and Cisco 7600 series routers do not support the IEEE bridging protocol for bridge groups. Configure bridge groups to use the VLAN-bridge or the DEC spanning-tree protocol.
- FlexWAN module interfaces support dNBAR. Do not configure NBAR or dNBAR on other interfaces.
- Ingress IP Packets with TTL=1 that are not addressed to the MSFC and that match QoS filtering parameters might cause overpolicing of other ingress traffic on the same ingress interface.
- When the outgoing interface list for group G traffic transitions to null on a last-hop multicast router, the router sends a (\*,G) prune message to the PIM neighbor toward the rendezvous point (RP) to stop the flow of group G traffic (if any) down the shared tree, but does not send an (S,G) prune message to stop the flow of traffic down the shortest path tree (SPT). The transition of the outgoing interface list to null does not trigger an (S,G) prune message. (S,G) prune messages are triggered by the arrival of (S,G) traffic.  
  
If the last-hop multicast router is a Catalyst 6500 series switch, traffic is forwarded in hardware. In most cases, RPF-MFD is installed for the (S,G) entries. The MSFC does not see the multicast traffic flowing down the SPT and does not send any traffic-triggered (S,G) prunes to stop the flow of traffic down the SPT. This situation does not have any adverse effect on the MSFC because the PFC processes and drops the unwanted (S,G) traffic.
- The **ip multicast rate-limit** command is not supported on LAN ports. (CSCds22281)
- Catalyst 6500 series switches and Cisco 7600 series routers do not support network booting.
- The IP HTTP server feature is disabled by default. Enter the **ip http server** command to use the feature.
- For LAN switching modules, the Cisco IOS **show controllers** command generates no output on a Catalyst 6500 series switch or Cisco 7600 series router. Enter the **show module** command instead.
- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.
- By default, the MSFC sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group.

With the **ip unreachable** command enabled (which is the default), the supervisor engine drops most of the denied packets in hardware and sends only a small number of packets (10 packets per second, maximum) to the MSFC to be dropped, which generates ICMP-unreachable messages.



To eliminate the load imposed on the MSFC CPU by the task of dropping denied packets and generating ICMP-unreachable messages, you can enter the **no ip unreachable** interface configuration command to disable ICMP unreachable messages, which allows all access-group denied packets to be dropped in hardware.

- MAC address-based Cisco IOS ACLs are not supported for packets that are Layer 3 switched in hardware. MAC address-based Cisco IOS ACLs will be applied on software-switched packets.
- If you enable multicast routing globally, then you should also enable multicast routing (using the **ip pim** command) on all Layer 3 interfaces on which you anticipate receiving IP multicast traffic. This command causes the packets to be sent to the process switching level to create the route entry. If you disable multicast routing on the RPF interface, the entry cannot be created and the packet is dropped. If the source traffic rate exceeds what can be handled by the process level, it can have an undesirable impact on the system. For example, routing protocol packets, such as EIGRP hello packets, might get dropped.
- 24-port 100FX switching modules ([WS-X6224-100FX-MT](#)) with a hardware version of 1.1 or lower only support IEEE 802.1Q VLAN trunking; they do not support ISL trunking. Do not configure ISL trunks on 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower. The restriction against ISL VLAN trunking is the only known problem with hardware version 1.1 or lower of these modules. If you do not require ISL VLAN trunking, these modules are fully functional. The ISL VLAN trunking problem has been corrected in hardware version 1.2 or later. If you want to return a WS-X6224-100FX-MT module with a hardware version of 1.1 or lower, contact Cisco Systems. You can identify WS-X6224-100FX-MT hardware versions using one of these two methods:
  - Command-line interface (CLI) method—Enter the **show module** command to identify the hardware version of the WS-X6224-100FX-MT module.
  - Physical inspection method—The part number is printed on a label on the outer edge of the component side of the module. Versions 73-3245-04 or lower do not support ISL trunking.
- The RJ-21 connectors on the 48-port 10/100TX switching module ([WS-X6248-TEL](#)) do not support Category 3 RJ-21 telco connectors and cabling. Category 3 connectors and cabling cause carrier sense errors. Use Category 5 RJ-21 telco connectors and cables (the module is keyed for Category 5 telco connectors and cables).
- The in and out ports displayed in Layer 3 table entries are set by the hardware at the time the entry is created. They are not guaranteed to be accurate in case multiple flows use the same entry (for example, if the flow mask is **Dest-only** and some kind of load sharing is active) or if the source or destination of the Layer 3 entry moves in the Layer 2 topology. The port information is not always available when the Layer 3 entry is established. This is the case if the destination port of the rewritten packet is unknown when the shortcut is created.
- For EtherChannels, you can configure the QoS trust state and default CoS directly on the EtherChannel interface with the **mls qos trust** or **mls qos cos** commands, respectively. These two parameters must be the same for all physical interfaces in the channel. No other QoS queueing configuration commands can be applied to EtherChannel interfaces. Other QoS queueing configuration commands can be applied, however, to individual EtherChannel physical interfaces. After the physical interfaces are bundled into an EtherChannel, QoS classification, marking, and policing by the Policy Feature Card (PFC) for the channel packets is determined by the service-policy attached to the EtherChannel interface. The service policies attached to the individual physical interfaces of the EtherChannel do not matter. The same is true for the port-based and VLAN-based QoS state of the EtherChannel interface. You can disable the PFC QoS features using the **no mls qos** interface configuration command on the EtherChannel interface.
- The maximum recommended number of Layer 3 multicast entries is 10,000. The maximum recommended number of multicast entries supported in the Layer 2 forwarding table is 12,000.

- After enabling Protocol Independent Multicast (PIM) on an interface, you need to enter the **ip mroute-cache** command on the interface to enable multicast fast-switching. If you have “no ip mroute-cache” configured, multicast packets that are not hardware switched will go to the process level that increases the load on the router.
- The **show ibc** command misleadingly displays Inter-Switch Link (ISL) trunk status as “disabled” and the GBIC as “missing,” because the IBC in a Catalyst 6500 series switch or Cisco 7600 series router is the internal electrical interface between the switch processor and the route processor. Trunk and media types are not given for this type of interface. (CSCdp21121, CSCdp21380)
- The **show access-list** command displays statistics only for traffic that matches ACLs processed in software on the MSFC. The **show access-list** command does not display statistics for traffic that matches an ACL supported in hardware on the PFC. (CSCdt14386)
- The **show interface stats** command does not display statistics for traffic that is Layer 3 switched by the PFC. The **show interface** command displays statistics (labelled **L2** and **L3**) for traffic that is Layer 3 switched by the PFC. (CSCds41388)
- To avoid subjecting routing protocol packets to policy-based routing, configure filtering in route maps so that it does not match routing protocol packets. (CSCds44369)
- Microflow policing does not support policing of identical flows arriving on different interfaces simultaneously. Attempts to do so lead to incorrectly policed flows. (CSCdt72147)
- Because the system does not boot from MSFC bootflash, if the NVRAM configuration is not valid (or not present), the **service config** option defaults to “on,” and the service config feature is enabled after the **erase startup-config** command is issued. (CSCdp12598)
- In a VTP version 1 domain with some switches running Catalyst software and some switches running Cisco IOS software on both the supervisor engine and the MSFC, if the VLANs were created on a switch running Catalyst software and then propagated through VTP to switches running Cisco IOS software, if you enter commands on the switches running Cisco IOS software to configure VTP version 2, you might receive messages about invalid VLAN configuration.

**Workaround:** Perform VLAN configuration on a switch running Catalyst software or enter VLAN configuration commands to correct all VLAN configuration errors reported in the messages. (CSCdp47622)

- The **interface range** command is not supported by the HTTP user interface. The command will execute on only the first interface in the specified range. Do not use the **interface range** command with the HTTP interface. (CSCdm54471)
- When using the UplinkFast feature, the system does not send out the dummy multicast packets used to notify upstream users of forwarding-path changes. Normal Layer 2 aging is used to delete invalid entries. (CSCdm65881)
- Running an SNMP topology discovery application might cause high CPU utilization. (CSCef12458)
- Following power up or a reload, you might see “%ALIGN-3-TRACE: -Traceback=” messages. (CSCed76016)
- A high CPU usage might occur when ERSPAN jumbo frames exceed the frame size of the adjacency MTU of the egress interface. The ERSPAN packets are processed by the MSFC, which causes the CPU usage to increase. The ERSPAN packets are dropped because the Don’t Fragment (DF) bit is set.

**Workaround:** The MTU failure packets are rate-limited when you enter the global configuration command **mls rate-limit all mtu-failure**. (CSCsd55182)

- When traffic with a multicast destination IP address and a broadcast destination MAC address is replicated to one or more VLANs, the destination MAC addresses in the replicated traffic are not rewritten, which preserves the broadcast destination MAC address. Systems that receive the traffic classify it as broadcast traffic instead of multicast traffic. IGMP snooping cannot constrain broadcast traffic.

**Workaround:** none. (CSCse07679)

## FlexWAN Limitations and Restrictions

- FlexWAN ports do not support SPAN or RSPAN.
- MPLS on the FlexWAN module does not support Virtual Private LAN Service (VPLS).
- On FlexWAN ports configured for EoMPLS, the counters displayed by the **show mpls** command for parallel links between LERs do not update. (CSCdw04208, CSCdu87648)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- Ethernet over Multiprotocol Label Switching (EoMPLS) per-VLAN traffic shaping does not work with a FlexWAN egress port. (CSCdx10583)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- To use the interfaces on the FlexWAN module, you must enable IP routing on the MSFC. (CSCdp34896)

## OSM Limitations and Restrictions

- In rare situations, with redundant supervisor engines, extra internal VLANs are allocated when you configure subinterfaces on OSMs. (CSCee27158)
- OSM WAN ports do not support SPAN or RSPAN.
- With 30,000 Virtual Private LAN Service (VPLS) VCs configured, OSM interfaces stop passing traffic if an RPR+ switchover occurs during a period of high CPU usage.

**Workaround:** Enter **no power enable module slot\_number** and **power enable module slot\_number** commands for the OSMs. (CSCed17668)

- If you use the Class-Based Weighted Fair Queueing (CBWFQ) **shape average** command and apply the configured policy map to an interface on an OSM, traffic-shaping accuracy cannot be guaranteed if the target bit rate specified is less than 256,000 bits per second. (CSCea06515)
- The PFC QoS **police** command and the PXF-based **set** command are both used to set IP precedence. However, when you configure the **set ip prec** command for an OSM VPN path, the **mls qos** command is ignored. (CSCdw83517)
- The Gigabit Ethernet WAN ports on the [OSM-4GE-WAN-GBIC](#) and [OSM-2+4GE-WAN+](#) switching modules do not support traffic in the native VLAN of an IEEE 802.1Q trunk. Do not configure a subinterface with the **encapsulation dot1q vlan\_id native** command. (CSCdx60011)
- When you apply the first policy map or remove the last policy map from an interface on an [OSM-1OC48-POS-SS,-SI,-SL module](#) traffic through the interface may be disrupted and the routing protocol may go up and down. (CSCdx94033)

- The channelized OSMs are not supported in the MPLS core. They support IP traffic on customer edge (CE) and provider edge (PE) router links only.
- Unless you enter the **mls qos** command to enable PFC QoS, when you enable MPLS and enter the **random-detect** command in the output policy map on an interface, all OSM traffic through the interface is marked with DSCP 0. (CSCdw79863)
- The WAN ports on the Gigabit Ethernet WAN modules do not support Gigabit EtherChannels.
- If you enter an input **set** command to modify IP precedence for an IP-to-Tag path, the MPLS experimental bits will continue to be derived from the prior IP-precedence setting. In order to modify the experimental bits, use the **set mpls exp** command on the ingress interface. (CSCdw66785)

## Service Module Limitations and Restrictions

- [DHCP snooping](#) does not work properly if DHCP packets to or from a Wireless LAN Service Module cross a WAN link. (CSCef08877)



**Note** In Release 12.2(18)SXD and rebuilds, DHCP snooping is supported only for use with a Wireless LAN Service Module.

- Generating an Rivest, Shamir, and Adelman (RSA) usage key pair with modulo 360 fails.  
**Workaround:** Use a higher modulo value. (CSCec49861)
- In rare situations, with a Supervisor Engine 720 and an IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) configured with IPsec tunnels that use a loopback address as the crypto local endpoint, a reload occurs if there are established IPsec tunnels and you remove the loopback interface. (CSCef77289)
- With an EzVPN connection to a [WS-SVC-IPSEC-1](#) module and XAUTH with a correct group password but an incorrect user password, an IKE SA is created on the WS-SVC-IPSEC-1 module that remains in CONF\_XAUTH and cannot be cleared, which might deplete IKE resources if large volumes of these SAs. (CSCed25345)
- When the NAM is configured as the NDE destination and the NAM is down, the NDE traffic is flooded.  
**Workaround:** Clear the NDE configuration for the NAM or enter the **clear arp-cache** command. (CSCdy55261)
- You cannot SPAN ingress traffic from the IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) or from the Firewall Services Module ([WS-SVC-FWM-1-K9](#)). (CSCec79733)
- With the tunnel MTU size configured to 9216 bytes, tunnel packets larger than 9211 bytes are corrupted.  
**Workaround:** None. (CSCec04627)

## Caveats

- [Caveats in Release 12.2\(18\)SXF and Rebuilds, page 213](#)
- [Caveats in Release 12.2\(18\)SXE and Rebuilds, page 286](#)
- [Caveats in Release 12.2\(18\)SXD and Rebuilds, page 333](#)

- [Caveats in Release 12.2\(17d\)SXB and Rebuilds, page 368](#)
- [Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 408](#)
- [Caveats in Release 12.2\(17a\)SX and Rebuilds, page 418](#)
- [Caveats in Release 12.2\(14\)SX and Rebuilds, page 426](#)

**Note**

- All caveats in Release 12.2(18)S also apply to Release 12.2(18)SXD and later 12.2SX releases. See the “Caveats” section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122srn.htm>
- All caveats in Release 12.2(17d) also apply to Release 12.2(17d)SXB and rebuilds.
- All caveats in Release 12.2(17b) also apply to Release 12.2(17b)SXA and rebuilds.
- All caveats in Release 12.2(17a) also apply to Release 12.2(17a)SX and rebuilds.
- For information about Release 12.2(17a), Release 12.2(17b), and Release 12.2(17d), refer to this publication: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/index.htm>
- All caveats in Release 12.2(14)S also apply to Release 12.2(14)SX and later 12.2SX releases. See the “Caveats” section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122srn.htm>

## Caveats in Release 12.2(18)SXF and Rebuilds

- [General Caveats in Release 12.2\(18\)SXF and Rebuilds, page 213](#)
- [Cisco IOS Software Modularity Caveats, page 267](#)
- [FlexWAN Caveats in Release 12.2\(18\)SXF and Rebuilds, page 268](#)
- [Service Module Caveats in Release 12.2\(18\)SXF and Rebuilds, page 274](#)
- [OSM Caveats in Release 12.2\(18\)SXF and Rebuilds, page 279](#)
- [SPA Caveats in Release 12.2\(18\)SXF and Rebuilds, page 282](#)

**Note**

- The caveat information for Release 12.2(18)SXF and rebuilds is updated frequently.
- Release 12.2(18)SXF2 includes all fixes that are in Release 12.2(18)SXF1, Release 12.2(18)SXE4, Release 12.2(18)SXD7, and Release 12.2(17d)SXB11.
- Release 12.2(18)SXF includes all fixes that are in Release 12.2(18)SXE3, Release 12.2(18)SXD6, and Release 12.2(17d)SXB10.

## General Caveats in Release 12.2(18)SXF and Rebuilds

- [Open General Caveats in Release 12.2\(18\)SXF6, page 214](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF6, page 214](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF5, page 218](#)

- [Resolved General Caveats in Release 12.2\(18\)SXF4, page 232](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF3, page 234](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF2, page 235](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF1, page 244](#)
- [Resolved General Caveats in Release 12.2\(18\)SXF, page 245](#)

## Open General Caveats in Release 12.2(18)SXF6

- With [WS-X6708-10GE](#) switching modules that are configured with Layer 2 [distributed EtherChannels \(DECs\)](#), in certain cases the MAC-address tables can become unsynchronized, which can result in 30 to 190 seconds of unknown unicast traffic flooding. Such flooding is possible even when out-of-band MAC-address table synchronization is enabled with the **mac-address-table synchronize** command, which is enabled by default when WS-X6708-10GE switching modules are installed. (CSCsc20900)
- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

## Resolved General Caveats in Release 12.2(18)SXF6

- When you configure an extended ACL that is using the same name as an active reflexive ACL a message appears, indicating that an error has occurred in the system time and a traceback might occur. A software-forced reload also might occur when a standard ACL is configured using the same name as an active reflexive ACL. These problems occur when the reflexive timer expires. This problem is resolved in Release 12.2(18)SXF6. (CSCin85894)
- A Supervisor Engine 720 might reload when you install a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXF6. (CSCse73539)
- When you connect to a Cisco IOS Secure Copy (SCP) server, and then you specify a full path consisting of one or more directories for the *destination-url* parameter in the **copy scp:destination-url** command, the following message is displayed:

```
%scp: error: unexpected filename: /tmp/test %Error writing
scp://root@172.18.124.187//tmp/test (Permission denied)
```

**Workaround:** Specify the destination IP address in the command. The file will be placed in the top level of the destination file directory. Move the file internally into the desired directory.

This problem is resolved in Release 12.2(18)SXF6. (CSCsb62045)

- When SNMP deletes an existing Network Time Protocol (NTP) reference clock peer, this configuration change is not synchronized on the standby supervisor engine. After SNMP deletes a reference clock peer, a reload occurs when you enter the **show running-config** command.

**Workaround:** Unconfigure refclock peers to prevent their interaction with SNMP.

This problem is resolved in Release 12.2(18)SXF6. (CSCek27504)

- Static routes that are configured with a name that includes an embedded space are not recognized after a reload. This problem is resolved in Release 12.2(18)SXF6. (CSCee77180)

- When a virtual circuit goes down, dynamic MAC addresses are not purged if Hierarchical Virtual Private LAN Service (H-VPLS) is configured. This problem is resolved in Release 12.2(18)SXF6. (CSCsb80468)
- When one port of a DEC goes down, a disruption in traffic forwarding might occur. This problem might cause some control protocols to timeout. This problem is resolved in Release 12.2(18)SXF6. (CSCsc56766)
- SNMP cannot retrieve the subinterface counters that are displayed when you enter the **show vlan counters** command. This problem is resolved in Release 12.2(18)SXF6. (CSCse29419)
- A system configured with an IPsec VPN SM or an IPsec SPA may incorrectly drop transit IPsec Network Address Translation (NAT) traversal packets that are transported over UDP port 4500. This problem occurs when the system is configured to terminate IPsec tunnels on the VPN SM, and if the NAT traversal packets need to traverse the crypto VLAN. This problem is resolved in Release 12.2(18)SXF6. (CSCse35278)
- A Virtual Router Redundancy Protocol (VRRP) master virtual router might respond to an ARP request to the IP address of the virtual router with its interface MAC address. This problem occurs after you enter the **shutdown** command and then the **no shutdown** command on the master virtual router VRRP interface. This problem is resolved in Release 12.2(18)SXF6. (CSCeg51303)
- An ATM permanent virtual circuit (PVC) configured to support ATM operation, administration, and maintenance (OAM) might not pass traffic. This problem is resolved in Release 12.2(18)SXF6. (CSCei39688)
- When you stop bit error rate testing (BERT) or if BERT exceeds the time interval, the BERT status shows that BERT is still running and can no longer be stopped. You also cannot restart BERT. This problem is resolved in Release 12.2(18)SXF6. (CSCek28561)
- When QoS low latency queueing (LLQ) is configured, latency remains high for an ATM PVC that has a bandwidth higher than 14 Mbps. This problem is resolved in Release 12.2(18)SXF6. (CSCsc00993)
- The Cisco Appliance Server Architecture (CASA) routing agent might cause high CPU utilization. This problem occurs when oversubscribed CASA client traffic is switched in software and placed on the IP input queue with a large number of wildcard updates from the host. This problem is resolved in Release 12.2(18)SXF6. (CSCse29465)
- A reload might occur when you use Web Cache Communication Protocol (WCCP) Layer 2 redirection and mask assignment mode with a host-based standard ACL as a WCCP redirect ACL. This problem is resolved in Release 12.2(18)SXF6. (CSCsa77785)
- Some objects in newly created rows of ciscoFlashCopyTable and ciscoFlashMiscOpTable cannot be read. Objects become readable after you set their values. This problem is resolved in Release 12.2(18)SXF6. (CSCdy11174)
- You can enter the **logging source-interface interface-type interface-number** command without errors occurring, but this command does not work. Syslog packets will continue to use the address of the interface that transmitted them. This problem is resolved in Release 12.2(18)SXF6. (CSCse23548)
- When an access control list (ACL) that is associated with a multicast boundary is modified to permit a statically joined group, the change does not take effect. This problem affects the static group memberships underlying MVPN tunnels by disrupting connectivity across them.

**Workaround:** Disable and reenter the **ip multicast boundary access-list** command.

This problem is resolved in Release 12.2(18)SXF6. (CSCek31478)

- If a system is configured with an IPsec VPN services module or an IPsec SPA, and a WS-X6582-2PA Enhanced FlexWAN module that contains a Fast Ethernet port adapter, the system might be unable to resolve ARP requests. This problem is resolved in Release 12.2(18)SXF6. (CSCsd47475)
- When the Spanning Tree Protocol (STP) blocks a port, some of the MAC addresses learned on that port are not purged. This problem is resolved in Release 12.2(18)SXF6. (CSCsd96121)
- A Supervisor Engine 720 might reload when you install a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXF6. (CSCse73539)
- When the system receives a corrupted heart beat message, a reload due to memory corruption might occur. This problem is resolved in Release 12.2(18)SXF6. (CSCse47430)
- If you configure unicast RPF checking to filter with an exception ACL, very high CPU usage might occur. This situation occurs even when no non-RPF traffic is present. This problem is resolved in Release 12.2(18)SXF6. (CSCsc81300)
- A reload might occur after displaying an ALIGN-1-FATAL message. This problem occurs after you modify a service policy on an ATM subinterface or a permanent virtual circuit (PVC). This problem is resolved in Release 12.2(18)SXF6. (CSCse02510)
- A memory leak might occur when you use the **ip pgm router** command to configure PGM router assist on GRE tunnel interfaces. This problem is resolved in Release 12.2(18)SXF6. (CSCse09435)
- On a system with QoS configured, egress voice traffic on a WS-X6148-21AF switching module is forwarded through a low-priority queue. This problem causes drops to occur in voice streams. This problem is resolved in Release 12.2(18)SXF6. (CSCse16512)
- When you use the **speed auto 10 100** command to set the port speed, the returned portAdminSpeed value is autoDetect(1). The correct return value for this command is autoDetect10100(2). This problem is resolved in Release 12.2(18)SXF6. (CSCse86602)
- For wildcard updates, the **debug ip casa packet** command might display incorrect values for the IP address and protocol. This problem is resolved in Release 12.2(18)SXF6. (CSCse45427)
- When you configure Multinode Load Balancing (MNLB), CASA traffic is process switched instead of CEF switched. This problem is resolved in Release 12.2(18)SXF6. (CSCse54768)
- If you enter the **crypto pki trustpoint** command, and then specify a loopback interface in the **ip-address** subcommand, this information will be lost after a reload. This problem is resolved in Release 12.2(18)SXF6. (CSCse29545)
- When CASA is configured with Multinode Load Balancing (MNLB), wildcard updates from the service manager might get dropped when a burst of 50 updates arrives. This problem is resolved in Release 12.2(18)SXF6. (CSCse76405)
- If more than 1500 NAT configuration statements are entered into a Telnet or Console session, a memory leak might occur. This problem is resolved in Release 12.2(18)SXF6. (CSCse51577)
- The cbQosCMDrop MIB counters are reset when you enter the **clear counters** command. This problem is resolved in Release 12.2(18)SXF6. (CSCse62117)
- An ICMP or an IGMP ACE that uses the fragment keyword in a numbered ACL is rejected during a reload. This problem is resolved in Release 12.2(18)SXF6. (CSCei26931)
- A spurious memory access message and traceback might occur when you enter the **show ipc queue** command to display information about the interprocess communication (IPC) retransmission queue and the IPC message queue. This problem is resolved in Release 12.2(18)SXF6. (CSCee23195)
- The system might suspend indefinitely when you use the **clear adjacency** command to clear and repopulate the adjacency table. This problem is resolved in Release 12.2(18)SXF6. (CSCej42121)



- When you enter the **udld port disable** command on the second uplink port of an active or standby supervisor engine, and then perform several HA switchovers, the **udld port disable** command might be removed from the configuration. This problem is resolved in Release 12.2(18)SXF6. (CSCsc59025)
- A reload might occur when you enter commands (for example, **clear ip route**) while a high-temperature alarm message is being displayed. This problem is resolved in Release 12.2(18)SXF6. (CSCsd95575)
- If you configure a network access server (NAS) for login authentication by entering the **aaa authentication login default none** command or the **aaa authentication login default local** command, an AAAA-3-NOREG message and a traceback might be displayed when you log in. This situation occurs because no TACACS or RADIUS group has been configured. You need to configure the NAS for login authentication by using the **aaa authentication login default group radius** command or the **aaa authentication login default group tacacs+** command. This problem is resolved in Release 12.2(18)SXF6. (CSCse45735)
- An HTTP request packet that is received during the initialization of the Cisco IOS firewall authentication proxy feature is not processed correctly. This situation causes the initialization to fail.

**Workaround:** Enter the **ip http auth aaa** command to initialize the Cisco IOS firewall authentication proxy feature manually.

This problem is resolved in Release 12.2(18)SXF6. (CSCse61025)

- When you configure routing protocols that use multicast packets for updating (for example, OSPF) on an ATM interface, pings might fail across the interface. This problem occurs when you enter the **clear cef linecard** command. This problem is resolved in Release 12.2(18)SXF6. (CSCeh32595)
- Traffic might stop passing through an IPsec VPN module or an IPsec SPA that is configured as a VLAN tunnel interface. This problem occurs when the outbound interface is an OSM interface and you enter the **no shut** command on that interface. This problem is resolved in Release 12.2(18)SXF6. (CSCse85399)
- A memory leak might occur on both the supervisor engine and the DFC when there is BGP-route instability. This problem is resolved in Release 12.2(18)SXF6. (CSCse61121)
- When all cache engines in a Web Cache Communication Protocol (WCCP) service group are lost, traffic is processed in software instead of being switched in hardware. This problem is resolved in Release 12.2(18)SXF6. (CSCse69713)
- Port numbers for self-originated TCP connections are determined by using an incremental method which causes them to be too easy to predict. Any self-originated TCP connection that uses non-well-known port numbers is subject to this behavior. This problem is resolved in Release 12.2(18)SXF6. (CSCee32814)
- A system might assign an incorrect MPLS label to a prefix when the prefix transitions from a nonrecursive to a recursive route. This problem might occur when you connect to a MPLS-VPN provider edge (PE) router that has floating static Null0 routes, and a per-user recursive static route is installed. This prefix will not be reachable from distant PEs. This problem is resolved in Release 12.2(18)SXF6. (CSCef32748)
- A reload might occur during initialization on a system configured for SSO switchover that has the **snmp mib notification-log default** command enabled. This problem is resolved in Release 12.2(18)SXF6. (CSCsc14034)
- Redistributed routes might not be advertised if they traverse an ISIS IPv4 VRF-enabled interface that goes up and down. This problem occurs when the redistributing router reloads. This problem is resolved in Release 12.2(18)SXF6. (CSCsc37212)

- The order in which attributes are sent from an AAA server determines which privilege levels are assigned to the users. This process can affect the operation of the RADIUS server and conflicts with RFC 2865 Section 5. This problem is resolved in Release 12.2(18)SXF6. (CSCsd71301)
- When you enter the **ip tcp header-compression** command or the **ip rtp header-compression** command, TCP or RTP packets are not compressed. This problem is resolved in Release 12.2(18)SXF6. (CSCse88171)
- Memory leaks and a reload might occur on an active supervisor engine when invalid Data Link Switching (DLSw) peers are defined. Memory leaks also occur on a standby supervisor engine whenever DLSw is configured. This problem is resolved in Release 12.2(18)SXF6. (CSCsf16715)
- All multicast data packets on ATM multipoint interfaces are dropped. An ATM OSM can direct multicast packets to a single VC configured on a multipoint interface, but the ATM SPA drops all of these packets regardless of the number of VCs configured. This problem is resolved in Release 12.2(18)SXF6. (CSCsf04301)
- You cannot apply a policy to an interface that was previously configured in a Layer 3 port channel. This problem is resolved in Release 12.2(18)SXF6. (CSCse19732)
- An enable authentication request might be sent erroneously to the AAA server group that was configured for login authentication. This problem is resolved in Release 12.2(18)SXF6. (CSCsd95752)
- With a Supervisor Engine 32, packets are recirculated unnecessarily when EtherChannels are configured. Packets also might be duplicated if this system is configured with IPsec SPAs, an IPsec VPN, or an FWSM. This problem is resolved in Release 12.2(18)SXF6. (CSCsc75397)

#### Resolved General Caveats in Release 12.2(18)SXF5

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

Conditions: The packets must be received on a trunk enabled port.

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXF5. (CSCsd34759)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXF5. (CSCsd34855)

- The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Only devices running certain versions of Cisco IOS are affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

This advisory will be posted at:

[http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth\\_proxy.shtml](http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml)

This problem is resolved in Release 12.2(18)SXF5. (CSCsa54608)

- When a peer has invalid certificates on an IPsec IKE responder, failed IKE sessions may not be deleted. These failed sessions may accumulate and eventually cause router instability. These failed sessions are displayed in the output of the **show crypto isakmp sa** command. The sessions fail when receiving a bad IKE certificate. This problem occurs when RSA signatures are used as the authentication method.

**Workaround:** You can remove the IKE sessions manually. You also can enter the **shutdown** command followed by the **no shutdown** command on the interface that is used for the IKE sessions. This action brings down all IKE sessions, including any active sessions. You also can reapply the crypto map to this interface. This action brings down all IKE sessions, including any active sessions.

This problem is resolved in Release 12.2(18)SXF5. (CSCeh78411, CSCsd68605)

- If OSPF is enabled on an interface, and then the configuration is changed to redistribute a connected route on this interface with a route map, then the route may not be redistributed correctly. This problem occurs only if the route map is used as a parameter with the **redistribute** command. This problem is resolved in Release 12.2(18)SXF5. (CSCee81606)
- Systems Network Architecture (SNA) packets are not bridged when VLAN 1025 is used on the bridged interface. When this problem occurs, SNA sessions cannot be established. This problem occurs on a Supervisor Engine 2. This problem is resolved in Release 12.2(18)SXF5. (CSCsc05015)
- If a Supervisor Engine 2 is configured with a Layer 2 nondistributed EtherChannel and a Layer 3 [distributed EtherChannel \(DEC\)](#), traffic ingressing on any port and egressing on the Layer 2 non-DEC, floods within the VLAN that contains the destination MAC address. This situation occurs

when the EtherChannel purging timer expires (approximately every 21 minutes). The number of flooded packets depends on the traffic rate and Layer 2 table size. This problem is resolved in Release 12.2(18)SXF5. (CSCsc54382)

- You might exceed the 255 buffer character limit for the **mac-address-table static** command if you enter too many interface names for the MAC in the same command. The following message is displayed:

```
Enter configuration commands, one per line. End with CNTL/Z.
% Incomplete command.
```

**Workaround:** Split the command that is specifying the interfaces into multiple commands. This problem is resolved in Release 12.2(18)SXF5. (CSCsc54552)

- Hardware switching is disabled because of an MLS CEF sanity failure after the following message is displayed:

```
%MLSCEF-SP-2-FREEZE: hardware switching disabled on card
```

This problem is resolved in Release 12.2(18)SXF5. (CSCsd64158)

- A reload might occur when the OSPF-MIB table ospfExtLsdbTable is queried with an SNMP walk. Alignment errors might occur when you enter the **show alignment** command because of this same problem. This problem is resolved in Release 12.2(18)SXF5. (CSCef11304)
- A system might not withdraw a BGP route from an iBGP peer. This problem occurs when you enter the BGP neighbor-specific **clear ip bgp neighbor-address soft out** command for a member of the system's peer group, and then changes occur to the outbound policy of that member. This problem is resolved in Release 12.2(18)SXF5. (CSCeg52659)
- An established Point to Point Tunneling Protocol (PPTP) connection fails when Network Address Translation (NAT) or Port Address Translation (PAT) translates a new PPTP Call ID incorrectly. This problem occurs when NAT dynamic overload is configured. This problem is resolved in Release 12.2(18)SXF5. (CSCeh35083, CSCsd56549)
- When a system receives an Multicast Listener Discovery (MLD) report for an IPv6 multicast group, the IPv6 MFIB entry for the group is updated on the MSFC but the MFIB entry on the supervisor engine is not updated for several seconds. This situation delays the start of multicast forwarding. This problem occurs when a receiver joins and leaves a multicast group several times. This problem is resolved in Release 12.2(18)SXF5. (CSCsb91644)
- Outbound ACLs that are applied to SVIs have no effect on traffic from Layer 3 interfaces. This problem is resolved in Release 12.2(18)SXF5. (CSCsd03882)
- High CPU utilization occurs while processing ingress IPv6 traffic. This problem occurs under the following conditions:
  - There are no forwarding entries corresponding to the destination addresses of the IPv6 multicast traffic.
  - The destination MAC address is 3333.0000.0001, 3333.0000.000d or 3333.0000.0016.
  - The ingress port is a routed port.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd25532)

- Memory leaks occur when a Certification Authority (CA) digital certificate has the serial number as an attribute in the subject name. This problem is resolved in Release 12.2(18)SXF5. (CSCsd43903)
- Memory leaks might occur in the Internet Key Management Protocol (IKMP) process when using Internet Security Association and Key Management Protocol (ISAKMP) certificates for peer authentication. This problem is resolved in Release 12.2(18)SXF5. (CSCsd45167, CSCsd49723, CSCsd49767)

- A Frame Relay interface might change the encapsulation on Frame Relay (FR) frames from Internet Engineering Task Force (IETF) encapsulation to Cisco encapsulation under these conditions:
  - Network Address Translation (NAT) or a reflexive ACL is configured on a Frame Relay permanent virtual circuit (FR PVC).
  - There is ingress and egress TCP traffic.

In an FRF.8 environment, this change in the encapsulation causes end-to-end TCP sessions to fail because an intermediate device drops the Cisco-encapsulated Frame Relay frames. This problem is resolved in Release 12.2(18)SXF5. (CSCsd58552)

- A Hot Standby Router Protocol (HSRP) active router does not respond to an ARP request for a virtual IP address. This problem might occur when the same HSRP virtual IP address is misconfigured on different HSRP groups on different routers. This problem is resolved in Release 12.2(18)SXF5 (CSCsd80754)
- When you enter the **show vlans *vlanID*** command, the counters do not display the same values as the SNMP counters. This problem is resolved in Release 12.2(18)SXF5. (CSCsd94687)
- A large memory leak might occur on a Supervisor Engine 720 when a VLAN, a portchannel, or an individual interface goes down. This problem occurs when the system is in egress replication mode and there are no DFCs present. The interface that goes down must be an outgoing interface of a multicast entry in the hardware. The memory leak is proportional to the number of multicast entries that apply to this interface.

**Workaround:** Put the system in ingress replication mode by entering the **mls ip multicast replication-mode ingress** global configuration command or install a DFC with the system in egress replication mode.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd98887)

- If you use Secure Copy to copy a configuration file, a bus error and a reload occurs. This problem is resolved in Release 12.2(18)SXF5. (CSCse12154)
- With VRF-aware IPsec configured on a VPN Services Module (VPNSM) or an IPsec SPA, the system does not send the peer device IKE DELETE NOTIFY message when it receives an IPsec packet that has an invalid Security Parameter Index (SPI). This situation causes loss of encrypted traffic. This problem is resolved in Release 12.2(18)SXF5. (CSCse15728)
- When you enter the IOS IP service level agreement (SLA) configuration command **rtr restart** to restart a probe, the probe is restarted and operates normally, but when you enter the **show rtr** configuration command, the following message is displayed:

```
Status of Entry (SNMP RowStatus): notInService
```

This problem is resolved in Release 12.2(18)SXF5. (CSCsa61284)

- If traffic loss occurs when there is a high volume of broadcast traffic, the input broadcast counter increments and the input counter does not increment. Because the value of the SNMP ifHCInUCastPkts MIB object is the difference between the input counter and the input broadcast counter, the value of ifHCInUCastPkts might become negative. This problem is resolved in Release 12.2(18)SXF5. (CSCsc62574)
- This DDTs documents changes in how Cisco IOS software handles packets destined to the router. This problem is resolved in Release 12.2(18)SXF5. (CSCek26492)
- A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a **show buffers** command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially

execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml>.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc64976)

- Policing stops working on a Layer 2 switchport after you enter the **shutdown** command and then the **no shutdown** command.

**Workaround:** Remove and reapply the service policy.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd15806)

- The SNMP MIB object `cardIfIndexEntry` is deprecated and should not appear in the SNMP view. This problem is resolved in Release 12.2(18)SXF5. (CSCek24053)
- Automatic detection of inline power does not work on WS-X6196-RJ-21 switching modules, and the following message is displayed:

```
%C6K_POWER-SP-4-PD_NOLINKUP: The device connected to 1/37 is powered up but
its link is not up in 5 seconds. Therefore, power is withdrawn from the port
```

This problem is resolved in Release 12.2(18)SXF5. (CSCek30589)

- After a reload a BGP neighbor might not be recognized as directly connected. This problem occurs when the crypto connect mode is configured to support a VPN service module or an IPsec SPA.

**Workaround:** Enter the **ebgp multihop** command to reconnect the neighbor.

This problem is resolved in Release 12.2(18)SXF5. (CSCsa98081)

- An OSPF route is lost after an interface goes up and down. This problem occurs when all of the following conditions are present:
  - A point-to-point interface such as a POS interface goes up and down briefly (shorter than 500 ms).
  - The neighbor does not notice the interface going up and down, so the neighbor's interface remains up.
  - The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).
  - OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes through this adjacency.
  - The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

**Workarounds:**

- Increase the carrier-delay time for the interface to about 1 second or longer.
- Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc07467)

- When more than one UDP Cisco IOS SLB virtual server is defined in a topology, traffic from the user to the Cisco IOS Server Load Balancing (SLB) real server will be process-switched in software in the MSFC, which degrades performance. This problem is resolved in Release 12.2(18)SXF5. (CSCek22536)

- When an inter-area, external, or not-so-stubby area (NSSA) route is learned using a link state update that follows the initial database synchronization, the route may not be added to the routing table by a partial shortest path first (SPF) computation even though the LSA is installed in the link state database. This problem occurs when a large number of type 3, type 5, or type 7 LSAs are advertised and withdrawn.

**Workaround:** A subsequent full SPF computation causes the route to be added.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc10494)

- When an ICMP unreachable message traverses a Cisco IOS SLB virtual server whose server farm is configured for Network Address Translation (NAT), the checksum of the translated packet is not correct, which causes the ICMP message to be ignored. This problem is resolved in Release 12.2(18)SXF5. (CSCeb77318)
- Cisco IOS enhanced object tracking always reports ports configured with the **switchport** command as down. This problem occurs after a reload with both the tracking configuration and the interface switchport configuration in the startup configuration.

**Workaround:** Delete and reconfigure the enhanced object tracking configuration.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc10914)

- IPv6 bootstrap router (BSR) message packets might fail the reverse path forwarding check. The following message is displayed:

IPv6: Beyond scope of source address

This problem is resolved in Release 12.2(18)SXF5. (CSCsb85290)

- Cisco IOS SLB configured in dispatch mode purges MLS NetFlow IP entries too often, which causes high CPU utilization on the supervisor engine. This problem is resolved in Release 12.2(18)SXF5. (CSCsc18986)
- OSPF might update and originate a new version of a link-state advertisement (LSA) when it should remove the LSA. This problem occurs on the originating router when it receives a self-originated aged out LSA before it can remove this LSA from its database. This problem might also occur when a neighbor calculates that it has a newer copy of the LSA from the originating router and sends the expired LSA to the originating router.

**Workaround:** Enter the **clear ip ospf process** command.

This problem is resolved in Release 12.2(18)SXF5. (CSCei45669)

- ICMP traffic between clients belonging to different Cisco IOS SLB sticky groups might be dropped if the clients are behind Firewall Load Balancer (FWLB) real servers. This traffic is dropped in the real-to-real link. This problem occurs when the **ip slb routing inter-firewall** command is enabled. This problem is resolved in Release 12.2(18)SXF5. (CSCea24341)
- A Dynamic Host Configuration Protocol (DHCP) agent might fail to write DHCP database information to an ATA file system. This problem is resolved in Release 12.2(18)SXF5. (CSCed93425)
- The OSPF MIB objects whose syntax is IPAddress have the incorrect syntax of INTEGER in a trap notification. This problem is resolved in Release 12.2(18)SXF5. (CSCee47792)
- A reload might occur under stress conditions when you unconfigure VRF instances. This situation occurs in a multicast VPN environment. This problem is resolved in Release 12.2(18)SXF5. (CSCei77227)

- The following message and a traceback may appear when Response Time Reporter (RTR) is configured:

```
%SCHED-3-SEMLOCKED: IP RTR Probe MaxName attempted to lock a semaphore, already locked by itself
```

This problem is resolved in Release 12.2(18)SXF5. (CSCei85359)

- An SNMP walk might not complete. This problem occurs because the MIB object identifiers (OIDs) are out of order. This problem is resolved in Release 12.2(18)SXF5. (CSCsb34180)
- With SSO redundancy configured, when you configure a VLAN, SNMP creates a ciscoBridgeExt MIB object cbeDot1dTpVlanAgingFromGlobal. If you set cbeDot1dTpVlanAgingFromGlobal from false to true, the standby supervisor engine will reload. This problem is resolved in Release 12.2(18)SXF5. (CSCsb79306)
- The CISCO-CLASS-BASED-QOS MIB object cbQosCMDropByte64, which displays the amount of bytes being dropped, is always equal to the CISCO-CLASS-BASED-QOS MIB object cbQosCMPrePolicyByte64, which displays the amount of traffic policed. This problem is resolved in Release 12.2(18)SXF5. (CSCeh42489)
- A DHCP snooping-enabled system can include information about itself in client-originated DHCP packets that the system forwards to a DHCP server. The system accomplishes this by using the Dynamic Host Configuration Protocol (DHCP) relay agent information option (option 82). If the DHCP server does not handle the option 82 data properly, and sends a DHCP reply with malformed option 82 data, the DHCP snooping-enabled system might reload. This problem is resolved in Release 12.2(18)SXF5. (CSCeh21210)
- When you enter the **show crypto ca timers** command, the RENEW time displayed in the output never changes. This problem is resolved in Release 12.2(18)SXF5. (CSCse11457)
- When Intermediate System-to-Intermediate System (ISIS) is configured, only one adjacency might be shown in the output of the **show clns** interface command, even though the **show clns neighbors** command might correctly display all the neighbors that are connected to the interface. When this situation occurs, and any one of the neighbors on a segment goes down, all routing updates may be lost. The single adjacency is torn down and routing stops because there are no adjacencies, even though the output of the **show clns neighbors** command still shows that the neighbors are up. This problem occurs when an adjacency goes down while it is still in the INIT state because the adjacency counter is incorrectly decremented.

#### Workarounds:

- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.
- Enter the **clear clns neighbors** command.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc63871)

- A bus error and a reload might occur when adding a shaper and policer under the same policy map, and then removing the policer and adding it back again. This problem occurs when POS switching modules are configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsc26237)
- A high CPU utilization might occur when a system executes a search for a dependent FIB entry of a dependent path. This search occurs when a FIB path is resolved or an adjacency has changed. This problem occurs on a system configured with a PFC2. This problem is resolved in Release 12.2(18)SXF5. (CSCsc77703)
- Memory corruption might occur on switching modules that have different DFC versions (for example, PFC3A on one switching module with PFC3B or PFC3BXL on another). This problem is resolved in Release 12.2(18)SXF5. (CSCsc94171)



- Alignment corrections might occur when DHCP snooping is configured and the DHCP relay agent information option (option 82) is in use. This problem is resolved in Release 12.2(18)SXF5. (CSCsd39189)
- An invalid IP header checksum might be calculated for a multipoint generic routing encapsulation (MGRE) broadcast message. This problem occurs when two clients are connected to the same service set identifier (SSID) and one of the clients sends a broadcast message. The message traverses a GRE tunnel, and then a rebroadcast is generated to reach other nodes. In this situation, the checksum is not recalculated and is invalid, which causes the message to be dropped. This problem is resolved in Release 12.2(18)SXF5. (CSCsd42850)
- In a WCCP redirect ACL list, ACEs that are configured with the log keyword are not programmed into the ternary content addressable memory (TCAM) table. This problem is resolved in Release 12.2(18)SXF5. (CSCsd28870)
- An AutoFail trap is generated when an NMS application polls with an invalid SNMP VLAN name. The appropriate response is an UNKNOWN\_CONTEXT\_NAME error. This problem is resolved in Release 12.2(18)SXF5. (CSCsc85922)
- When establishing a DLSw Ethernet redundancy master and slave relationship, two devices never receive LLC frames transmitted one another. This problem is resolved in Release 12.2(18)SXF5. (CSCsd55300)
- The ipMRouteInterfaceOutMcastOctets MIB object counters do not increment. This problem is resolved in Release 12.2(18)SXF5. (CSCsd37537)
- When a NetFlow shortcut is established to perform Network Address Translation (NAT) in hardware, the hardware cannot parse and perform the translation on the Simple Client Control Protocol (SCCP) portion of a TCP packet. This problem is resolved in Release 12.2(18)SXF5. (CSCsd37634)
- An outbound ACL that is applied to a VLAN interface does not block traffic to a specific host. This problem is caused by an incorrect TCAM entry. This problem is resolved in Release 12.2(18)SXF5. (CSCsb53810)
- Cisco IOS SLB virtual server configuration mode **access** commands might cause almost all traffic sent from a user to the real server associated with the virtual server to be dropped. This problem is resolved in Release 12.2(18)SXF5. (CSCek22595)
- The runts counter does not increment in the output of the **show interface** command but it does increment in the output of the **show interface name counters errors** command. This problem occurs when the interface is a 10 Mbps half-duplex link connected to a WS-X6148-GE-TX Ethernet switching module. This problem is resolved in Release 12.2(18)SXF5. (CSCsd68266)
- Traffic might stop forwarding over an IPsec SPA or an IPsec VPN service module that is configured in crypto connect mode, when the secure side interface is an ATM interface. The problem occurs when ATM traffic shaping is changed in the PVC configuration. This problem is resolved in Release 12.2(18)SXF5. (CSCsd52633)
- An SNMP get or walk fails to find a value for the MIB object dsx1FarEndInterval. This problem occurs because the dsx1FarEndInterval MIB table is not populated after the first three entries. This problem is resolved in Release 12.2(18)SXF5. (CSCsc90782)
- The **show idprom** command does not support all XENPAKs. Unsupported XENPAKs fail a security check, and the interfaces associated with them are shut down. In releases where this problem is resolved, the show idprom command supports non-Cisco XENPAKs. TAC does not support non-Cisco XENPAKs. This problem is resolved in Release 12.2(18)SXF5. (CSCsd49280)

- The following error message and tracebacks may occur after configuring a SPAN session or an IP phone port:

```
%BIT-SP-4-OUTOFRANGE: bit 0 is not in the expected range of 1 to 4095
```

This problem occurs when you configure an access port with the **switchport voice vlan dot1p** command and you configure a VSPAN session. This problem is resolved in Release 12.2(18)SXF5. (CSCsd29927)

- Cisco IOS SLB real servers with non-ping probes within a VRF (for example, Cisco IOS SLB access interfaces in a VRF) do not work, and the real servers do not reach operational state. This problem is resolved in Release 12.2(18)SXF5. (CSCsc38892)
- An IGMP leave will fail for a group on a switch port if that group has any outstanding IGMP queries to process on the same interface. An IGMP general query takes 10 seconds to send a query report, an IGMP specific query takes 1 second. This problem is resolved in Release 12.2(18)SXF5. (CSCsd65434)
- After an interface goes up and down, ARP results might take up to 30 minutes to appear in a MAC address table. This problem is resolved in Release 12.2(18)SXF5. (CSCsd40211)
- When BGP receives an update that has an inferior metric route compared to a previously received route for multiple equal-cost routes, the BGP table is updated correctly but the routing table is not. This situation prevents the old path from being deleted from the routing table. This problem is resolved in Release 12.2(18)SXF5. (CSCsb36755)
- Egress traffic monitoring might stop when RSPAN is enabled and then disabled, and then SPAN is enabled on the same device with the same session number. This problem is resolved in Release 12.2(18)SXF5. (CSCsd42247)
- A bus error and a reload might occur when you enter the IPv6 OSPF **summary prefix** command. This problem is resolved in Release 12.2(18)SXF5. (CSCsd64173)
- High CPU utilization might occur on a Supervisor Engine 720 or a Supervisor Engine 32 when the IP spoofing feature is configured on a cache engine and WCCP redirection is configured in the egress direction. IP-spoofed packets coming from the cache engine, whose destination is either the client or the server, are switched in software instead of hardware.

**Workaround:** Use the **ip wccp service redirect in** command for both the inbound and the outbound interfaces.

This problem is resolved in Release 12.2(18)SXF5. (CSCsb61021)

- Recently configured MPLS VPN VRFs on a Provider Edge (PE) router might not forward traffic.

**Workaround:** Remove the VRF and reconfigure it. When removing the VRF, remove it from the BGP configuration, then from the interface configuration, and finally delete the VRF from the global configuration. Reconfigure the VRF in the reverse order.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd25611)

- Multicast OSPF hello messages might get dropped when you enter the **mls ip verify length minimum** command. This problem is resolved in Release 12.2(18)SXF5. (CSCsd43481)
- The point of local repair (PLR) router erroneously resets the Local protection desired flag in the SESSION\_ATTRIBUTE object of a path message, which it sends to a merge point that has inbound fast reroute (FRR) enabled. If this flag resets, a merge point that does not run Cisco IOS removes the protected label switch path (LSP). This problem is resolved in Release 12.2(18)SXF5. (CSCek35484)

- In an HA topology, dynamic addresses that are secure on a port do not appear on both a standby and an active router after an NSF stateful switchover (SSO). This situation can be seen when you enter the **show port security** *[mod/port]* command. This problem is resolved in Release 12.2(18)SXF5. (CSCsb86198)
- The EtherChannel Min-Links feature might stop working temporarily during a port channel reset or a switching module reset. This situation might cause the port channel to remain in the M state (minimum links not met) and not configure. This problem is resolved in Release 12.2(18)SXF5. (CSCsc61809)
- In a general packet radio service (GPRS) Tunneling Protocol (GTP) load-balancing configuration with Cisco IOS SLB configured, a reload might occur when you remove a real server without taking the real server out of service with the GTP international mobile subscriber identity (IMSI) feature enabled.

**Workaround:** Clear the GTP IMSI sticky entries before removing the real server by entering the **clear ip slb sticky gtp imsi** command.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc46301)

- IPsec VPN service modules and IPsec SPAs do not use the default IPsec security association (SA) lifetime to build SAs. This problem does not affect performance. This problem is resolved in Release 12.2(18)SXF5. (CSCsd67456)
- After a switchover from an active to a standby Supervisor Engine 32, the new active supervisor engine goes online with an empty DHCP snooping binding table. This problem is resolved in Release 12.2(18)SXF5. (CSCsd75929)
- When a Cisco IOS SLB virtual server is set to port 0 and the HTTP probe is set to port 80, the HTTP probe goes to port 80, but the host tag displays 0 instead of the port 80, which is configured in the probe. This situation causes PROBE\_FAILED errors to occur when the host is using IIS Version 6 Windows 2003. This problem is resolved in Release 12.2(18)SXF5. (CSCeb68312)
- A reload might occur when open shortest path first (OSPF) inter-area route changes occur. This problem occurs when incremental shortest path first (iSPF) is configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsd84489)
- SNMP queries issued on Cisco IOS SLB connection state objects continuously cycle. This problem is resolved in Release 12.2(18)SXF5. (CSCsd17174)
- The Supervisor Engine 32 does not support the [WS-X6516-GBIC](#) switching module, hardware revisions 5.0 through 5.4. The following message is displayed when you install the module:  

```
C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot <slot-no>, power not allowed:
Module not at an appropriate hardware revision level.
```

This problem is resolved in Release 12.2(18)SXF5. (CSCek31437)

- The link from a PoE Axis Video Camera to a [WS-X6148A-RJ-45](#) switching module with a PoE daughtercard installed does not come up. This problem is an autonegotiation issue between the Broadcom 5248 on the [WS-X6148A-RJ-45](#) switching module and the ASIC in the camera. This problem is resolved in Release 12.2(18)SXF5. (CSCsd67341)
- When VRF-aware GTP Cisco IOS SLB is configured, a GTP IMSI sticky idle timeout query cannot egress and cannot reach its intended GPRS Gateway Support Node (GGSN). This situation causes the Cisco IOS SLB to delete a GTP IMSI sticky entry even if the GGSN includes the Packet Data Protocol (PDP) context. This problem is resolved in Release 12.2(18)SXF5. (CSCsd64741)
- The port ID advertised by Cisco Discovery Protocol (CDP) might not correspond to the value of the SNMP ifName object on some interface types. These interface types include PoS, portchannel, and Fast Ethernet subinterfaces. This problem is resolved in Release 12.2(18)SXF5. (CSCef78565)

- Port channel interface configuration changes do not propagate to inactive member ports. When the member ports become active, the channels do not form because of this configuration mismatch. This problem is resolved in Release 12.2(18)SXF5. (CSCei93025)
- Setting the rttMonCtrlOperState MIB object rttmonCtrlAdminStatus to active does not cause the probe to become active. This problem is resolved in Release 12.2(18)SXF5. (CSCin62031)
- When the source MAC address of NAT traffic changes, the corresponding NAT CEF entry is not updated and return traffic is sent to the old MAC address. This problem occurs with static or dynamic NAT. This problem is resolved in Release 12.2(18)SXF5. (CSCsd71047)
- BGP best path never reschedules so that BGP can choose between multiple routes to the same destination. This problem occurs on a BGP configuration that functions in an MPLS VPN environment. This problem is resolved in Release 12.2(18)SXF5. (CSCuk58462)
- A traceback and a reload might occur on a Supervisor Engine 720. This problem occurs because the internal VLAN assigned in the active supervisor engine is not synchronized to the standby supervisor engine. This problem is resolved in Release 12.2(18)SXF5. (CSCsc89229)
- When an IPv6 PIM configuration is acting as the first hop to a source, the SR flag is set after approximately 60 seconds. This situation causes PIM to be disabled on the output interface. This problem is resolved in Release 12.2(18)SXF5. (CSCsc98828)
- When multiple certification authority (CA) trustpoints are specified within a single Internet security authentication key management protocol (ISAKMP) profile, Internet Key Exchange (IKE) tests only the last trustpoint configured. This problem is resolved in Release 12.2(18)SXF5. (CSCef21434)
- Multicast source-only traffic might get dropped when running in bidirectional mode with egress replication. This problem is resolved in Release 12.2(18)SXF5. (CSCsd70494)
- A WS-X6148A-45AF switching module might not initialize correctly when the device is power cycled. When this situation occurs, and you enter the **show module** command, the status that is displayed is unknown. This problem occurs when there are at least eight modules installed in the chassis. This problem is resolved in Release 12.2(18)SXF5. (CSCsd98390)
- Timer expired tracebacks might occur when a system has a large number of RIP neighbors and short update timers configured. This problem is resolved in Release 12.2(18)SXF5. (CSCef17647)
- When you enter the **ipv6 multicast-routing** command and the **no ipv6 multicast-routing** command several times while IPv6 multicast traffic is being processed, a reload might occur. This problem is resolved in Release 12.2(18)SXF5. (CSCej78303)
- A remote-originated LSA received over an OSPF demand circuit may change from DoNotAge to aging when the OSPF process on the far end of the link goes up and down. This problem is resolved in Release 12.2(18)SXF5. (CSCej89011)
- When you enter the **distribute-list interface** command in a global RIP routing context, and the interface that is specified in the command is a VRF interface, the command fails and the following error message appears:

```
% The interface is not in the same VRF as the process
```

You cannot configure another way to filter networks received in updates through a VRF interface because the **distribute-list interface** command is not implemented in the IPv4 VRF address family. This occurs in releases where the fix for CSCee32557 is present.

**Workaround:** Enter the **distribute-list extended-ACL-reference** command in which the source-part of the extended ACL specifies the prefixes and the destination part matches the IP address of the RIP neighbor.

This problem is resolved in Release 12.2(18)SXF5. (CSCeg16631)

- A standby supervisor engine in SSO mode might reload when the configuration on the active supervisor engine is changed over a web connection. This problem occurs when the changed configuration is synchronized on the standby supervisor engine. This problem is resolved in Release 12.2(18)SXF5. (CSCsb16702)
- If you enter the **clear ip device tracking** command several times in succession, a series of BADEVENT tracebacks are displayed. This problem is resolved in Release 12.2(18)SXF5. (CSCsc08857)
- A switchover, and eventually a reload, might occur on a system configured with an IPsec VPN service module or an IPsec SPA that is connected to a third-party VPN client. Watchdog timeouts occur after the switchover, and cause the reload. This problem occurs because of high CPU usage, and reoccurs every 24 hours when the IKE lifetime times out. This problem is resolved in Release 12.2(18)SXF5. (CSCsc71245)
- With compression mode configured, if you enter the **write memory** command when there is approximately 3.1 MB of RAM available, it takes an unexpectedly long time (approximately 2 minutes and 10 seconds) to save the configuration. This problem is resolved in Release 12.2(18)SXF5. (CSCsc97279)
- When a WS-X6502-10GE Ethernet switching module is connected to a WS-X6704-10GE Ethernet switching module, cyclic redundancy check (CRC) errors occur on the WS-X6502-10GE module.

**Workaround:** Enter the **inter-packet gap 6502-mode** interface configuration command on the WS-X6704-10GE interfaces to increase the interpacket gap.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd59975)

- If you enter the **mls rate-limit layer2 pdu** command and then perform an SSO switchover, the supervisor engine stops receiving bridge protocol data unit (BPDU) messages and Cisco Discovery Protocol (CDP) packets. This problem is resolved in Release 12.2(18)SXF5. (CSCsd70948)
- When you unplug a PC from a phone and then plug the PC directly into the switch, or plug the PC into another phone, the new port that the PC is plugged into goes into error disable mode. This problem occurs with a Cisco 7940/60/70 series IP phone and port security on each port. This problem is resolved in Release 12.2(18)SXF5. (CSCsd86340)
- A PIM registered tunnel might be added and removed from (S,G) entries at regular intervals, which causes (S,G) traffic to become ineligible to be switched in hardware. This situation results in a temporary disruption of IPv6 multicast traffic forwarding. This problem is resolved in Release 12.2(18)SXF5. (CSCsd68993)
- When Multicast Listener Discovery (MLD) snooping report-suppression is enabled (default), and a receiver leaves from the (S,G) channel, multicast traffic outage occurs for that (S,G) channel on other receivers, ports in the same VLAN. This outage occurs until the router sends the next periodic MLD general query. This problem is resolved in Release 12.2(18)SXF5. (CSCsd59274)
- Supervisor Engine 32 does not support the **xconnect vfi** command on SVIs. This problem is resolved in Release 12.2(18)SXF5. (CSCse23889)
- With DLSw Ethernet Redundancy configured, circuits might be established through the passive switch. This problem is resolved in Release 12.2(18)SXF5. (CSCse17611)
- The SNMP IF MIB object ifInOctets might have a negative value for a multilink PPP interface. This problem occurs after all of these actions have occurred:
  - The multilink interface goes up and down several times.
  - The member links go up and down several times.
  - A CPE router connected to the multilink interface reloads.

This problem is resolved in Release 12.2(18)SXF5. (CSCsc33562)

- On a system configured with a Supervisor Engine 720, packet loss might occur when you enter the **ip default-network** command, and when MPLS is enabled on the outgoing interface. There is no CEF hardware entry, packets are routed in software and then rate-limited. This problem is resolved in Release 12.2(18)SXF5. (CSCsd28995)
- A bus error and a reload may occur when you enter a command while the command buffer is full of white space. This problem occurs when you enter a partial command, and then you use the tab key while the command buffer is full. This problem is resolved in Release 12.2(18)SXF5. (CSCsd32923)
- An egress class of service (CoS) value might get rewritten when an ingress Internet Printing Protocol (IPP) message is routed as multicast traffic. This problem occurs when the multicast routed traffic is configured with trust CoS on an ingress trunk interface. This problem is resolved in Release 12.2(18)SXF5. (CSCsd94127)
- A reload might occur when SNMP queries the CISCO-SYSLOG-MIB object clogHistoryEntry. This problem is resolved in Release 12.2(18)SXF5. (CSCee24395)
- You might see empty syslog messages immediately after system messages (for example, SYS-3-LOGGER\_FLUSHING, OIR-SP-STDBY-6-CONSOLE). This problem is resolved in Release 12.2(18)SXF5. (CSCsd77751)
- A VPN hub router might reload while terminating IPsec connections when you enter the **clear crypto session remote ip-address** command after the peer at the IP address location has disconnected. The problem occurs only when the remote peer disconnects because of a power off or because of a LAN cable disconnect, and then the peer reconnects with a different public IP address. This problem is resolved in Release 12.2(18)SXF5. (CSCei37299)
- A VACL might not filter RSPAN traffic if there is an active [distributed EtherChannel \(DEC\)](#) on the system. This problem is resolved in Release 12.2(18)SXF5. (CSCse41963)
- Port 2 or port 4 on a [WS-X6816-GBIC](#) switching module might go up and down when port 1 is enabled, not connected, and set to autonegotiate. This problem occurs if a 1000BASE-T GBIC was ever inserted since the last time the module was reloaded. This problem is resolved in Release 12.2(18)SXF5. (CSCse12195)
- For a link configured on a IPsec VPN services module or an IPsec SPA, if the far end of the link is configured to support jumbo frames and to carry a crypto tunnel, and the far end is down when a reload occurs, the link drops jumbo frames through the crypto tunnel. This problem occurs because the MTU of the VPN tunnel is not adjusted properly when the link comes back up. This problem is resolved in Release 12.2(18)SXF5. (CSCsd95279)
- A memory leak might occur on a system configured with an IPsec VPN services module or an IPsec SPA. This problem is resolved in Release 12.2(18)SXF5. (CSCsb29028)
- The ciscoIpMRouteIfInMcastOctets MIB object identifier (OID) counter is a 64-bit counter but functions like a 32-bit counter and resets to zero at a much smaller number than expected. This problem is resolved in Release 12.2(18)SXF5. (CSCsc69155)
- A ROMMON upgrade with corrupted ROMMON NVRAM memory in a flash device might cause a failure of the runtime image to load and cause this message to display:  
  
Warning: Rommon NVRAM area is corrupted. Initialize the area to default values  
Cat6k-Sup720/RP platform with 1048576 Kbytes of main memory  
  
This problem is resolved in Release 12.2(18)SXF5. (CSCek35417)
- When a static ARP entry associated with a VRF interface is deleted, the VRF adjacency is not cleared. Packets sent from the VRF interface continue to use the old destination MAC address. This condition persists until the adjacency is resolved. This problem is resolved in Release 12.2(18)SXF5. (CSCsa76455)

- With a RADIUS authentication server configured, AAA authentication generates unexpected accounting start records, which results in unreliable accounting records. This problem is resolved in Release 12.2(18)SXF5. (CSCsa99158)
- A standby supervisor engine may experience continuous bus errors during initialization after synchronizing with the active supervisor engine. When this problem occurs, the following message is displayed on the standby supervisor engine console:

```
%RP_MLP-4-MISCONFIGLINK: Links across linecards or dCEF disabled, giving control to RP
```

This problem is resolved in Release 12.2(18)SXF5. (CSCsc37902)

- An Easy VPN IPsec tunnel that is configured for RSA may not come up when XAuth is enabled. This problem occurs on a tunnel that is configured between an Easy VPN remote client and an IPsec VPN services module or an IPsec SPA that functions as an Easy VPN server.

**Workaround:** Disable XAuth.

This problem is resolved in Release 12.2(18)SXF5. (CSCed61394)

- The class of service (CoS) VLAN priority value stored in an Ethernet over Multiprotocol Label Switching (EoMPLS) packet may become corrupt when the packet is sent over an EoMPLS tunnel. This problem is resolved in Release 12.2(18)SXF5. (CSCse41480)
- The following message might display when you configure 4 VRFs with 1000 routes each, and then you enter the **clear ip bgp \*** command:

```
%FIB-4-FIBCBLK: Missing cef table for tableid 2829 during Table removal event
```

This problem is resolved in Release 12.2(18)SXF5. (CSCea71711)

- A bus error and a reload might occur when you print queue statistics for priority classes within the same layer of a policy map. This problem occurs when HQoS is supported for Ethernet over an MPLS (EoMPLS) virtual connection. This problem is resolved in Release 12.2(18)SXF5. (CSCec80902)
- When you enter the **maximum-paths ibgp number** command to configure 10-Gigabit Ethernet links and BGP adjacencies, memory corruption and a reload might occur. This problem is resolved in Release 12.2(18)SXF5. (CSCek45564)
- Some UDP packets that have the Terminal Access Controller Access Control System (TACACS) port (49) as their destination might remain suspended in the interface queue. This problem occurs when TACACS+ is configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsb11698)
- When a hardware interface goes down, packets in the egress direction are processed in software. This situation might cause high CPU usage during heavy traffic until routing and CEF updates occur in the routing table. This problem is resolved by setting the default TCAM action to deny processing of egress traffic when the interface is down instead of bridging the traffic. Traffic that is dropped before the routing table updates will generate ICMP unreachable responses to the sender. The lost packets can be retransmitted until the routing tables have been updated. The number of ICMP unreachable messages generated is subject to the current ICMP unreachable rate-limiting configuration. This problem is resolved in Release 12.2(18)SXF5. (CSCsd96511)
- With the Cisco IOS Firewall CBAC feature enabled, if a client opens a connection to a server, which causes a firewall session to be created, and the connection is terminated on both the client and the server, the firewall session may never time out. This problem occurs with applications that use fixed source and destination ports. This problem is resolved in Release 12.2(18)SXF5. (CSCsc72722)

## Resolved General Caveats in Release 12.2(18)SXF4

- The SNMP ifAdminStatus state for the ATM layer or the ATM Adaptation Layer 5 (AAL5) of an ATM interface or subinterface might go down. This situation can occur without entering a **shutdown** command, and prevents SNMP from monitoring the proper status of the ATM interfaces. This problem is resolved in Release 12.2(18)SXF4. (CSCsb12329)
- When a Reverse Path Forwarding (RPF) change affects approximately 30,000 multicast routes, a CPUHOG message might be displayed. This problem is resolved in Release 12.2(18)SXF4. (CSCek26627)
- When the SNMP ifOperStatus MIB object for an interface that is a member of a multilink group is placed in the down state, the ifStackStatus entry that links the interface to the multilink group interface is removed from the IF-MIB. This problem is resolved in Release 12.2(18)SXF4. (CSCeh62084)
- A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability. This vulnerability is present in all versions of Cisco IOS that support the `tcsh` command.

**Workaround:** This advisory with appropriate workarounds is posted at <http://www.cisco.com/warp/public/707/cisco-response-20060125-aatcl.shtml>.

This particular vulnerability only affected Cisco IOS versions 12.3(4)T trains and onwards. (12.3 Mainline is not affected) Please refer to the Advisories “Software Versions and Fixes” table for the first fixed release of Cisco IOS software.

This problem is resolved in Release 12.2(18)SXF4. (CSCsd28570)

- Virtual Router Redundancy Protocol (VRRP) does not function correctly with proxy ARP. The master and backup routers both transmit a proxy ARP reply, and the backup router replies with a burned-in address (BIA) instead of a virtual MAC address. This problem is resolved in Release 12.2(18)SXF4. (CSCsc47919)
- Multinode Load Balancing (MNLB) affinity is installed with an incorrect dispatch address that does not match the Cisco Appliance Server Architecture (CASA) update received by the CASA forward agent. This problem is resolved in Release 12.2(18)SXF4. (CSCsc72066)
- When a Multicast-VPN (MVPN) PE router has two entries of the VPNv4-based multicast distribution tree (MDT) in the VPNv4 BGP table that are reflected by redundant route reflectors (RRs), and the current best VPNv4 MDT is withdrawn by one RR, BGP does not inform Protocol Independent Multicast (PIM) of the presence of the new best VPNv4 MDT. The corresponding (S,G) is pruned immediately and left in the pruned state, and then deleted. This problem is resolved in Release 12.2(18)SXF4. (CSCef35386)
- When using Auto-RP, the PIM Group-to-RP mappings time out when the up time value displayed by the **show ip pim rp mapping** command is less than 30 minutes. This problem occurs when two upstream routers flood Auto-RP discovery messages (group 224.0.1.40) to multiple downstream routers over more than one VLAN, and the downstream routers are leaf routers (such as access switches). This problem is resolved in Release 12.2(18)SXF4. (CSCeh67947)



- A reload might occur when the output of the **show ip pim mdt bgp** command is being displayed. This problem occurs when withdrawals for a MDT source group are received by PIM from BGP and you enter the **show ip pim mdt bgp** command. This problem is resolved in Release 12.2(18)SXF4. (CSCei27448)
- After you enter the **clear arp** command, high CPU utilization might occur and the console might not respond for approximately 30 seconds. This problem occurs on a system configured with many (approximately 2000) static ARP entries. This problem is resolved in Release 12.2(18)SXF4. (CSCsa64947)
- If you use a route map that includes the **set weight** command in the inbound policy, the route map cache for software reconfiguration is not created when a BGP peer is initialized. This problem is resolved in Release 12.2(18)SXF4. (CSCsa68988)
- A reload might occur during BGP convergence when MVPNs are configured. This problem occurs after a duplicate BGP MDT extended community message is received that specifies a different route descriptor (RD) for an MDT that already exists for the specified MDT source and group address. This problem is resolved in Release 12.2(18)SXF4. (CSCsb33258)
- BGP does not advertise all of the routes to a peer that sends a route-refresh request. This symptom is observed under the following conditions:
  - The system is in the process of converging all of its peers and has updates ready in the output queue for the peer.
  - The peer sends a route-refresh request. This may occur when you enter the **clear ip bgp \* soft in** command on the peer or when a VRF is added to the peer.
  - The system processes the route-refresh request from the peer while the system still has updates in the output queue for the peer.

In this situation, all of the prefixes are lost that are advertised by the unsent updates in the output queue for the peer. This problem is resolved in Release 12.2(18)SXF4. (CSCsc59089)

- High CPU usage might occur and the BGP table versions of BGP peers are reset to zero. This problem occurs when you update a complex policy when there is a complex configuration of BGP peers present. This problem is resolved in Release 12.2(18)SXF4. (CSCsc73436)
- When a VRF route is redistributed into the MP-BGP cloud, a routing loop may occur for the prefix that represents the VRF route between the EIGRP cloud and the MP-BGP cloud. This problem occurs on a device that functions as a PE router when the following conditions are present:
  - The router has EIGRP configured on the link to a CE router.
  - The router has a static VRF route that is redistributed into the configuration that is defined by the **address-family vrf vrf-name** command and that is part of the BGP routing process.

This problem is resolved in Release 12.2(18)SXF4. (CSCsc76327)

- On a system configured with MPLS-VPN, some of the sham-links might not come up. This problem is resolved in Release 12.2(18)SXF4. (CSCsd12904)
- When a QoS policy map has more than one priority queue attached to more than one ATM VC or ATM LFI VC, traffic might stop flowing in the priority queues or a reload might occur. This problem is resolved in Release 12.2(18)SXF4. (CSCsd19203)
- The Cisco IOS Authentication, Authorization, and Accounting (AAA) user database connection count might not include a VPN client session that is abnormally terminated and then reconnected. This can cause problems in accuracy when the maximum login value is used to track connected users. This problem is resolved in Release 12.2(18)SXF4. (CSCsc65256)

- SSTP BPDUs that are sent out on trunk ports might have incorrect VLAN ID Type-Length-Values (TLVs) that cause the peer switch to place its ports in a PVID inconsistent state. This problem occurs if the following conditions exist:
  - The spanning tree mode is PVST.
  - Optimized BPDU transmission is enabled. The transmission is enabled when you see “spanning-tree optimize bpdu transmission” in the running configuration.
  - There are one or more trunk ports in the VLAN.
  - VLAN translation is enabled on one or more of the trunk ports.

This problem is resolved in Release 12.2(18)SXF4. (CSCsd02881)

- A reload might occur when a certificate revocation list (CRL) expires that has been downloaded and stored in the local cache. This problem is resolved in Release 12.2(18)SXF4. (CSCsa63387)
- Spurious errors and tracebacks might occur on a system configured with OSPF under heavy traffic. This problem occurs only when MPLS VPNs using OSPF as a PE-CE protocol are configured. This problem is resolved in Release 12.2(18)SXF4. (CSCsd11631)
- SNMPv3 **get** and **set** commands fail after an RPR or an RPR+ switchover. This problem occurs in a system that is configured with RPR or RPR+, and the default value for the SNMP EngineID is still configured. This problem is resolved in Release 12.2(18)SXF4. (CSCsb14936)
- An IPv6 internal Border Gateway Protocol (iBGP) session might not reach the established state across a link with an IPv6 peer. This problem is resolved in Release 12.2(18)SXF4. (CSCed82273)
- A `tcb_isvalid` traceback might occur in the TCP remote shell process for a link from a remote shell (RSH) or a remote copy protocol (RCP) server to an RSH or an RCP client. This problem is resolved in Release 12.2(18)SXF4. (CSCeg61169)
- If you enter the **set ip next-hop in-vrf** command in the import map, routes that were distributed from one VRF instance to another do not appear in the VRF routing table, even though they do appear in the Border Gateway Protocol (BGP) VRF table. This problem is resolved in Release 12.2(18)SXF4. (CSCsc67367)
- During the initialization of a VPN client session, if the Extended Authentication (Xauth) first is successful, and then the session is unsuccessful, the user might be suspended in the local database. This situation can cause problems when the **max-logins** configuration command is used, because a user is included in the count but is no longer active. This problem is resolved in Release 12.2(18)SXF4. (CSCsc91075)

### Resolved General Caveats in Release 12.2(18)SXF3

- When you have MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) routers, a routing loop may occur between the MPLS VPN core and the CEs. This situation occurs if a route is learned from two paths and one path has cost community and the other path does not. This problem is resolved in Release 12.2(18)SXF3 (CSCsa81039)
- For a system configured as an IP HTTP server, tracebacks and a reload might occur during HTTP transactions with URL tokens greater than 128 characters long. A token is a string delimited by slashes in a URL. This problem is resolved in Release 12.2(18)SXF3. (CSCeg62070)
- A memory leak might occur when you enter the **show mls nde** command. The leak will eventually disable Cisco Express Forwarding (CEF). This problem is resolved in Release 12.2(18)SXF3. (CSCsc89044)

- A bus error and a reload might occur on a system configured with Network-Based Application Recognition (NBAR). This problem occurs when Real-Time Protocol (RTP) traffic passes through an Ethernet interface that is configured with a service policy that contains MATCH PROTOCOL RTP AUDIO. This problem is resolved in Release 12.2(18)SXF3. (CSCsb69614)
- A Supervisor Engine 720 configured with a WS-X67xx switching module might experience fabric receive errors on all fabric channels and frequent fabric synchronization errors during the initialization of the module. This problem is resolved in Release 12.2(18)SXF3. (CSCsc55949, CSCsd20092)
- EIGRP-specific Extended Communities might be corrupted and shown as 0x0:0:0 when EIGRP-specific Extended Community 0x8800 is received over an IPv4 EBGp session. This problem is resolved in Release 12.2(18)SXF3. (CSCec12299)
- A “no such instance” SNMP exception might be returned for an SNMP **get** request if DFC modules are installed. This problem is resolved in Release 12.2(18)SXF3. (CSCsc39902)
- MAC addresses are not flushed when an associated permanent virtual circuit (PVC) goes down. This problem is resolved in Release 12.2(18)SXF3 (CSCsd01885)

### Resolved General Caveats in Release 12.2(18)SXF2

- With both WCCP and NDE configured, you might see numerous tracebacks caused by alignment errors and CPU utilization might be unacceptably high. This problem is resolved in Release 12.2(18)SXF2. (CSCsb21972)
- DLSw circuits are established over the same peer connection when DLSw load balancing is configured and when there are multiple peers that have the **dls w icanreach mac-address mac\_addr** command enabled with the same remote MAC address for the *mac\_addr* argument. This problem is resolved in Release 12.2(18)SXF2. (CSCsa45750)
- When you enter the reload command, the following message is displayed:

```
Error in setting Reload Reason
```

This problem is resolved in Release 12.2(18)SXF2. (CSCei92291)

- If you configure fallback bridging on a Supervisor Engine 32, multicast data packets loop and are duplicated within the bridge-group endlessly. This problem is resolved in Release 12.2(18)SXF2. (CSCei46182)
- A reload might occur when a standby supervisor engine is inserted. This problem occurs with the following conditions: SNMP MIB notifications are enabled, the notification log is configured, and the redundancy mode SSO is configured. This problem is resolved in Release 12.2(18)SXF2. (CSCej08355)
- Occasionally in an IGMP multicast configuration, the PFC or DFC FIFO stops processing, and this message is displayed:

```
EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
```

This problem is resolved in Release 12.2(18)SXF2. (CSCej21698)

- Duplicate interface index numbers might be assigned to tunnel interfaces when Protocol Independent Multicast (PIM) and multicast distribution tree (MDT) tunnels are created. These duplicate interface index numbers might prevent traffic from being forwarded from these multicast interfaces. This situation might cause a bus error and a reload when these tunnels are deleted and recreated. This problem is resolved in Release 12.2(18)SXF2. (CSCei80699)

- The **clear ip bgp update-group** [*index-group* | *ip-address*] command clears all the Border Gateway Protocol (BGP) peers, including members of other update groups. This problem is resolved in Release 12.2(18)SXF2. (CSCsb24535)
- A reload might occur after upgrading the Erasable Programmable Logic Device (EPLD) image file on a WS-X6548-GE-TX module in accordance with Field Notice: FN - 29407. The reload also causes the EPLD upgrade to fail. This problem is resolved in Release 12.2(18)SXF2. (CSCsb49326)
- With Cisco IOS SLB and VRF configured, when traffic is fragmented, if a trailing fragment arrives before the leading fragment within a VRF, the trailing fragment is dropped by the supervisor engine. This problem occurs with Cisco IOS SLB enabled. This problem is resolved in Release 12.2(18)SXF2. (CSCsb70996)
- If a service module is installed instead of a redundant supervisor engine, and you change the redundancy mode, this message displays continuously, and then eventually the service module reloads:

```
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsc03429)

- In certain LAN topologies, the PIM assert mechanism can cause an upstream router to erroneously remove downstream interfaces from output interface lists. When this situation occurs, it causes multicast traffic to be dropped. This problem occurs when two or more upstream routers with routes to the same rendezvous point or traffic source are connected to the same LAN segment as two different downstream routers. The problem occurs when the two downstream routers select different upstream routers as their next hop. This problem is resolved in Release 12.2(18)SXF2. (CSCeh17756)
- After an SSO switchover, some SPAN destination ports of RSPAN sessions might stop monitoring traffic. This problem is resolved in Release 12.2(18)SXF2. (CSCsb34213)
- If you enter the **channel-group** command or the **pri-group** command issued in a T1/E1 interface controller mode or a similar configuration to create interfaces, and then you enter the **channel-group** command or the **pri-group** command to unconfigure or reconfigure these interfaces, a Network Time Protocol (NTP) server receiving NTP requests through these interfaces will stop synchronizing with a NTP client. When this problem occurs, the NTP application stops functioning instead of changing interfaces and maintaining synchronization. This problem is resolved in Release 12.2(18)SXF2. (CSCeh48548)
- The global IP address instead of the IP address of the VPN of the egress PE router is displayed in a traceroute VRF. This problem occurs under the following conditions:
  - The egress PE router is configured with a Supervisor Engine 720.
  - The **mls qos** command is configured on the egress PE router.
  - A service policy is configured on the egress PE router.
  - The **no mpls ip propagate-ttl** command is configured on the ingress PE router.
  - The outgoing label on the egress PE router is an aggregate label.

The problem also occurs under these conditions:

  - The egress PE router is configured with Supervisor Engine 720.
  - The **no mpls ip propagate-ttl** command is configured on the ingress PE router.

- The outgoing label on the egress PE router is an aggregate label.
- Recirculation of MPLS packets with an aggregate label is turned on (using the **mls mpls recir-agg** command).

This problem is resolved in Release 12.2(18)SXF2. (CSCsb80866)

- Egress multicast replication traffic for an outgoing interface (OIF) might be dropped. The supervisor engine generates this replication traffic to synchronize its copy of the multicast expansion table (MET) with the copy on a DFC. If this replication traffic is dropped, it is never resent and the synchronization is never attempted again. This problem is resolved in Release 12.2(18)SXF2. (CSCsb67152)
- CPUHOG messages might be displayed if PIM snooping is enabled on several VLANs. This problem is resolved in Release 12.2(18)SXF2. (CSCsc26048)
- A standby supervisor engine in SSO mode might reload. This problem occurs when SNMP fills a data structure, and overwrites a byte of memory after the data structure. This problem is resolved in Release 12.2(18)SXF2. (CSCsc07793)
- In a Gateway Load Balancing Protocol (GLBP) configuration, when the static router address for a SVI is configured on two different Layer 2 addresses for dual ASICs on the same forwarding card, the MAC address for one of the ASICs is not removed from the forwarding table if you enter the **shutdown** command on this SVI. The forwarding cards that feature dual ASICs are the WS-F6700-DFC3A, WS-F6700-DFC3B and the WS-F6700-DFC3BXL. This problem is resolved in Release 12.2(18)SXF2. (CSCsc26490)
- When a system is configured with a new OSPF area, the links that are configured for traffic engineering are not flooded in the new area. This problem occurs when you configure an area using entering the **mpls traffic-eng area number** command as part of the router open shortest path first (OSPF) configuration. This problem is resolved in Release 12.2(18)SXF2. (CSCeh51720)
- When the cpim MIB object family in the CISCO-PIM-MIB is queried with an SNMP walk, the output of MIB entry **cpimLastErrorRP** is truncated. This problem is resolved in Release 12.2(18)SXF2. (CSCef65806)
- Data Link Switching (DLSw) circuits might not connect using DLSw Ethernet redundancy. This problem occurs when DLSw Ethernet redundancy is configured with the following commands where the *local-mac* and *remote-mac* values are the same real MAC addresses of the remote host:
  - **dls transparent switch-support**
  - **dls transparent map local-mac local-mac**
  - **remote-mac remote-mac**

If both DLSw routers are rebooted, clients can immediately establish a session with the remote host through one of these DLSw routers using the real MAC address. This real circuit is outside of Ethernet redundancy, and until the circuit is disconnected, Ethernet redundancy cannot be established. This problem is resolved in Release 12.2(18)SXF2. (CSCeh18295)

- When you enter the **reload** command, the following message is displayed:

```
Error in setting Reload Reason
```

This problem is resolved in Release 12.2(18)SXF2. (CSCei92291)

- If multiple WS-X6748-GE-TX ports have port security configured and are sending a high rate of traffic to hundreds of MAC addresses, not all of the MAC addresses are learned and secure. After a reload, traffic is dropped for MAC addresses that have not been learned properly. This problem is resolved in Release 12.2(18)SXF2. (CSCeh78028)

- A router that is configured with thousands of RIP routes might reload when multiple links go down and up. This problem is resolved in Release 12.2(18)SXF2. (CSCdv07156)
- RIPv2 routes do not age out or flush in the routing table after you shut down an ATM interface. However, these routes correctly flush from the RIP database. This problem is resolved in Release 12.2(18)SXF2. (CSCeg12616)
- DLSw load balancing using the circuit-count configuration does not distribute circuits evenly. This problem occurs when all the circuits attempt to connect at the same time. Configure the **dls w load-balance round-robin** command initially, start DLSw, and then configure using **dls w load-balance circuit-count**. This problem is resolved in Release 12.2(18)SXF2. (CSCeh18390)
- When Network Address Translation (NAT) is configured, TCP translations do not time out properly when the TCP session is closed in a normal way.

**Workaround:** Lower the global NAT translation timeout period using the **ip nat translation tcp-timeout seconds** command.

This problem is resolved in Release 12.2(18)SXF2. (CSCsa51150)

- An OSPF opaque link state advertisement (LSA) may not be advertised after an MPLS-TE-enabled interface goes down and up or after a system reboot. This problem is resolved in Release 12.2(18)SXF2. (CSCsa62908)
- If you send an SNMP query for IF-MIB information of paths to VLANs that are unroutable, the query might not complete. Also, if you enter the **show vlan counter** command, the prompt may not appear. This problem is resolved in Release 12.2(18)SXF2. (CSCsb18498)
- A system might drop Rx SPAN packets when there is an outbound ACL applied on the source interface of the SPAN session. This problem is resolved in Release 12.2(18)SXF2. (CSCsb21148)
- When you enable the **logging event link-status default** command in the global configuration and the **no logging event link-status** command is configured at the interface level, the link up and down events are still logged. This situation has no affect on the performance of the switch, and should only result in the following message being logged for all interfaces on the switch regardless of how the logging link status is configured on the interface:

```
*Aug 19 14:58:52 UTC: %LINK-SP-5-CHANGED: Interface FastEthernet1/3, changed state to
administratively down
*Aug 19 14:58:52 UTC: %LINEPROTO-SP-5-UPDOWN: Line protocol on Interface
FastEthernet1/3, changed state to down
*Aug 19 14:58:53 UTC: %LINK-SP-3-UPDOWN: Interface FastEthernet1/3, changed state to
down
*Aug 19 14:58:55 UTC: %LINK-SP-3-UPDOWN: Interface FastEthernet1/3, changed state to
up
*Aug 19 14:58:55 UTC: %LINEPROTO-SP-5-UPDOWN: Line protocol on Interface
FastEthernet1/3, changed state to up
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsb66248)

- SNMP AuthenticationFailure traps are being sent out with a source IP address of 0.0.0.0. This problem is resolved in Release 12.2(18)SXF2. (CSCsb67916)
- A reload might occur because of a memory corruption or a CPUHOG condition. This problem occurs in a configuration with a large LSA with 64 parallel links that have OSPFv3 enabled in broadcast mode and when all the links with a neighbor router go up and down. This problem is resolved in Release 12.2(18)SXF2. (CSCsb74588)
- A missing global label in the ternary content addressable memory (TCAM) table causes user internet access traffic to be dropped on a provider edge (PE) interface. This problem occurs if there are multiple paths to a next hop router in a MPLS VPN network for customer internet access using a global keyword. This problem is resolved in Release 12.2(18)SXF2. (CSCsb76540)

- After an NSF with SSO switchover, you might see the following message:

```
00:31:29: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 55BE2914 time 0x1CD561
(00:00:00 ago).
```

This problem occurs when several switching modules send IPC hello messages at the same time. This problem is resolved in Release 12.2(18)SXF2. (CSCsb83521)

- The **path-mtu-discovery** command is not supported on a GRE tunnel that is accelerated by a VPNISM or an IPsec SPA. This problem is resolved in Release 12.2(18)SXF2. (CSCea38318)
- With a Supervisor Engine 2, some flows might not get exported through NetFlow Data Export (NDE). This problem occurs when a MAC address, that is used for direct export becomes stale because of new MACs that become associated with interfaces when you enter the **mac-address** command. Only the flows created on the PFC are affected. This problem is resolved in Release 12.2(18)SXF2. (CSCei86937)
- If the software accesses an ARP table that is corrupted, a bus error and a reload might occur. The ARP table gets corrupted when a process accessing the table is suspended and then resumed. This problem is resolved in Release 12.2(18)SXF2. (CSCea34586)
- The SNMP monitor application constantly sends messages indicating that the ifOperStatus of the control plane interface is down. This situation occurs because the control plane interface does not support SNMP. To prevent these messages, the control plane interface has been removed from the list of interfaces in the MIB database. This problem is resolved in Release 12.2(18)SXF2. (CSCej57810)
- A message sent to add an SFP entity into the ENTITY-MIB tree sometimes is not processed. Because the SFP entity has not been added to the ENTITY-MIB tree, the SFP entity will not be displayed when you enter the **show inventory** command. This problem is resolved in Release 12.2(18)SXF2. (CSCsc05500)
- Internet Key Exchange (IKE) security associations (SAs) are not replicated to the standby supervisor engine. This problem is resolved in Release 12.2(18)SXF2. (CSCsc59207)
- The achieved bandwidth of policed egress Ethernet over Multiprotocol Label Switching (EoMPLS) traffic is much lower than the policing value when there is also ingress EoMPLS traffic on the same port whose destination is not the source MAC address of the egress EoMPLS traffic. This problem is resolved in Release 12.2(18)SXF2. (CSCsc13720)
- An OSPF autonomous system boundary router (ASBR) configured with the **area area-id nssa default-information originate** command might continue to advertise a default route on an not-so-stubby area (NSSA) even after the default BGP route has been withdrawn and removed from the routing table. This problem is resolved in Release 12.2(18)SXF2. (CSCsc03828)
- A reload might occur with memory corruption when a SPAN session is removed from service modules. This problem does not occur when the SPAN session is removed from all service modules configured on the system at once. This problem occurs when you enter the **no monitor session servicemodule module 3-4** command and slots 3 and 4 were occupied by Firewall Service Modules. This problem is resolved in Release 12.2(18)SXF2. (CSCsc06620)
- BGP updategroup selection for peers that are in nonprivate autonomous systems that use the remove-private-as features, needs to be improved to optimize convergence time and flexibility of neighbor configuration. This problem is resolved in Release 12.2(18)SXF2. (CSCei53226)
- Port Address Translation (PAT) with overload traffic might be routed in software. This problem is resolved in Release 12.2(18)SXF2. (CSCsc18728)
- Cisco IOS SLB does not support code 50 messages. This problem is resolved in Release 12.2(18)SXF2. (CSCsc08602)

- A TCP session fails to time out because it is suspended in the FINWAIT1 state. The following message is displayed:

```
%TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
```

This problem occurs in a BGP configuration that is connected to a non-Cisco router after the BGP authentication password has been changed. This problem is resolved in Release 12.2(18)SXF2. (CSCsb51019)

- A memory leak occurs on a Supervisor Engine 720 when a console session is opened. This problem is resolved in Release 12.2(18)SXF2. (CSCsc08741)
- When a parallel link comes up between two routers running OSPF that have iSPF enabled, routes may not be installed over this new added parallel link. This problem is resolved in Release 12.2(18)SXF2. (CSCsa79783)
- IP multicast streams can be interrupted when IGMP snooping receives an IGMP leave for a group while another leave from the same group and from the same port is already being processed. This problem is resolved in Release 12.2(18)SXF2. (CSCsc32198)
- A memory leak might occur on a system configured with an IPsec VPNM or an IPsec SPA. A large memory leak might occur on an aggregator or a hub for a large number of spokes, or in configurations where Dead Peer Detections (DPDs) are enabled and the IPsec SA lifetime is a small value (for example, 120 seconds). This problem is resolved in Release 12.2(18)SXF2. (CSCsc52105)
- In a redundant topology with SONET controllers present and configured with Multi-router automatic protection switching (APS), while protection is active, an SSO switchover might cause an inconsistent state for a packet-over-SONET (POS) APS interface. When you enter the **show aps** command, the status for the interface changes from inactive on the slave to interface down after the switchover. This problem is resolved in Release 12.2(18)SXF2. (CSCin46297)
- A loopback interface in a VRF cannot be routed when there is a nonhost static route pointing to the loopback interface in the global routing table. This problem occurs in a VRF-lite configuration. This problem is resolved in Release 12.2(18)SXF2. (CSCsc50692)
- A system configured with an IPsec VPNM or an IPsec SPA might reload when GRE and IPsec fragmentation occur on the same packet. This problem occurs when 1,000 packets that are the appropriate size are transmitted with the MTU size set to require both GRE and IPsec fragmentation. This problem is resolved in Release 12.2(18)SXF2. (CSCek03772)
- CPU utilization might be high when an existing ARP entry that was learned on an MPLS-enabled interface is updated. This problem occurs if the IP address for that interface is also currently being used with a different ARP entry, for an adjacency pointer. This problem is resolved in Release 12.2(18)SXF2. (CSCsb16512)
- When querying the cbQosCMStatsTable of the CISCO-CLASS-BASED-QOS-MIB, values returned for byte and bit rate statistics are always zero. The output of the **show policy-map interface** command indicates that these statistics are not zero. This problem occurs on FlexWAN, Enhanced FlexWAN and SPA port adapters. This problem is resolved in Release 12.2(18)SXF2. (CSCsc04015)
- When multicast packets are sent through a VPN service module or an IPsec SPA, the multicast packet counters increment but the downstream router does not receive most of the packets. This problem is resolved in Release 12.2(18)SXF2. (CSCsb68513)
- IEEE 802.1X authenticated ports might lose the authenticated state when an SSO switchover occurs. Traffic is disrupted while the ports are reauthenticated. This problem is resolved in Release 12.2(18)SXF2. (CSCsc09557)



- NetFlow Data Export (NDE) is not exporting all the flow records. The number of flows per second reported by the NetFlow collector is much lower than the actual traffic. This problem is resolved in Release 12.2(18)SXF2. (CSCsa79630)
- With Frame Relay local switching configured on a FlexWAN, an Enhanced FlexWAN, or a SIP interface, when the DLCI becomes inactive or active on one of the local-switching configured interfaces, a second local-switching configured interface might go up and down. This problem occurs when the WAN interface is configured as data terminal equipment (DTE). This problem is resolved in Release 12.2(18)SXF2. (CSCsc31921)
- A system configured with a WS-X6748-SFP or a WS-X6724-SFP switching module and copper SFPs might display the following message during initialization:

```
%SYS-CFC1-3-CPUHOG: Task is running for (4000)msecs, more than (2000)msecs
(1/0),process = fw_lcp process.
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsc59332)

- A reload might occur when a system regenerates SSH RSA keys under low memory conditions. This problem is resolved in Release 12.2(18)SXF2. (CSCee32606)
- When you insert a WS-X6148-FE-SFP switching module into a chassis, SNMP populates the CISCO-STACK-MIB PortTable MIB object with an invalid e100baseEmpty port type. This problem is resolved in Release 12.2(18)SXF2. (CSCsb93068)
- If Auto-RP is configured on redundant supervisor engines, a switchover to the standby supervisor engine while multicast traffic is flowing over a few hundred multicast routes might result in a series of CPU Hog messages and tracebacks. A reload occurs eventually because of prolonged memory utilization. This problem is resolved in Release 12.2(18)SXF2. (CSCsb60206)
- A configuration is not saved when you enter the **do write memory** command from configuration mode, change the running configuration, exit the configuration mode, and then do a reload. This problem is resolved in Release 12.2(18)SXF2. (CSCsb89834)
- A system configured with EIGRP might experience a memory leak in the EIGRP Work Ent process. This process ID name is actually EIGRP Work Entry, but it is truncated by nearby data entries that are very large and corrupt the ID string. You can use the **show process memory** command to display the process ID names and determine if this problem has occurred. This problem is resolved in Release 12.2(18)SXF2. (CSCsa99924)
- Simultaneously reading Advanced Technology Attachment (ATA) file directory entries from different processes (example, two vty sessions) might cause data corruption. This problem is resolved in Release 12.2(18)SXF2. (CSCej42935)
- When you enter the **no mls ip slb search icmp** command, ICMP packets that are not destined for a vserver IP address are still handled by Cisco IOS SLB in the MSFC. These packets should be hardware switched. This problem is resolved in Release 12.2(18)SXF2. (CSCsb80141)
- Some ATM PVCs that are marked for deletion might not be deleted. This problem is resolved in Release 12.2(18)SXF2. (CSCsc62474)
- When SNMP traps are generated, the **show alignment** command displays spurious memory access and tracebacks. This problem is resolved in Release 12.2(18)SXF2. (CSCsa53394)
- Some vendors might generate LSAs with a mix of ones and zeros for the LSA ID when they advertise OSPF external routes with the same network address but a different network mask. These LSA IDs are not recognized by Cisco IOS software. This problem is resolved in Release 12.2(18)SXF2. (CSCei65553)
- On a Supervisor Engine 32, Spanning Tree Protocol (STP) does not work for ATM and Frame Relay interfaces configured for bridging. This problem is resolved in Release 12.2(18)SXF2. (CSCsc33110)

- A system configured with multiple spanning tree (MST) might not start a topology change for the MST instances when that topology change is the result of a boundary port changing to the forwarding state. As a result, some of the CAM entries for the VLANs mapped to the MST instances may be incorrect, and they might prevent traffic from forwarding until they are updated by traffic or aged out. This problem is resolved in Release 12.2(18)SXF2. (CSCsc39939)
- A reload might occur when there is heavy traffic on an IPsec SPA or VPN SM configured with IKE Dead Peer Detection (DPD). This problem is resolved in Release 12.2(18)SXF2. (CSCee86692)
- A reload might occur when two or more Telnet or console sessions are open and the following events occur:
  - In one session, you enter the **show ip as-path-access-list acl-number** command, and the output pauses at the --more-- prompt when there is more than one page output.
  - In another session, you enter the **no ip as-path access-list acl-number** command and use the same *acl-number* argument in the **show ip as-path-access-list acl-number** command.
  - In the first session, you type in **enter** or **space** in the first session to display the rest of the **show** command output.

This problem is resolved in Release 12.2(18)SXF2. (CSCec75641)

- A system configured with IPsec stateful failover with a large number of Internet Key Exchange (IKE) security associations (SAs) might reload because of memory corruption. The crashinfo file might display the following messages:

```
%SYS-3-BADFREEPTRS:
%SYS-6-BLKINFO: Corrupted previous pointer in next of freed block
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsc94266)

- On a Supervisor Engine 720 configured with a PCMCIA Compact Flash Memory device, if you attempt to write a crashinfo file to the PCMCIA, a reload could occur. You can configure the PCMCIA to collect the crashinfo file; it will also be used if the bootflash is full. This problem is resolved in Release 12.2(18)SXF2. (CSCeh44660)
- If you enter the **ip mtu** interface configuration command to set the maximum transmission unit (MTU) size of the IP packets on an IPsec tunnel interface, entering the **no ip mtu** interface configuration command does not restore the default value. This problem is resolved in Release 12.2(18)SXF2. (CSCei60249)
- A reload might occur when a marking input policy is attached to an Enhanced FlexWAN POS interface and an output policy is attached to a SPA. The reload occurs when traffic is ingressing on the Enhanced FlexWAN interface and egressing on the SPA. This problem is resolved in Release 12.2(18)SXF2. (CSCej77367)
- A Supervisor Engine 720 that is configured as a Cisco IOS server load balancing (SLB) server with Hot Standby Router Protocol (HSRP) and uses MPLS to communicate with another Cisco IOS SLB server, might display the following message and then reload after an HSRP switchover:

```
Nov  4 05:53:49: %IP-3-LOOPPAK: Looping packet detected and dropped -
src=, dst=, hl=4261816683, tl=1684290561, prot=0, sport=37374, dport=251
in=, nexthop=, out=
options=Vlan1300
-Process= "IP Input", ipl= 0, pid= 122
-Traceback= 4078490C
%ALIGN-1-FATAL: Corrupted program counter
pc=0x31203041, ra=0x31203041, sp=0x520F13F8
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsc40027)

- A segmentation violation error might cause a reload during an NSF with SSO redundancy mode switchover. This problem is resolved in Release 12.2(18)SXF2. (CSCsb93316)
- PIM snooping does not populate the MAC address table with all the PIM neighbors because Auto-RP packets are not received from these neighbors. This problem is resolved in Release 12.2(18)SXF2. (CSCsc30532)
- When an MWAM service module or an OSM is installed, a reload might occur in a low memory configuration or when allocating a large amount of memory. This problem is resolved in Release 12.2(18)SXF2. (CSCef11195)
- A system might drop a TCP connection when there is high traffic. This situation occurs when the remote end of a TCP connection is oversubscribed with a high traffic rate, the remote end advertises a zero window. When the remote end processes some data, the window re-opens and the new window is advertised. If the transmitter has buffered data to send to the receiving device, the system might drop the TCP connection. This problem is resolved in Release 12.2(18)SXF2. (CSCsc39357)
- A reload occurs when configuring an ATM multipoint subinterface and an ATM PVC discovery is enabled on that subinterface. This problem occurs when you have already configured some ATM subinterfaces and you have already enabled ATM PVC discovery on these interfaces. This problem is resolved in Release 12.2(18)SXF2. (CSCsc49134)
- Multicast networks running PIM sparse mode might experience high CPU utilization and instabilities with a multicast group count of approximately 10,000 members, if all multicast routes are traversing the same interface. This problem will most likely occur during physical or logical topology change events. This problem is resolved in Release 12.2(18)SXF2. (CSCsc76666)
- When RIP is configured with MD5 interface authentication, the received packets always fail the authentication check. This problem is resolved in Release 12.2(18)SXF2. (CSCsb79895)
- If you enter the **ip default-network** command, the **show ip route** command does not display the default gateway. This problem is resolved in Release 12.2(18)SXF2. (CSCed87897)
- A (\*,G) prune is not processed on a nondesignated router when there is a link (link A) to a PIM neighbor and a backup router that has a link (link B) to another PIM neighbor. When you shut down link A and bring up link B, the outgoing interface list (OIL) of the DR router is Null on (S,G) but on its PIM neighbor, the OIL on (S, G) still points to link A. PIM does not prune link A for 3 minutes. This problem is resolved in Release 12.2(18)SXF2. (CSCsb61487)
- Power may be incorrectly applied to the wrong port of a WS-X6148-21AF or a switching module equipped with a PoE daughter card, when the module is reset. A device that cannot tolerate inline power might get damaged if you plug it into this port. This problem is resolved in Release 12.2(18)SXF2. (CSCsc92114)
- After an NSF with SSO switchover, this message might display:  

```
FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Loopback0 with illegal
if_number: 0
```

This problem is resolved in Release 12.2(18)SXF2. (CSCei77396)
- Members of a BGP update group might have different versions of BGP tables, which could prevent BGP from removing networks that do not have a path. This problem is resolved in Release 12.2(18)SXF2. (CSCsb09852)
- If SNMP sets an ERSPAN crcERSpanIFTable MIB object entry to not-in-service, and the status does not change for 50 minutes, a memory corruption occurs. This problem is resolved in Release 12.2(18)SXF2. (CSCej87462)
- A serial interface might remain configured in an MFR bundle link after the serial interface has been removed. This problem is resolved in Release 12.2(18)SXF2. (CSCsb67941)

- A bus error and a reload might occur on a system configured with SNMP views. This problem occurs if the views are being polled by SNMP while they are being changed or updated, which happens when the running configuration is updated. This problem is resolved in Release 12.2(18)SXF2. (CSCsc82214)
- In a topology with multiple multicast forwarding devices sharing the same physical medium, if one of the forwarding devices reloads, then a Catalyst 6500 switch or a Cisco 7600 router acting as the other forwarding device might fail to forward some traffic. This problem is resolved in Release 12.2(18)SXF2. (CSCei13579)
- A PA-A3 or PA-A6 port adapter in an Enhanced FlexWAN module, or an ATM SPA might not initialize correctly after a reload if it is configured for bridging using RFC1483 bridged routed encapsulation (BRE). The BRE Local Target Logic (LTL) is not populated properly and traffic does not pass from Ethernet to ATM on the BRE connection. This problem is resolved in Release 12.2(18)SXF2. (CSCsb89241)
- The **no mls qos mpls trust exp** command does not work after a reload. This problem is resolved in Release 12.2(18)SXF2. (CSCsc93283)
- A reload might occur when you remove a service policy after you enter the **mls qos mpls trust exp** command and then you enter the **no mls qos mpls trust exp** command. This problem is resolved in Release 12.2(18)SXF2. (CSCsc93607)

#### Resolved General Caveats in Release 12.2(18)SXF1

- A reload might occur with a breakpoint exception (signal=5). This problem can occur in any release that contains the fix for CSCee28288 when a 32-bit counter continues to increment until it wraps around to 0. In most cases approximately 40 to 50 weeks of continuous uptime elapses before this problem is observed. This problem is resolved in Release 12.2(18)SXF1. (CSCsb98702)
- When a statically mapped rendezvous point is defined as an interface address and the interface is in the down/down state, the router can still attempt to become the rendezvous point for the defined groups. This problem occurs when the interface that reached the down/down state was not administratively brought down (for example, a cable was unplugged). This problem is resolved in Release 12.2(18)SXF1. (CSCsb64585)
- A Supervisor Engine 720 may reload when two simultaneous **write memory** commands from two different VTY sessions are executed. Messages similar to the following may appear in the crashinfo file:

```
validblock_diagnose, code = 10
current memory block, bp = 0x48FCC7D8,
memory pool type is Processor
data check, ptr = 0x48FCC808
next memory block, bp = 0x491AC060,
memory pool type is Processor
data check, ptr = 0x491AC090
previous memory block, bp = 0x48FCBBE8,
memory pool type is Processor
data check, ptr = 0x48FCBC18
```

This problem is resolved in Release 12.2(18)SXF1. (CSCeb05456)

- The following message might display after an SSO switchover before all the retries have completed:  
%IPFAST-DFC2-4-FASTPORTOPENWARN: Attempt to open FIB Master: DFS.process\_level.msgs failed. Will be retried 60 times (last error:no such port)

This problem is resolved in Release 12.2(18)SXF1. (CSCsb85748)

## Resolved General Caveats in Release 12.2(18)SXF

- The Multiprotocol Border Gateway Protocol (MP-BGP) network entries counter increases above the actual number of reachable networks.

This problem occurs in a nonconverged environment. The correct number of network entries is restored when there is a period of BGP stability that lasts for approximately 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is continuous churning and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the actual number of reachable networks. This problem is resolved in Release 12.2(18)SXF. (CSCeh16989)

- Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

This problem is resolved in Release 12.2(18)SXF. (CSCeh73049)

- Multiple Cisco products contain vulnerabilities in the processing of IPsec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPsec and can be repeatedly exploited to produce a denial of service.

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

This advisory is posted at

<http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml>.

This problem is resolved in Release 12.2(18)SXF. (CSCed94829)

- A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

**Workaround:** Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL). By doing this, the offending router will not be able to participate within the mVPN data trees.

The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a rACL:

```
!
ip receive access-list 111
!
access-list 111 deny udp host <ip address of router sending malformed join
request> host 224.0.0.13 eq 3232
access-list 111 permit ip any any
!
```

**Note**

Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to “Protecting Your Core: Infrastructure Protection Access Control Lists” at:

<http://www.cisco.com/warp/public/707/racl.html>

This problem is resolved in Release 12.2(18)SXF. (CSCsb52717)

- With a Supervisor Engine 720 and DFC3A-equipped switching modules, a memory allocation failure and reload might occur if you configure SPAN. This problem is resolved in Release 12.2(18)SXF. (CSCei20107)
- If you configure the QoS policing violate action to be the same as the exceed action, after a reload, the violate action is drop instead of the configured action. This problem is resolved in Release 12.2(18)SXF. (CSCsa87178)
- The **clear bgp ipv4 unicast \*** command clears IPv4 BGP peers from the routing table, but does not clear BGP routes from the routing table. The **clear bgp ipv6 unicast \*** command clears IPv6 BGP peers from the routing table, but does not clear BGP routes from the routing table. This problem is resolved in Release 12.2(18)SXF. (CSCsa87034)
- In rare situations, a reload might occur if you make QoS configuration changes to a range of interfaces when a large QoS policy that has 63 microflow policers is attached to the interfaces. This problem is resolved in Release 12.2(18)SXF. (CSCsa57222)
- SNMP polling of the IPsec MIBS (ciscoIPsecMIB, ciscoIpSecFlowMonitorMIB, and ciscoIpSecPolMapMIB) results in memory being held indefinitely by the device. This problem is resolved in Release 12.2(18)SXF. (CSCec64333)
- When a protected interface comes up and a new label switch path (LSP) is generated, a ‘Path Tear’ message may be ignored for an old LSP at a merge point. As a result, the LSP is not torn down. This problem is resolved in Release 12.2(18)SXF. (CSCea64025)
- With many configured tunnels, the output from the **debug ip rsvp resv** privileged EXEC command might be excessive and cause an indefinite pause or a reload. This problem is resolved in Release 12.2(18)SXF. (CSCeb60432)
- In a system with redundant supervisor engines, if you modify the configuration file on the active supervisor engine, these changes may not be saved in the configuration file for the standby supervisor engine. This problem is resolved in Release 12.2(18)SXF. (CSCeb70508)
- The **ip radius source-interface subinterface-name vrf vrf-name** command forces the IP address of a specified interface to be used for all outgoing Remote Authentication Dial In User Service (RADIUS) packets on a per-VRF basis. This command has no effect in certain configurations. In these cases, packets are forwarded through the global **ip radius source-interface**. If no interface is configured, packets are forwarded through the interface IP address that points to the RADIUS server. This problem is resolved in Release 12.2(18)SXF. (CSCec21537)
- RADIUS packets use the outgoing interface's physical address as the RADIUS packet source instead of the interface configured by software commands. This problem is resolved in Release 12.2(18)SXF. (CSCec72111)

- MPLS FRR LSPs may fail to provide protection with a next-next hop (NNHOP) backup tunnel. This symptom occurs only when a primary LSP reaches beyond a merge point. This problem is resolved in Release 12.2(18)SXF. (CSCed75295)
- A Simple Network Management Protocol (SNMP) request sent to a VPN routing and forwarding (VRF) instance uses the wrong source address in the reply. This problem is resolved in Release 12.2(18)SXF. (CSCee92763)
- RSVP ResvConfirm messages are dropped when two parallel equal cost links to MPLS destinations are present. This problem is resolved in Release 12.2(18)SXF. (CSCef32588)
- When an EXEC session is at the “More” prompt, the session fails to time out. This problem is resolved in Release 12.2(18)SXF. (CSCef35192)
- Cisco Express Forwarding (CEF) may not be correctly updated with a route change when the route type changes from interior Border Gateway Protocol (iBGP) to exterior Border Gateway Protocol (eBGP) or vice versa. This symptom occurs when running IPv6 BGP. This problem is resolved in Release 12.2(18)SXF. (CSCef61721)
- On a system with source-route translational bridging (SR/TLB) configured, all pings fail when an ATM-DXI encapsulation is in use. This problem is resolved in Release 12.2(18)SXF. (CSCef71011)
- A redundant MSFC might reload with the following error message when you reload the active supervisor engine:

```
%RSP-3-IPC: slave could not create named port port in use
```

This problem is resolved in Release 12.2(18)SXF. (CSCef78145)

- An interface configured with routed sub-interfaces and 802.1Q encapsulation does not receive Cisco Discovery Protocol (CDP) packets if the native VLAN is configured as other than VLAN1. This problem is resolved in Release 12.2(18)SXF. (CSCeg02753)
- The memory leak might occur on a BGP router configured to redistribute into Enhanced Interior Gateway Routing Protocol (EIGRP) that has no network statement. This problem is resolved in Release 12.2(18)SXF. (CSCeg06612)
- Packet drops occur in the ingress direction on a Distributed Multilink PPP (dMLP) or Distributed Multilink Frame Relay (dMLFR) link with traffic at 95 percent of the line rate and when the number of packets with a small size is high. This symptom occurs on a system that functions as a provider edge (PE) router that is configured for Layer 2 Tunneling Protocol version 3 (L2TPv3) Layer 3 IP VPN (L3VPN) architecture and that has dMLP or dMLFR links to a customer edge (CE) router. This problem is resolved in Release 12.2(18)SXF. (CSCeg24422)
- An LSP ping reports that an LSP is functioning correctly although the LSP cannot carry MPLS payloads such as VPN traffic. This occurs when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1. With this fix, an LSP ping can detect LSP breakages that are caused by untagged interfaces. This problem is resolved in Release 12.2(18)SXF. (CSCee93598)
- A supervisor engine may reload while a multiple number of ATM commands are being executed simultaneously on one ATM Virtual Circuit (VC) from different sessions. This problem occurs in a large configuration and is resolved in Release 12.2(18)SXF. (CSCdw25402)
- When a VPN client acquires a login popup window and attempts to log in, the following popup windows are not displayed after the username and password. This problem is resolved in Release 12.2(18)SXF. (CSCef07048)

- The following messages can occur on a standby MSFC when a LDP Management Information Base (MIB) walk is performed on the active MSFC if it is configured with an ATM interface:

```
00:03:02: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x4065AE98 reading 0x0
00:03:02: %ALIGN-3-TRACE: -Traceback= 4065AE98 4050BFD0 40496270 40497670 404E9908
4050EE6C 402B6D60 402B287C
```

This problem is resolved in Release 12.2(18)SXF. (CSCeg03837)

- RSVP ResvConfirm messages are dropped when multiple equal cost paths are present in the network. This problem is resolved in Release 12.2(18)SXF. (CSCef32588)
- A system reloads when the name of the Embedded Event Manager (EEM) Tool Command Language (TCL) Policy is longer than 12 characters. This problem is resolved in Release 12.2(18)SXF. (CSCeh25105)
- Routes may be unexpectedly removed from the routing table.

This problem occurs when you use Intermediate System-to-Intermediate System (ISIS) to advertise IP prefixes and you enter a distance command that changes the overall configuration but keeps a subset of the prefixes at the same distance as in the previous configuration. The routes to that subset of IP prefixes may get automatically removed from the routing table.

Two examples of this behavior, when starting with a distance 115 ip for ISIS are as follows:

```
router isis
  distance 255 ip
  distance 115 ip
or
router isis
  distance 115 0.0.0.0 255.255.255.255
```

This problem is resolved in Release 12.2(18)SXF. (CSCeh00090)

- During a Non-Stop Forwarding (NSF) MSFC switchover, open shortest path first (OSPF) convergence may be delayed up to 5 minutes. This problem occurs when an OSPF Database Description (DBD) exchange error occurs while the adjacency is brought up. This problem is resolved in Release 12.2(18)SXF. (CSCeh09588)
- When there is a user configured “deny ip any any” in the Web Cache Communication Protocol (WCCP) redirect access control list (ACL) and many WCCP service groups are being serviced, the traffic associated with some service groups is not redirected to CE routers. This problem is resolved in Release 12.2(18)SXF. (CSCeh85087)
- If you enter the **header-compression iphc-format** command, compressed Real-Time Protocol (RTP) errors may occur and half of the packets are dropped. These drops are counted as output drops on the interface. This problem is resolved in Release 12.2(18)SXF. (CSCeh23943)
- Currently you can only enter eight authentication, authorization, and accounting (AAA) **authentication login** and **authorization network** commands into a configuration. The following messages display when you add a ninth command:

```
%AAAA-3-NOFREELISTS: % AAA: No free authentication lists for "login"
or:
% AAA: No free authorization lists for "network".
```

This problem is resolved in Release 12.2(18)SXF. (CSCeh74440)

- Release 12.2SX does not support Turbo ACLs, but the CLI commands related to this functionality are still present. This problem is resolved in Release 12.2(18)SXF. (CSCeh96957)



- A VRF ping fails to reach an OSPF neighbor interface when the platform on which the ping originates and the OSPF neighbor interface are connected by an OSPF sham link that is used for interconnecting traffic between two VPN sites. This problem is resolved in Release 12.2(18)SXF. (CSCeg51291)
- In some network configurations, traffic loss might occur if an output ACL contains a TCP deny ACE that is configured with **range 1 1023**. Packet loss occurs with an ACL “range” configured. For example:

```
deny tcp any <ip_address> <mask> range 1 1023
```

**Workaround:** rewrite the offending statement to either this:

```
deny tcp any <ip_address> <mask> range 0 1023
```

Or this:

```
permit tcp any <ip_address> <mask> eq 0
deny tcp any <ip_address> <mask> lt 1024
```

This problem is resolved in Release 12.2(18)SXF. (CSCeg54004)

- A CE1 to PE1 ping fails when multilink and VRF are configured. This problem is resolved in Release 12.2(18)SXF. (CSCeh31550)
- CEF adjacencies are not established if you configure Internet Engineering Task Force Frame Relay encapsulation (encap Frame Relay IETF) on a serial interface. This problem is resolved in Release 12.2(18)SXF. (CSCeh35068)
- Tracebacks might occur during initialization of a system configured with distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) MLP-QoS. This problem is resolved in Release 12.2(18)SXF. (CSCeh42292)
- A stale non-best path multipath remains in the Routing Information Base (RIB) after the path information changes, and BGP does not consider the stale path part of the multipath. This problem occurs on a system that has the soft-reconfiguration inbound command enabled and only when BGP Multipath Loadsharing is enabled for three or more paths (the number-of-paths argument of the maximum-paths number-of-paths command has a value of three or more).

**Workaround:** Disable the soft-reconfiguration inbound command for the neighbor sessions for which BGP Multipath Loadsharing is enabled or reduce the maximum number of paths for BGP Multipath Loadsharing to two paths.

This problem is resolved in Release 12.2(18)SXF. (CSCeh53906)

- When a Web Cache Communication Protocol (WCCP) service is enabled, Mask Assignment is configured as the assignment method, and five or more caches are in the service group, protocol messages sent to the cache may overflow and cause memory corruption and a reload. This problem is resolved in Release 12.2(18)SXF. (CSCeh56916)
- A file in an Advanced Technology Attachment (ATA) file system may become corrupted by any command that extends the file such as the **show interfaces ethernet | append disk0:file** command. When this situation occurs, the output of the **dir** command or of the **show** command will not list the file. This problem is resolved in Release 12.2(18)SXF. (CSCeh91772)
- BGP next-hop information is not redistributed as expected by the OSPF routing protocol. This problem is resolved in Release 12.2(18)SXF. (CSCeh92012)
- When Compressed Real-Time Protocol (cRTP) errors occur, half of the cRTP packets are dropped. These drops are counted as output drops on the interface. This problem is resolved in Release 12.2(18)SXF. (CSCei02826)
- With BGP configured, conditional advertisement of the default route that is connected to a route map does not work when you enter the **neighbor default-originate** command. This problem is resolved in Release 12.2(18)SXF. (CSCei06089)

- An Advanced Technology Attachment (ATA) file system error causes the system to suspend operation after an MSFC reload. On a system configured with redundant supervisor engines, when the active MSFC reloads, the active supervisor engine starts to reload and then displays the following error message continuously with a traceback:

```
%SYS-2-INTSCHED: 'idle' at level 7
```

This problem is resolved in Release 12.2(18)SXF. (CSCin88077)

- With a large number of interfaces configured, you might see this type of message:

```
Error adding idb to list_type idb list
```

(*list\_type* can be a list name, for example, *macaddr*). This problem is resolved in Release 12.2(18)SXF. (CSCsa80223)

- After a switchover, traffic for OSPF routes might be suspended for approximately 10 to 15 seconds. This problem is resolved in Release 12.2(18)SXF. (CSCsa95973)
- Control plane policing (CoPP) may fail to match packets that arrive tagged with the VPN aggregate MPLS label. This problem is resolved in Release 12.2(18)SXF. (CSCsa69060)
- When Any Transport over MPLS (AToM) is enabled, AToM virtual circuits to a peer may not be reestablished after an interface goes up and down or after being reconfigured because the required targeted LDP session is not reestablished. This situation occurs when LDP is not configured on any interfaces with the **mpls ip interface configuration** command. The LDP will not be configured with this command when MPLS TE tunnels are used to transport AToM traffic between endpoints, and when the **mpls ip interface configuration** command is not enabled on any TE tunnels. This problem is resolved in Release 12.2(18)SXF. (CSCsb04721)
- After a standby supervisor engine boots up in Stateful Switchover (SSO) mode, its MAC address table entries are not synchronized. This problem is resolved in Release 12.2(18)SXF. (CSCsa68043)
- Multicast traffic over generic routing encapsulation (GRE) tunnels may be software switched after an SSO switchover if the underlying physical interface is a port channel. This problem is resolved in Release 12.2(18)SXF. (CSCsa76530)
- Do not enable Cisco Discovery Protocol (CDP) on Firewall Services Module (FWSM) gigabyte interfaces *slot\_number*/2 through *slot\_number*/6. This problem is resolved in Release 12.2(18)SXF. (CSCsa74926)
- The output of **show interface flowcontrol** shows the operational status of flow control as on when the interface is shut down. This problem is resolved in Release 12.2(18)SXF. (CSCsa81282)
- A reload may occur while loading the image for a standby supervisor engine during the initialization. This situation occurs when you configure the **hw-module slot slot-number image disk0: image** command. This problem is resolved in Release 12.2(18)SXF. (CSCsa92394)
- When you change the Next Hop Resolution Protocol (NHRP) mapping configuration, an incorrect NHRP cache entry and incorrect crypto socket entry may occur. When you change the NHRP static mapping entry by entering the **ip nhrp map** command, the NHRP cache entry is not updated with the new mappings and the crypto socket entry is incorrect. This problem is resolved in Release 12.2(18)SXF. (CSCsb03192)
- When configured as an IOS SSH server, stops accepting SSH IPv6 connections even though IPv4 SSH still works. This situation occurs when an IPv4 access class is configured on the VTY line. This problem is resolved in Release 12.2(18)SXF. (CSCsa77158)
- A system configured with a provider edge (PE) interface fails to resend routes to a reloaded BGP peer. This problem is resolved in Release 12.2(18)SXF. (CSCei26899)

- An ISIS routing protocol **redistribute protocol** command is not synchronized to a redundant MSFC, and routes that are dependent on this command fail after a switchover. This problem is resolved in Release 12.2(18)SXF. (CSCin65241)
- A reload may occur during an LSP traceroute when a transit router responds with a downstream map Type-Length-Value (TLV) that contains a multipath length field that is set to 0, 1, 2, or 3. This reload occurs during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. All implementations of the draft version 3 will encode the length as four bytes and reply with a multipath length of four bytes.

When an LSP traceroute is invoked, a transit router replies with a downstream map TLV that contains a multipath length field which is set to a length shorter than four bytes. This situation causes memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet.

**Workaround:** If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value less than four, do not invoke an LSP traceroute.

The implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this problem.

This problem is resolved in Release 12.2(18)SXF. (CSCsa70274)

- OSPF flooding may occur on a system that is configured for OSPF and MPLS traffic engineering and cause a reload. This situation occurs when 1600 OSPF interfaces are configured in an OSPF area that is also configured for MPLS traffic engineering, and when OSPF interfaces and OSPF adjacencies go up and down.

**Workaround:** Reduce the number of OSPF interfaces in the OSPF area to 300 or fewer. You can check the number of OSPF interfaces by entering the **show ip ospf** or **show ip ospf interface [interface-type interface-number]** command. All interfaces that are covered by network statements are counted.

This problem is resolved in Release 12.2(18)SXF. (CSCsa75512)

- An LSP ping (or traceroute packet) is incorrectly sent from an unlabeled interface, preventing the LSP ping from detecting LSP breakages when a one-hop LSP is pinged. This situation occurs on an MPLS operation and maintenance (OAM) configuration. This problem is resolved in Release 12.2(18)SXF. (CSCsa77105)
- If you erase NVRAM with **write erase** and then enter a **write mem** command, the system may reload. Warning messages are displayed when the configuration is saved before the reload. This problem is resolved in Release 12.2(18)SXF. (CSCsa86572)
- A BGP speaker may fail to send all of its prefixes to a neighbor BGP speaker if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation may occur between any pair of BGP speakers. A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). This situation occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE. This problem is resolved in Release 12.2(18)SXF. (CSCsa87473)

- In some scalability cases with a large number of tunnels, SVIs, or VLANs, FIB tracebacks occur after an SSO switchover. This situation occurs because traceback recording for the general event log and the interface event log is on by default. The fix for this problem turns off traceback recording for the general event log and the interface event log. This problem is resolved in Release 12.2(18)SXF. (CSCsa88145)
- A reload can occur when an interface is configured to run ISIS, and then later changed to a passive interface. This problem is resolved in Release 12.2(18)SXF. (CSCsa90719)
- PPP packets are dropped while running software compression under heavy traffic. This problem is resolved in Release 12.2(18)SXF. (CSCsa47223)
- ISIS authentication on point-to-point LAN interfaces may stop functioning after a reload. This problem is resolved in Release 12.2(18)SXF. (CSCsa51095)
- The **service tcp-keepalive-in** command sent from a Supervisor Engine 720 fails to generate a TCP keepalive every 60 seconds to a remote peer to prevent Telnet sessions from timing out. This problem is resolved in Release 12.2(18)SXF. (CSCsa57888)
- When configuring a static Address Resolution Protocol (ARP) entry in conjunction with Network Address Translation (NAT), the static ARP configuration may be incorrectly removed. This situation occurs when the ARP entry corresponds to an address that collides with an address configured for NAT and the NAT entry times out. This problem is resolved in Release 12.2(18)SXF. (CSCsa73847)
- If the WS-X6704-10GE module is installed in the system, the **show interface capability** command displays the following output:

```
Router# show interface tengigabitethernet 5/1 capability
TenGigabitEthernet5/1
  Model:                WS-X6704-10GE
  Type:                  No Connector
  Speed:                 10000
  Duplex:                none
```

“Duplex” should be displayed as “full”. This problem is resolved in Release 12.2(18)SXF. (CSCsa74075)

- Spurious memory accesses might occur when the cbQosREDTailDropByte64 or cbQosREDRandomDropByte64 MIB objects (belonging to the CISCO-CLASS-BASED-QOS-MI) are polled using SNMP. This problem is resolved in Release 12.2(18)SXF. (CSCdz84448)
- Packets that are of minimal length, and transported across a Frame Relay over MPLS (FRoMPLS) VC, are dropped due to a platform-specific minimum packet length requirement. This problem is resolved in Release 12.2(18)SXF. (CSCsb32099)
- An RPR+ switchover might cause CEF inconsistencies on DFC-equipped modules. This problem is resolved in Release 12.2(18)SXF. (CSCuk57124)
- Malformed VTP packets can cause a reload when debugging output is enabled for VLAN Trunk Protocol (VTP) events. This problem is resolved in Release 12.2(18)SXF. (CSCsa82334)
- When a serial link is removed from a multilink bundle by entering the **no ppp multilink** command in the serial link configuration, the link remains at the line protocol down state and does not recover. This problem is resolved in Release 12.2(18)SXF. (CSCei09755)
- A reload or spurious memory access occurs when HSRP rapidly changes states or goes up and down. This problem occurs with Cisco IOS SLB configured and with virtual servers that are monitoring these HSRP groups and probes that are configured on their server farms. This problem is resolved in Release 12.2(18)SXF. (CSCin94752)
- A reload may occur if IEEE 802.1X authentication is disabled and then reenabled while authentication is in progress. This problem is resolved in Release 12.2(18)SXF. (CSCsb29783)

- The general packet radio service (GPRS) Tunneling Protocol (GTP) load-balancing feature that is configured for Intelligent Packet Solution (IPS) 2.0 stops functioning when the **mls ip slb search wildcard rp** command is entered.

The **mls ip slb search wildcard rp** command is recommended for IPS 2.0 because many Radius Load Balancer (RLB) and FireWall Load Balancer (FWLB) are configured as a part of the solution. Without this command, ternary content addressable memory (TCAM) capacity errors and other issues may be seen in the IPS 2.0 environment.

This problem is resolved in Release 12.2(18)SXF. (CSCei37692)

- When you use point-to-point GRE tunnels, non-RPF multicast traffic may get passed to the MSFC and forwarded to the network after an SSO switchover. This situation occurs for approximately 2 minutes after the switchover if the shared tree and the PIM shortest path tree have point-to-point GRE tunnels as incoming interfaces. This problem is resolved in Release 12.2(18)SXF. (CSCsb02590)
- Spurious memory accesses occur when a link goes down and up. This problem is resolved in Release 12.2(18)SXF. (CSCsb23906)
- When the **crypto connect** mode is deconfigured, the interface defaults are updated to L3\_DENY in both the ingress and egress directions. This situation creates incorrect default results in the egress direction if the interface has been converted to a regular Layer 3 interface by configuring the ip address on this interface. This problem is resolved in Release 12.2(18)SXF. (CSCei52441)
- An Cisco IOS SLB GTP virtual server may start rejecting calls when all the real servers in the server farm are in the MAXCONN state. This situation occurs under stress conditions when there are many simultaneous creations and deletions of sessions and when the sticky GTP international mobile subscriber identity (IMSI) feature is enabled on the server. No additional PDP contexts can be created through Cisco IOS SLB even though none of the GPRS Gateway Support Nodes (GGSNs) currently have any contexts. This problem is resolved in Release 12.2(18)SXF. (CSCsb14175)
- When all the GGSNs in a server farm send reassign notifications because of a call admission control failure, the Cisco IOS SLB maximum reassign counter may reach maximum value. If this situation occurs, Cisco IOS SLB fails to relay the create response back to the Serving GPRS Support Node (SGSN). This problem is resolved in Release 12.2(18)SXF. (CSCsb37618)
- For a Supervisor Engine 720 configured with the keepalive feature on a GRE tunnel interface, GRE keepalive packets might be dropped. This situation causes the connection to go up and down continuously. This problem is resolved in Release 12.2(18)SXF. (CSCsa86103)
- After a switchover, a reload may occur when you enter the **no snmp-server** command. This problem is resolved in Release 12.2(18)SXF. (CSCsb44308)
- The NetFlow process has excessive CPU utilization while NetFlow is enabled which continues after NetFlow is disabled. This problem was triggered by an Error-Correcting Code (ECC) correction of a hardware data error in the NetFlow table. This problem is resolved in Release 12.2(18)SXF. (CSCsb34354)
- If a channel port receives a bridge protocol data unit (BPDU) message with an inconsistent VLAN ID from a neighbor, the supervisor engine successfully puts the port in a Port VLAN ID (PVID) inconsistent state but fails to block that port. The channel port could eventually move to the forwarding state due to an update in the STP topology. This situation occurs when the channel port is acting as a standby and is further blocked due to a PVID inconsistency. This situation could also occur if the inconsistency is not cleared. This problem is resolved in Release 12.2(18)SXF. (CSCsb10031)

- A system may make alignment corrections in its executable memory. Entering the **show align EXEC** output displays that an alignment correction has occurred. For example, this alignment correction may occur in `ipc_process_raw_pak` or elsewhere in executable memory:

```
0x40429C2C:ipc_process_raw_pak(0x40429c0c)+0x20
```

This problem is resolved in Release 12.2(18)SXF. (CSCsa58550)

- Entering the **ip multicast longest-match** command fails to cause Reverse Path Forwarding (RPF) checks to function correctly in response to Protocol Independent Multicast (PIM) bootstrap router (BSR) messages. This problem is resolved in Release 12.2(18)SXF. (CSCsa79597)
- In some rare cases, a Route Processor Redundancy (RPR) switchover or a boot up can cause the supervisor engine to reload. This problem is resolved in Release 12.2(18)SXF. (CSCsa79713)
- A system configured with MSDP does not send a triggered Source-Active (SA) message when it is the nondesignated router on a segment for a directly connected source. This situation can induce a delay in the start of the multicast stream for remote receivers. This problem is resolved in Release 12.2(18)SXF. (CSCsb02976)
- CPU utilization is unacceptably high while QoS is parsing large access control lists (ACLs), because an ACL merge occurs for each access control entry (ACE) in the ACL. This problem is resolved in Release 12.2(18)SXF. (CSCsb08236)
- When incremental shortest path first (iSPF) attaches a stub network to the shortest-path tree, it does not check for an existing transit network that describes the same network. This situation might cause a better route to be replaced by a worse route in the routing table. This problem is resolved in Release 12.2(18)SXF. (CSCsb08380)
- A GTP Cisco IOS SLB server may reload when the GTP sticky IMSI feature is disabled while a Packet Data Protocol (PDP) context deletion is in progress. This problem is resolved in Release 12.2(18)SXF. (CSCsb14306)
- A system that is configured with HSRP and proxy ARP, with no active HSRP groups, may respond to an ARP request with a MAC address of an HSRP group that is not configured. This problem is resolved in Release 12.2(18)SXF. (CSCsb15224)
- The Class-Based Quality of Service Management Information Base (CBQoSMB) MIB displays large random values for the class of service (CoS) monitoring MIBs such as the following objects in the `cbQoSMBStatsTable` table:

```
.1.3.6.1.4.1.9.9.166.1.15.1.1.3 = cbQoSMBDropByte64
.1.3.6.1.4.1.9.9.166.1.15.1.1.6 = cbQoSMBPrePolicyByte64
.1.3.6.1.4.1.9.9.166.1.15.1.1.10 = cbQoSMBPostPolicyByte64
.1.3.6.1.4.1.9.9.166.1.15.1.1.14 = cbQoSMBDropPkt64
```

This problem is resolved in Release 12.2(18)SXF. (CSCdv87113)

- The following error messages might appear on the console and in the log:

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
-Process= "TTY Background", ipl= 6, pid= 20
-Traceback= 801BA4D4 801BA798 80114D94 801CEF34
```

This message indicates a situation that does not appear to affect any system service. The system generates these log messages when you enter the **terminal monitor** command and encounter excessive SSH traffic (such as debug messages). This problem is resolved in Release 12.2(18)SXF. (CSCdy80670)

- An attempt to make an active FTP connection to a Linux FTP server will fail and the following message will result:

```
425 Can't build data connection: connection refused.
```

This problem is resolved in Release 12.2(18)SXF. (CSCeg06261)

- Some statics may not get redistributed into a VRF through RIPv2 protocol during a switchover. This problem is resolved in Release 12.2(18)SXF. (CSCeh20051)
- The identification field in all TACACS+ packets is always 0 when the synchronize (SYN) flag is set and the TACACS+ packet goes through a firewall to the AAA server. The firewall interprets this 0 identification field as a Fragment Overlap Attack and drops additional new connections. This problem is resolved in Release 12.2(18)SXF. (CSCeh48684)
- In a multi-router automatic protection switching (APS) configuration with working routers and protect routers and traffic flowing through the active working router, if the working router is powered off, the protect becomes the active router and starts forwarding traffic with minimal packet loss. When the working router is reloaded, the protect router switches to the working router (before the working router's forwarding path is up), causing significant traffic loss. This problem is resolved in Release 12.2(18)SXF. (CSCsa93725)
- Some labels may be missing in the output of an LSP traceroute. This problem is resolved in Release 12.2(18)SXF. (CSCsb38242)
- Network management systems (NMS) stations display an alert because a Supervisor Engine 720 control plane interface state is ifAdminStatus up but ifOperStatus is down. Also, when a switchover occurs, an SNMP trap (linkdown) is sent to the NMS. These problems are resolved in Release 12.2(18)SXF. (CSCsb55343)
- Occasionally, the PS-Fan status in the **show power** command displays as n/a for a functional power supply. This problem is resolved in Release 12.2(18)SXF. (CSCee01435)
- A login authentication fails to appear as default after a VTY is configured. This problem is resolved in Release 12.2(18)SXF. (CSCsa91175)
- On a provider edge (PE) router with multihop eBGP configured to the customer edge (CE) router, a per-VRF aggregate label might get deleted from the MPLS forwarding table. This problem occurs when a connected prefix comes up and when there is already a same prefix that is learned locally from eBGP or another PE-CE protocol. This problem is resolved in Release 12.2(18)SXF. (CSCsb32695)
- If you attach QoS ACL to an interface that is in the MPLS to IP path, the ACL occasionally can cause traffic forwarding problems for the routes that use this path. This problem is resolved in Release 12.2(18)SXF. (CSCsb33744)
- A DHCP client may fail to renew an IP address when DHCP snooping is enabled. This problem is resolved in Release 12.2(18)SXF. (CSCsb36874)
- A reload might occur if you attempt to resequence an ACL. This problem occurs when you delete a few ACEs and then immediately enter the **ip access-list resequence access-list-name starting-sequence-number increment** command. This problem is resolved in Release 12.2(18)SXF. (CSCsa50971)
- A Supervisor Engine 720, configured for OSPF, EIGRP or BGP, may take up to two minutes for multicast RIP traffic to propagate on the first SSO switchover after a reload. The problem is isolated to a system operating in egress replication mode where the outgoing interfaces are local to DFC3B or DFC3A-equipped modules. This problem is resolved in Release 12.2(18)SXF. (CSCsb71242).

- LSP ping packets or traceroute packets received with an untagged output interface are discarded. This situation causes the MPLS echo request packet to timeout while waiting for a reply. This problem is resolved in Release 12.2(18)SXF. (CSCsa82640)
- You might see the following messages when configuring an EtherChannel on a WS-X6548-GE-TX module or a WS-X6548V-GE-TX module:

```
%CAPI_EC-4-RATE_LIMITED: Adding WS-X6548-GE-TX interfaces to an etherchannel will
limit channel throughput to 1 Gbps!
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb16475)

- ACL counters might display twice as many matches than actually exist. This problem occurs only when class maps are nested because the **rate-limit llq classify** command is configured along with class-based classification. When the ACL counters are used in policies with these class maps, the counts are included once for each of the classifications when displaying accounting output for the **show policy interface** command. Twice as many packets appear to have entered the network and are matched on these ACLs. This problem is resolved in Release 12.2(18)SXF. (CSCee56209)
- With both Cisco IOS SLB and NAT configured, if flows are subjected to NAT, NetFlow entries installed to perform NAT in hardware might have the wrong adjacency contents, which might cause SSH or Telnet sessions to stop responding. This problem is resolved in Release 12.2(18)SXF. (CSCsa76016)
- When you load or unload a packet description language module (PDLM), the port map configuration is removed from the running configuration. This problem is resolved in Release 12.2(18)SXF. (CSCea65031)
- With a Supervisor Engine 2 and a WS-6816-GBIC switching module, you might see these messages if you disable and then enable the Switch Fabric Modules (SFMs), or remove and then replace them, and then perform a switchover:

```
%SM-SP-4-BADEVENT: Event 'WS-X6816-GBIC_running' is invalid for the current state
'WS-X6816-GBIC_disabled_with_legacy_and_no_fab_thr': fabman_lc_switching_mode LS:9
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb13885)

- Correctly, power is always allocated for a redundant supervisor engine, even if a switching module is installed in the redundant supervisor engine slot. If a WS-X6148-45AF or WS-X6148-21AF switching module is installed in the redundant supervisor engine slot, the **show power** command display for the redundant supervisor engine slot is incorrect. The display indicates that power is allocated for the installed switching module instead of for a redundant supervisor engine. All other power values displayed by the **show power** command are correct. This problem is resolved in Release 12.2(18)SXF. (CSCsa71097)
- A Supervisor Engine 720 exhibits a spurious memory access when the following commands are entered: **show fm auth-proxy interface vlan 1** and **show fm inspect interface vlan 1**. The error message does not appear again until the supervisor engine has been reloaded. This problem is resolved in Release 12.2(18)SXF. (CSCeh37316)
- A Response Time Reporter (RTR) DNS probe might fail when the target name is a fully qualified DNS name, and the IP domain list with a corresponding domain name is configured. This problem is resolved in Release 12.2(18)SXF. (CSCef59378)
- When a tracking object is configured for an 802.1Q trunk port, IOS Enhanced Object Tracking reports the interface as down even though it is up. This problem is resolved in Release 12.2(18)SXF. (CSCei32920)
- An SNMP walk might fail, and then display these messages:

```
transmission.dsl.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
```



```

19.7 119
transmission.ds1.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
19.8 119
transmission.ds1.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
19.9 119
. . .

```

This problem is resolved in Release 12.2(18)SXF. (CSCeg39518)

- With a complex VRF configuration that is processing a large amount of routing information, you might see messages similar to these after an SSO switchover:

```

02:12:34: %FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
02:12:36: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
(272/145),process = IPC LC Message Handler.
-Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093
100 410932B8

```

This problem is resolved in Release 12.2(18)SXF. (CSCei07805)

- If an intermittent multicast source is inactive for 3.5 minutes, (S,G) entries in the MSDP cache might become inconsistent with a neighbor's cache which can cause multicast packet loss. This problem is resolved in Release 12.2(18)SXF. (CSCsb23433)
- A response to an IPv6 traceroute may include an asterisk instead of the IP address. This problem is resolved in Release 12.2(18)SXF. (CSCeh53775)
- If traffic shaping is configured, and then the data-link connection identifier (DLCI) for a Frame Relay permanent virtual circuit (PVC) is modified, traffic-shaping tracebacks are displayed. This problem occurs when the Frame Relay local management interface (LMI) feature is enabled. This problem occurs only when the DLCI for the Frame Relay PVC is modified with a single configuration command. This does not occur when an installed DLCI is unconfigured and a new DLCI is configured. This problem is resolved in Release 12.2(18)SXF. (CSCeh17470)
- When the **ipv6 mfib forwarding** command is configured on the tunnel interface, IPv6 multicast packets are dropped by an IPv6 tunnel. This problem is resolved in Release 12.2(18)SXF. (CSCee52317)
- The RIB removes routes whose next hop lies on an interface that has gone down. If the route is an OSPF route and the link goes down and up so quickly that the topology appears unchanged to OSPF, the SPF will not be run and the routes will not be repopulated. This problem is resolved in Release 12.2(18)SXF. (CSCei13040)
- Temporary traffic loss occurs on an EtherChannel made up of ports from the active and standby supervisor engines. This occurs after a reload of the standby supervisor engine. This problem is resolved in Release 12.2(18)SXF. (CSCsb13267)
- After a reload, NetFlow Data Export (NDE) records are malformed and report a bad sampling interval. This affects flow statistics. This problem is resolved in Release 12.2(18)SXF. (CSCsa70679)
- Random multicast packet loss might occur when a host leaves or joins a multicast group and the outgoing interface (OIF) list has approximately 85 entries. The problem occurs when the (\*,G) and the (S,G) entries that are affected by the joins or leaves have the same set of OIFs. This problem is resolved in Release 12.2(18)SXF. (CSCsa70835)
- In GRE-based forwarding mode, WCCP unnecessarily uses a software cache that increases MSFC CPU utilization. This problem is resolved in Release 12.2(18)SXF. (CSCsb18740)

- With OSPFv3 configured, when you enter the **show running-config** command or **process-min-time percent percent** command, a spurious memory access or a reload might occur. This problem is resolved in Release 12.2(18)SXF. (CSCei58597)
- If you enter a **write memory** command over the console connection and a **show startup-config** command over a Telnet connection, the startup-config file is deleted. This problem is resolved in Release 12.2(18)SXF. (CSCsa86252)
- An OSPF interface may show a connected route as an OSPF route after the connected network goes up and down or is shutdown. This problem is resolved in Release 12.2(18)SXF. (CSCsa70039)
- On occasion, when you delete a VLAN that is being monitored by ingress Switched Port Analyzer (SPAN), the traffic in other monitored VLANs might stop being monitored. This problem is resolved in Release 12.2(18)SXF. (CSCsb08489)
- When a server farm is configured with two probes, and a real server is taken out of service and then brought back into service, one of the two probes configured for the server farm does not display the real server when you use the **show ip slb probe** command. This problem is resolved in Release 12.2(18)SXF. (CSCsa73607)
- When NHRP receives an invalid packet, it attempts to reply to the sender with an error message that contains part of the original packet. This situation might result in a large memory allocation and a traceback, memory alignment errors, address access errors, and possibly a system reload. This problem is resolved in Release 12.2(18)SXF. (CSCin95836)
- If a policy is configured with a no drop action, then no policer is allocated and no statistics are displayed even if you enter the **mls qos marking statistics** command.

**Workaround:** Because the policer with a no drop action is equivalent to a trust dscp action, you should configure the **trust dscp** command instead in software where this fix is not available. This problem is resolved in Release 12.2(18)SXF. (CSCeh41511)

- When RSVP sends an updated path message to reflect a modification in its QoS request, the updated path message may not get forwarded by a downstream RSVP-aware router. This situation occurs when the downstream router has two RSVP features configured at the same time: local policy and refresh reduction. This problem is resolved in Release 12.2(18)SXF. (CSCei65865)
- When Data Link Switching Plus (DLSw+) is configured with VRF, the local-peer address can belong to any VRF. But DLSw+ will react as if belonged to the main VRF. This problem is resolved in Release 12.2(18)SXF. (CSCea48658)
- The **show ip rsvp interface** interface command displays the wrong allocated bandwidth value. This problem occurs when either a TE tunnel or an RSVP reservation is present, and if the bandwidth is changed while tunnel or reservation is up/up. This problem is resolved in Release 12.2(18)SXF. (CSCec26696)
- A system runs out of memory if configured with at least 15,000 Virtual Private LAN Service (VPLS) virtual circuits and all the LDP session go up and down several times. This problem is resolved in Release 12.2(18)SXF. (CSCsb50995)
- Cisco IOS SLB real servers move to FAILED TESTING or READY\_TO\_TEST when a PROBE\_ABDICATE event occurs. After this event occurs, the real servers will never become operational with per-packet virtual servers and Internet Control Message Protocol (ICMP) probes. This problem is resolved in Release 12.2(18)SXF. (CSCsb14185)
- A system configured with a summary address, which is also an OSPF not-so-stubby area (NSSA) area border router (ABR), might incorrectly age out and flush the summary address. This occurs when NSSA external type 1 or type 2 routes are present. This problem is resolved in Release 12.2(18)SXF. (CSCsb28595)

- If you enter the **no ip vrf vrf\_name** command, this message might be displayed:

```
%FIB-4-FIBCBK: Missing cef table for tableid 1 during CEF table change event.
```

This problem occurs in simple configurations with no routing protocols configured. This problem is resolved in Release 12.2(18)SXF. (CSCee26209)

- In a configuration that includes LSP Verification (LSPV) support, an LSP Verification Manager process may be created, and a UDP port 3503 may be opened even if there are no MPLS applications. This problem is resolved in Release 12.2(18)SXF. (CSCee71911)
- After you enter **shutdown** and **no shutdown** commands on an interface, there might be long delays between ARP requests and subsequent long delays in traffic flow under these circumstances:
  - Multiple subinterfaces belonging to different VRFs are configured on one interface.
  - All the VRFs have the same address on each subinterface and are recursive static.
  - All the VRFs are handling traffic destined to the same address that is reachable through a static route.

This problem is resolved in Release 12.2(18)SXF. (CSCef93058)

- The **distance** command may affect the OSPF path selection algorithm between two paths learned within one OSPF process. The problem occurs when the same IP prefix originates from two different devices and there is a nondefault administrative distance for one of those two devices, which can cause an unpredictable best route selection for the prefix. This problem is resolved in Release 12.2(18)SXF. (CSCeh46993)
- The snmpEngineTime MIB counter resets when the sysUptime MIB counter reaches its maximum value and starts counting from zero again. This problem is resolved in Release 12.2(18)SXF. (CSCeh49492)
- Enhanced Interior Gateway Routing Protocol (EIGRP) unicast routes cannot be preferred over the default IP multicast static route (mroute). This problem is resolved in Release 12.2(18)SXF. (CSCeh50392)
- When you remove a secondary address with the **no ip address** command, all MLS multicast entries for the VLAN associated with the address are deleted, which might affect multiple subnets. This problem is resolved in Release 12.2(18)SXF. (CSCei13379)
- Broadcast packets are not translated to multicast packets when you use the **ip multicast helper-map broadcast** command. This problem is resolved in Release 12.2(18)SXF. (CSCei33038)
- The **exception crashinfo file filename** command needs to be enhanced to collect more information in the crashinfo file because information about a system reload is not being obtained. This problem is resolved in Release 12.2(18)SXF. (CSCei38898)
- When one MPLS-enabled interface is configured, and you enter the **ip vrf forwarding vrf-name** command, occasionally all LDP local binding for all connected interfaces might be removed. This situation makes them unavailable for advertising to a remote LDP peer and causes MPLS VPN traffic to be dropped. This problem is resolved in Release 12.2(18)SXF. (CSCei51486)
- ISIS fails to age LSP versions out of the ISIS local RIB. This situation leaves old routes with out-of-date metrics in the routing table. When a route fails, the old routes are used, which causes routing loops and ignores better alternate routes. This problem is resolved in Release 12.2(18)SXF. (CSCei58655)
- If you convert a Layer 2 port channel interface to a Layer 3 port channel interface, with the same channel-group number, some of the members do not bundle correctly. Entering the **shutdown** and **no shutdown** interface commands on either end of these EtherChannels makes them unstable. This problem is resolved in Release 12.2(18)SXF. (CSCsa58933)

- If you enter a **write memory** command or a **reload** command, this message is displayed:

```
%PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the standby
RouterBaseboard index set to 147
```

This is actually two messages, with a new line placed before “Baseboard.” A previous bug fix added a period and a new line, but “Baseboard index set to 147” may not be printed on systems that have an older version of ROMMON. This problem is resolved in Release 12.2(18)SXF. (CSCsa76833)

- A system may display many CPUHOG error messages and then a reload because of a watchdog timeout. This problem is resolved in Release 12.2(18)SXF. (CSCsa85229)
- The WS-X6704-10GE switching module default settings for the **set port flowcontrol** command are **send desired** and **receive off**. When ports on both sides are connected with these default settings the operational flow control status is **send on** and **receive off**. This prevents flow control autonegotiation. This problem is resolved in Release 12.2(18)SXF. (CSCsa89506)
- The **set dot1x max-req count** command and the **set dot1x tx-period seconds** command do not work. This problem is resolved in Release 12.2(18)SXF. (CSCsa89917)
- An FIBNULLIDB message might be displayed after a switchover in several circumstances, such as deleting a subinterface or doing an OIR of a new switching module. A spurious access may occur instead of the message. This problem is resolved in Release 12.2(18)SXF. (CSCsa97090)
- You may see spurious traceback messages on a standby supervisor engine. These spurious traceback messages are caused by FIB interface entries that do not have corresponding interface entries. This problem is resolved in Release 12.2(18)SXF. (CSCsa97101)
- An egress ACL that denies all UPD packets for a range of Layer 4 port numbers drops all multicast traffic if you apply it to an interface configured to support PIM. This problem is resolved in Release 12.2(18)SXF. (CSCsb06413)
- On an Cisco IOS SLB real server, some traffic entering on a VLAN interface on which an output ACL is configured might be rate limited which would cause traffic loss. This problem is resolved in Release 12.2(18)SXF. (CSCsb14855)
- An inbound ACL may cause WCCP redirection to fail with the loss of all redirected traffic. This problem is resolved in Release 12.2(18)SXF. (CSCsb26773)
- The **ip msdp filter-sa-request** command incorrectly rejects standard ACLs, and displays this message:

```
This command only accepts named extended IP access-lists.
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb29318)

- Private VLAN (PVLAN) host ports cannot coexist with a private VLAN promiscuous port, a trunk port, or a SPAN destination port on the same port ASIC. An attempt to have the port coexist might result in only one of the ports forwarding while the other port will be put in inactive mode.

In Release 12.2(18)SXF and later releases, to prevent traffic loss, ports configured with the **switchport mode dynamic auto** and **switchport mode dynamic desirable** commands are added to the Private VLAN (PVLAN) 12-port and 24-port restrictions described in the “Private VLAN Configuration Guidelines and Restrictions” section of the “Configuring Private VLANs” chapter at these URLs:

- For Catalyst 6500 series switches:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/pvlans.htm>

- For Cisco 7600 series routers:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/pvlans.htm>

This problem is resolved in Release 12.2(18)SXF. (CSCsb44185)

- A system that is configured with Dynamic Multipoint VPN (DMVPN) tunnels might reload during DMVPN deployment with the following bus error:

```
SYS-2-FREEBAD: Attempted to free memory at 41D7A6E4, not part of buffer pool
-Traceback= 40E93794 41CDF084 41CD7CD0 41CBD568 41CBD884 41CBF070 41CC10F0
41CC2068
0x40E93794:free(0x40e936f0)+0xa4
0x41CDF084:ace_polo_send_hapi(0x41cdeb40)+0x544
...
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb16146)

- After you delete a path on an LSP end router of a tunnel to a neighbor, the neighbor reloads. For this problem to occur, the following conditions must occur in this order:
  - If you enter the **shutdown** command followed by the **no shutdown** command on the tunnel headend, the tunnel headend sends a path by RSVP to a neighbor. This problem occurs when the Resv message is delayed.
  - There is only one path to the destination under this session.
  - At the neighbor, the cleanup timer expires for the path before the Resv message arrives.
  - The path is deleted in cleanup and the RSVP Reservation State Block (RSB) data structure is damaged.
  - This damaged data structure is accessed and the neighbor reloads.

This problem is resolved in Release 12.2(18)SXF. (CSCei16615)

- The output of the **show memory summary** command is corrupt. This problem is resolved in Release 12.2(18)SXF. (CSCec21114)
- OSPFv3 may write zeros into incorrect memory locations. Depending on where this memory is, the symptom may be a reload or a warning. This problem occurs when you unconfigure an OSPFv3 area or use the **clear ipv6 ospf process** command. The area being removed or the process being cleared must contain one or more non-self-originated type-4 LSAs, and the system must not have an intra-area path to the autonomous system boundary router (ASBR) described by the type-4 LSA. This problem is resolved in Release 12.2(18)SXF. (CSCei75375)
- A reload might occur when you enter the **write memory** command. This situation occurs on a system that has the **snmp mib community-map** command configured with a very long community string (40 characters) followed by an engine ID. The situation may also occur when the long community string is removed from the configuration. The situation does not occur when you enter the **copy running-config startup-config EXEC** command. This problem is resolved in Release 12.2(18)SXF. (CSCee83917)
- In releases where caveat CSCef46191 is resolved, attempts to open a Telnet connection may result in a “No Free TTYs” message even though many TTYs are available. This problem occurs after simultaneous Telnet requests. This problem is resolved in Release 12.2(18)SXF. (CSCeg15044)
- When a policy is applied on 300 VLANs, the standby supervisor engine displays error messages and the policy is not programmed on the standby supervisor engine. After an SSO switchover, the policy does not exist on the new active supervisor engine. This problem is resolved in Release 12.2(18)SXF. (CSCsa83541)
- If IEEE 802.1q encapsulation is configured on FlexWAN Ethernet interfaces or SPA Ethernet interfaces, routes might not propagate. If this situation occurs, when you enter the **show interface** command for these interfaces, giant packets are shown to have been received on these interfaces. This problem is resolved in Release 12.2(18)SXF. (CSCsb54233)

- IEEE 802.1x authentication takes approximately 150 seconds to authenticate 270 supplicants. This problem is resolved in Release 12.2(18)SXF. (CSCsb29951)
- If you enter the **no ip vrf vrf\_name** command followed by any of the following commands, the supervisor engine reloads:
  - **no ip multicast- routing**
  - **no ip multicast-routing vrf vrf\_name**
  - **no mls ip multicast**

This problem is resolved in Release 12.2(18)SXF. (CSCsa95660)

- A bus error and a reload might occur. To see this problem, you must configure at least 100 VRFs on two PEs and a point-to-point GRE tunnel for each VRF. This generates approximately 140 multicast routes per vrf. The bus error occurs when you delete all the tunnels and all the VRFs. This problem is resolved in Release 12.2(18)SXF. (CSCsb06233)
- Traffic sent over a DEC, configured from a DFC-equipped module, to a WS-X67xx switching module can cause information to be lost about a MAC address learned over the DEC. This loss causes traffic from hosts that are connected from the DFC-equipped module to the MAC address to be flooded to all ports on the DEC. This problem is resolved in Release 12.2(18)SXF. (CSCsb10662)
- In a large LSA configuration that includes at least 44 OSPFv3-enabled links, a reload might occur when an adjacent link with a peer router goes down. This problem is resolved in Release 12.2(18)SXF. (CSCsb36589)
- With multitopology IS-IS in transition mode configured, IPv6 routes that are learned from other IPv6 routers might not be installed in the RIB. This problem is resolved in Release 12.2(18)SXF. (CSCeh41328)
- Multicast virtual private network (MVPN) tunnels may be mapped to an incorrect VRF forwarding table. This problem has been observed in systems that are configured for data multicast distribution tree (MDT) groups. This problem is resolved in Release 12.2(18)SXF. (CSCei22697)
- A PE router that is configured with 100 or more multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF. Also, a tunnel may be a duplicate of another mVRF. This problem occurs when you reload a PE router that is configured for MVPN. This problem is resolved in Release 12.2(18)SXF. (CSCei30764)
- DMVPN Internet security authentication key management protocol (ISAKMP) security associations (SAs) are deleted, and then rebuilt every 2 minutes. This problem occurs when you are using DMVPN spoke-hub and DMVPN spoke-spoke tunnels.

#### Workarounds:

- For DMVPN spoke-hub or spoke-spoke tunnels, an ACL on the physical interface can block GRE packets that have been just decrypted. To solve this problem, configure ACL on the physical interface so it does not block GRE tunnel packets.
- For DMVPN spoke-spoke tunnels, one-way data traffic through the spoke-spoke tunnel can cause this problem. To solve this problem, do not send one-way traffic through spoke-spoke tunnels.

This problem is resolved in Release 12.2(18)SXF. (CSCed84769)

- After a manual switchover occurs in RPR+ mode, a VPN that is configured on a Frame Relay subinterface fails to recover and CEF may be disabled on switching modules.

**Workaround:** Enter the **hw-module slot number reload** command.

This problem is resolved in Release 12.2(18)SXF. (CSCei48972)

- With IGMP version 3 (IGMPv3) enabled on a Switched Virtual Interface (SVI) interface, IGMP snooping does not properly process IGMPv3 reports that have a mixture of exclude mode groups and include mode groups. The system then refuses to forward multicast traffic from the IP addresses specified in these include mode groups to receivers that handle this type of IGMPv3 report. This problem is resolved in Release 12.2(18)SXF. (CSCsa60107)
- On a Supervisor Engine 720, when you enter the **show version** command, the wrong reason is displayed for a system reload after recovery. This problem is resolved in Release 12.2(18)SXF. (CSCeh49742)
- Spurious memory accesses might occur on a SIP-200 module, a FlexWAN module, or an Enhanced FlexWAN module. This situation occurs when a service policy is attached to a Frame Relay serial interface containing at least one Data Link Control (DLC) connection with RFC 1490 bridging configured. This problem is resolved in Release 12.2(18)SXF. (CSCei51175)
- A Cisco device, running IOS and enabled for Intermediate System-to-Intermediate System (IS-IS) routing protocol, may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed IS-IS packet. The IS-IS protocol is not enabled by default. The IS-IS crafted malformed IS-IS Packet that requires processing will not be forwarded across a Level 2 boundary. The specifically crafted malformed IS-IS packet would require local attachment to either a Level 1 or Level 2 router. A Cisco device receiving the malformed IS-IS packet will forward the malformed packet to its neighbors, and may reset.

**Workaround:** There is no workaround. Enabling IS-IS Authentication is seen as a best practice, and can be leveraged as a mitigation technique.

This problem is resolved in Release 12.2(18)SXF. (CSCeh61778)

- A system configured with Cisco IOS server load balancing (SLB) and multiple access interfaces might display several CPUHOG messages and suspend operations in the Cisco IOS SLB process. This problem is resolved in Release 12.2(18)SXF. (CSCei01237)
- The following traceback may be seen when an iBGP prefix changes to an aggregate route (either connected or BGP aggregate) without reinitializing the interface:

```
3d03h: %BGP-3-PER_VRF_AGGR: pervrffaggr label: invalid intag, intag=0 type=5 for
vpn1:10.10.10.10/255.255.255.255
```

This message is informational, indicating that the Tag Forwarding Information Base (TFIB) is requesting a label and may be ignored. This error message indicates that this TFIB request can be ignored because this is a per-vrf-aggregate entry that will get assigned a per-vrf-aggr label. This problem is resolved in Release 12.2(18)SXF. (CSCeh85817)

- With Bridge Control Protocol (BCP) configured on a SIP-200 or a FlexWAN interface, the interface does not become part of STP after an OIR removal and reinsertion. This problem is resolved in Release 12.2(18)SXF. (CSCei02695)
- A reload might occur while processing a malformed Internet Key Exchange (IKE) ID payload. This problem is resolved in Release 12.2(18)SXF. (CSCed94829)
- The Supervisor Engine 720 reloads after changing the spanning tree mode from per-VLAN spanning tree (PVST) to either Rapid Spanning Tree protocol (RSTP) or Multiple Spanning Tree (MST). This problem is resolved in Release 12.2(18)SXF. (CSCsb04346)
- The **mls acl team default-result permit** command does not work. Even if you configure the command, when you send traffic through an interface and make a change to the ACL applied to that interface, packets are dropped. This problem is resolved in Release 12.2(18)SXF. (CSCsb01861)
- With BGP configured, a reload can occur after a switchover. This problem is resolved in Release 12.2(18)SXF. (CSCsb69773)

- A reload might occur when receiving a TACACS+ packet that has its header length set to zero. This problem is resolved in Release 12.2(18)SXF1. (CSCef77265)
- With QoS configured, a reload might occur if you enter the **show running-config** command or the **write memory** command after configuring the first cos-mutation map with default values. This problem is resolved in Release 12.2(18)SXF. (CSCsb11224)
- A system may advertise an IPv6 default route into the Level2 topology. For this problem to occur, the system must:
  - Be running the ISIS routing protocol on both Level1 and Level2
  - Be advertising IPv6 prefixes
  - Have the ISIS ATT bit set
  - Have Level1 connectivity to another Level1 and Level2 ISIS router
  - Do an SSO switchover or lose and then regain connectivity to the Level2 topology

The system mistakenly adds a default route from its Layer1-only link to its neighbor's Layer2-only link. This problem is resolved in Release 12.2(18)SXF. (CSCei04683)

- The following log might appear when there is a switchover from the active to a standby supervisor engine:

```
00:10:45: %SYS-DFC-3-CPUHOG: Task is running for (4936)msecs, more than (2000)msecs
(0/0),process = SCP LC EVENT MGR.(c61c-sp-3-dso-b.so+0x76358)
```

This message is informational only; there are no other symptoms. This problem occurs on the WS-X6816-GBIC switching module only. This problem is resolved in Release 12.2(18)SXF. (CSCsa82912)

- A 30- to 40-millisecond interruption in traffic forwarding might occur when you modify the tunnel bandwidth by entering the **tunnel mpls traffic-eng bandwidth** command. This problem occurs on a system configured for MPLS traffic engineering with ISIS as the associated Interior Gateway Protocol (IGP). This problem is resolved in Release 12.2(18)SXF. (CSCei12603)
- An SVI for a VLAN carrying 1483 or 1490 multipoint bridging (MPB) traffic fails to forward multicast packets over a link in the VLAN. This problem occurs when the SVI is associated with a SPA or a port adapter on a FlexWAN module. This problem is resolved in Release 12.2(18)SXF. (CSCei16701)
- An I/O memory corruption might occur and cause a reload when you use Telnet, reverse Telnet, rsh, or other vty-based applications (for example: a vty-based application used to access a service module). This problem is resolved in Release 12.2(18)SXF. (CSCeh47169)
- Layer 3 traffic ingresses over one port of a [distributed EtherChannel \(DEC\)](#), and then egresses over a different port in the same distributed EtherChannel, might cause continuous flooding after the first time the aging timer expires. This problem is resolved in Release 12.2(18)SXF. (CSCsb38273)
- Higher than normal CPU utilization might be experienced in the BGP I/O process if BGP neighbors go up and down and generate a high volume of BGP updates. This problem is resolved in Release 12.2(18)SXF. (CSCeg07274)
- A VRF forwarding entry is not removed when you enter the **no interface vlan vlan\_num** command. This problem is resolved in Release 12.2(18)SXF. (CSCei38036)
- On a system configured for VRF-lite, a reload occurs when you enter the **no ip vrf vrf-name** to remove the VRFs. This problem does not occur when BGP is configured. This problem is resolved in Release 12.2(18)SXF. (CSCsb22489)
- A reload might occur if you reset an IPsec SPA or a IPsec VPNSM that is supporting active IPsec tunnels. This problem is resolved in Release 12.2(18)SXF. (CSCeh81794)



- All traffic egressing over an Layer 3 DEC is flooded to all fabric channels associated with members of that EtherChannel. Only traffic forwarded over a member interface that is associated with that fabric channel should pass over the fabric channel. This problem is resolved in Release 12.2(18)SXF. (CSCsb16051)
- A Telnet, SSH, or console session might suspend operation when you enter the **show policy-map** command or the **show class-map** command, or while configuring various modular QoS features. This problem occurs when one terminal session leaves these commands at the More prompt. Other terminal sessions may suspend operation while configuring modular QoS features or executing other **show policy-map** or **show class-map** commands before the command in the original session has completed. This problem is resolved in Release 12.2(18)SXF. (CSCed71844)
- IEEE 802.3ad link aggregation control protocol (LACP) creates separate port channels for ports that have different properties. If the properties for these ports are changed to make them compatible, the port channels are aggregated but are still displayed individually in the output of the **show interface flowcontrol** command. This problem is resolved in Release 12.2(18)SXF. (CSCsa81344)
- Packets generated on a system might not be classified on a FlexWAN, Enhanced FlexWAN or SPA for dMLP or dMLFR interfaces. This problem is resolved in Release 12.2(18)SXF. (CSCsa56959)
- During an SSO switchover, a reload of the standby supervisor engine might occur. This problem is resolved in Release 12.2(18)SXF. (CSCsb46607)
- ERSPAN is supported only when the global fabric switching mode is set to compact mode on a Supervisor Engine 720. This problem is resolved in Release 12.2(18)SXF. (CSCec70695)
- If you enter a command with a VLAN range that includes VLAN 1005–1006 during an ERSPAN source session configuration the command is rejected. You can enter separate commands, one with a range that includes 1005 and another with a range that includes 1006, the command is accepted. This filter VLAN configuration will function correctly until the system reloads, and then the configuration will be rejected. This problem is resolved in Release 12.2(18)SXF. (CSCin92518)
- A Label Distribution Protocol (LDP) tunnel might continue to go up and down after an SSO switchover. This problem is resolved in Release 12.2(18)SXF. (CSCsb15156)
- A reload might occur when you configure and then unconfigure a switchport. This problem is caused when an interface configuration is not synchronized in a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXF. (CSCsb49530)
- Secure Sockets Layer (SSL) traffic that is hardware switched over a GRE or MDT tunnel might be routed periodically in software on the MSFC. This situation occurs because hardware entries for multicast routes are continuously removed from and installed into the hardware forwarding table.

**Workaround:** You can disable the multilayer switching for multicast (MLSM) and multicast route consistency checker by entering the **no mls ip multicast consistency-check type scan-mroute count 50 period 10** command.

This problem is resolved in Release 12.2(18)SXF. (CSCsa85752)

- If MACs are learned on an EtherChannel that is configured over a switching module, which has dual switch-fabric connections, they might get out of synchronization. This situation might cause unnecessary unicast flooding. This problem is resolved in Release 12.2(18)SXF. (CSCeh53682)
- When running Generic Online Diagnostic (GOLD) to test a WS-X6148V-GE-TX switching module, the test suite TestLoopback and TestNetflowInlineRewrite causes the module to go into a failed state. The diagnostics tests turn the inline power off to the port, and then turn it back on. When power is restored, the module requires time to recover before configuring the port for loopback. The time delay in the on-demand online diagnostics is not long enough. This problem does not occur when the port is set to negotiate speed. This problem is resolved in Release 12.2(18)SXF. (CSCei63781)

- Egress control plane traffic might get dropped for a distributed Multilink PPP (dMLP) or a distributed multilink Frame Relay (dMFR) interface. This problem occurs only when the multilink interface is oversubscribed. PPP control packets are processed differently and never dropped.

**Workarounds:**

- Reduce the traffic rate.
- Apply some type of queueing mechanism on the interface.

This problem is resolved in Release 12.2(18)SXF. (CSCin96524)

- MAC entries on a DFC that uses dual switch-fabric connections might get out of synchronization. This problem causes unicast flooding over EtherChannels. This problem is resolved in Release 12.2(18)SXF. (CSCeh53682)
- Several IPC-5-WATERMARK messages might be displayed when several IP communications (IPC) messages are displayed. This problem occurs when interfaces go up and down or route changes occur. This problem is resolved in Release 12.2(18)SXF. (CSCeh62781)
- Ping fails when you remove a member link from MLP, and then reconfigure the link. This problem occurs when invalid shim header messages are displayed:

```
Serial2/1/3/27:13 packet dropped: Invalid Shim Header Serial2/1/3/27:13 packet dropped:
Invalid Shim Header
```

This problem is resolved in Release 12.2(18)SXF. (CSCei06406)

When you configure an ATM subinterface and enter the **no power enable module 2** command, and then the **power enable module 2** command, the ATM subinterface will no longer be in the IF-MIB. This problem is resolved in Release 12.2(18)SXF. (CSCsa68717)

- If an empty ACL is specified when configuring a bidirectional PIM rendezvous point, a catchall (\*,G/m) (that is, \*, 224/4) entry is not installed in the hardware FIB table, even though software will use the rendezvous point IP address for the entire multicast address range (that is, 224/4). This problem is resolved in Release 12.2(18)SXF. (CSCsb05822)
- In a VRF-lite configuration, Cisco Express Forwarding (CEF) tables are not synchronized between the active and standby supervisor engines. This problem is resolved in Release 12.2(18)SXF. (CSCsb12896)
- An IPv6 PIM register encapsulation tunnel does not come up after a switchover. The PIM register feature does not work for sources directly connected to the router. This problem occurs when you have entered the **ipv6 pim register-source** global configuration command. This problem is resolved in Release 12.2(18)SXF. (CSCsb27969)
- CPUHOG messages and tracebacks might occur on an OSPF Area Border Router (ABR) that is generating and removing a large number of Type 3 summary link-state advertisements (LSAs) because of routes going up and down. This problem is resolved in Release 12.2(18)SXF. (CSCsb36550)
- Packets are not marked when you set the EoMPLS Hierarchical Quality of Service (HQoS) action for a match criteria to execute the **set mpls experimental topmost** command. This problem also occurs when you set the conform, exceed, and violate HQoS policing action to execute the **set mpls experimental topmost transmit** command. This problem occurs in EoMPLS HQoS on a FlexWAN module, an Enhanced FlexWAN module or a SIP. This problem is resolved in Release 12.2(18)SXF. (CSCeh41080)

## Cisco IOS Software Modularity Caveats

- [Open Cisco IOS Software Modularity Caveats in Release 12.2\(18\)SXF6, page 267](#)
- [Resolved Cisco IOS Software Modularity Caveats in Release 12.2\(18\)SXF6, page 267](#)
- [Resolved Cisco IOS Software Modularity Caveats in Release 12.2\(18\)SXF5, page 267](#)

### Open Cisco IOS Software Modularity Caveats in Release 12.2(18)SXF6

- With a Cisco IOS Software Modularity image and a FlexWAN module that has serial port adapters installed, you might need to do a reload if a remote registry call is blocked. (CSCsg08736)
- The IPv4 unicast routing table on a standby MSFC might have a remotely learned route listed as a locally connected interface. This situation occurs when there is a loopback interface in a down state that has the same IP address as the remotely learned route. This situation causes the interface to be recognized erroneously as up after an SSO switchover.

**Workaround:** Unconfigure loopback interfaces instead of placing them in the down state when they are not in use. (CSCse56549)

### Resolved Cisco IOS Software Modularity Caveats in Release 12.2(18)SXF6

### Resolved Cisco IOS Software Modularity Caveats in Release 12.2(18)SXF5

- No error message is displayed when you move or remove a search root that has a binding defined for it. This problem occurs when you enter the **install bind** configuration command to define the binding for a search root, and you then enter the **install clear** command or the **install move** command on that search root. If a search root that is bound is moved or removed a future reboot may fail because the image is no longer in the location that the system expects it to be in. This problem is resolved in Release 12.2(18)SXF5. (CSCsc28126)
- When the RPF link towards a Rendezvous Point (RP) goes down or is brought up, the active designated forwarder (DF) on the receiver VLAN changes to an alternate path. During DF transition, the DF election goes down and up several times and multicast packets loop in the network for up to 20 seconds. This problem is resolved in Release 12.2(18)SXF5. (CSCsc87117)
- If you create a tag using the **install commit** command, and then perform a rollback to an earlier point in time, and that rollback requires a reload during activation, then the created tag will only be partially deleted. If you attempt to create a tag with the same name, an error will occur. If you attempt to remove that tag name, an error will also occur and that name can no longer be used as a tag. This problem is resolved in Release 12.2(18)SXF5. (CSCsd07913)
- An Interior Gateway Protocol (IGP) adjacency may go down because of an abrupt increase in multicast traffic or an abrupt increase in CPU usage. High CPU usage might occur when you enter the **show ip mroute count** command with a large number of multicast routes present. This problem is resolved in Release 12.2(18)SXF5. (CSCej20707)
- A memory leak might occur when EEM TCL policies are registered to execute. This problem is resolved in Release 12.2(18)SXF5. (CSCek26158)
- A reload might occur if an out-of-memory condition occurs during the execution of a Tool Command Language (TCL) script. This problem is resolved in Release 12.2(18)SXF5. (CSCsc22552)
- In a topology with equal cost Reverse Path Forwarding (RPF) paths, PIM might not select the path with the highest IP address. This is inconsistent with PIM specifications. Because the paths have equal costs, this selection has no impact on traffic flow or performance. This problem is resolved in Release 12.2(18)SXF5. (CSCsc96746)

- A reload might occur because of buffer exhaustion when 30,000 to 60,000 multicast links in sparse mode go up and down. This problem occurs when ingress replication is configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsd03416)
- When the command-line interface (CLI) **action label cli frequency** command is defined in an Embedded Event Manager (EEM) applet, and this applet is triggered by an EEM event, the “sequence number out of sync” error message is generated. This problem is resolved in Release 12.2(18)SXF5. (CSCsc89979)
- If you use SNMP or HTTP to change the running-config file, the changes you made are lost after a process restarts. This problem is resolved in Release 12.2(18)SXF5. (CSCek24385)
- An EEM TCL policy execution is delayed by an amount of time that relates to the size of the configuration. Large configurations may have a delay of 20 seconds or more. The delay before policy execution is approximately equal to the time required to display output from the **show run** command. This problem is resolved in Release 12.2(18)SXF5. (CSCsd08411)
- When you insert or remove Compact Flash cards into or from the Compact Flash Type II slots (disk0 or disk1), no SNMP device trap messages are broadcast by the system even though console messages are displayed. This problem is resolved in Release 12.2(18)SXF5. (CSCsc06891)
- With PIM configured, a memory leak might occur. A memory allocation failure (MALLOCFAIL) eventually might cause a reload. You can monitor the process memory by entering the **show proc mem detailed process\_id sorted holding** command. This problem is resolved in Release 12.2(18)SXF5. (CSCse05960)
- If you install a patch with a tag that covers that patch, and then enter the **install rollback** command and the **install activate** command, the following error message is displayed:

```
Failed updating bill-of-materials file.
Installer information will be out-of-sync.
```

The output from the **show install running** command indicates that the patch is in the pending rollback state, but the processes have already been restarted and are not running the patched code. If you reload the device, the processes start using the patch again as if the activation has not taken place. If you attempt another activation, error messages are displayed, and no processes restart. This problem is resolved in Release 12.2(18)SXF5. (CSCsd25447)

- The only entries in the EEM MIB table are for the event history table size. The event map table and event notification history are missing. You can verify this situation by performing a MIB walk on the EEM MIB table. This problem is resolved in Release 12.2(18)SXF5. (CSCsc29942)
- EEM may become suspended when scanning for patterns provided by **action CLI** commands that match CLI event patterns. This problem is resolved in Release 12.2(18)SXF5. (CSCek26155)
- If you enter the **show processes cpu** command multiple times during a period of heavy stress a reload might occur. This problem is resolved in Release 12.2(18)SXF5. (CSCse00284)

## FlexWAN Caveats in Release 12.2(18)SXF and Rebuilds

- [Open FlexWAN Caveats in Release 12.2\(18\)SXF6, page 269](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF6, page 269](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF5, page 270](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF4, page 270](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF3, page 271](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF2, page 271](#)

- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF1, page 271](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXF, page 272](#)

## Open FlexWAN Caveats in Release 12.2(18)SXF6

None.

## Resolved FlexWAN Caveats in Release 12.2(18)SXF6

- IMA member link state on a PA-A3-8T1/8E1 port adapter might be down when the IMA group interface is up. When you enter the **show ip interface brief** command, the line protocol state of the member link is displayed. This problem is resolved in Release 12.2(18)SXF6. (CSCse64269)
- An Enhanced FlexWAN Fast Ethernet port adapter cannot support a VPN in crypto connect mode unless the port can immediately transition to promiscuous mode when you enter the **crypto connect** command on the VLAN interface. This problem is resolved in Release 12.2(18)SXF6. (CSCek46996)
- Ping might fail on interfaces over a PA-MC-STM1 port adapter after you remove and reconfigure the PA-MC-STM1 controller. This problem is resolved in Release 12.2(18)SXF6. (CSCsc20064)
- An address error and a reload might occur on a system configured with an Enhanced FlexWAN module. This problem occurs when you administratively bring down a serial interface on a PA-E3, and then bring it back up. This problem is resolved in Release 12.2(18)SXF6. (CSCse54611)
- A Reverse Path Forwarding (RPF) entry created by an (S,G) RPT-bit prune for a particular source might not change when the RPF interface receives an (S,G) S-bit join for the same source. This problem is resolved in Release 12.2(18)SXF6. (CSCsd49955)
- Spurious memory accesses and tracebacks might occur after you configure a VLAN database and create an ATM multipoint subinterface. This problem occurs when you use the **atm-bridge enable** command for the main interface and the **bridge vlan vlan-id** command for the subinterface. This problem is resolved in Release 12.2(18)SXF6. (CSCsd53513)
- When NAT is configured, all NetBIOS TCP 139 traffic is process switched in software, which causes high CPU utilization. This problem is resolved in Release 12.2(18)SXF6. (CSCsd69052)
- The output drops that are displayed when you enter the **show interface** command do not match the total of the drops displayed by the **show queuing interface** command and the OutDiscards displayed by the **show interfaces interface counters error** command. This situation occurs when QoS is enabled. This problem is resolved in Release 12.2(18)SXF6. (CSCse15906)
- ARP packets with known opcodes are sent to a dummy multicast MAC address of 0100.0ccd.cdcd during Flex Link switchovers or UplinkFast switchovers. This situation might cause problems for some applications. This problem is resolved in Release 12.2(18)SXF6. (CSCse87417)
- A PIM border router that is positioned between a PIM dense-mode cloud and a PIM sparse-mode cloud may fail to send triggered security associations (SAs) for sources in the PIM dense-mode cloud that are not directly connected. This problem occurs on the PIM router when these conditions occur:
  - The router is configured with the **ip pim dense-mode proxy-register list** command.
  - The router is elected as the rendezvous point for groups specified in the **proxy-register** list command.
  - The router is performing Anycast-RP using Multicast Source Discovery Protocol (MSDP).

This problem is resolved in Release 12.2(18)SXF6. (CSCse20714)

- Memory corruption and a reload might occur when Extended Authentication (Xauth) is enabled and client sessions are brought down. This problem is resolved in Release 12.2(18)SXF6. (CSCsf03566)
- An aggregate policer might stop working after an SSO switchover.  
**Workaround:** Remove and reapply the policer.
- This problem is resolved in Release 12.2(18)SXF6. (CSCse09460)

#### Resolved FlexWAN Caveats in Release 12.2(18)SXF5

- The alarm LED on the PA-MC-8TE1+ stays on even if all the ports on the PA are shutdown. This problem is resolved in Release 12.2(18)SXF5. (CSCsd14307)
- All the Enhanced FlexWAN modules configured on a system might reload when one of the modules reloads. This problem is resolved in Release 12.2(18)SXF5. (CSCsc30268)
- A FlexWAN module might reload when there are multilink bundles with Compressed Real-Time Protocol (cRTP) configured on them. This problem is resolved in Release 12.2(18)SXF5. (CSCsd34741)
- A FlexWAN module might reload when service policy maps are configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsa68661)
- Egress Simple Network Management Protocol (SNMP) counters do not update on PA-2FE or PA-1FE port adapter Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic. This problem occurs when the ingress and egress interfaces are not on the same module. This problem is resolved in Release 12.2(18)SXF5. (CSCec87736)

#### Resolved FlexWAN Caveats in Release 12.2(18)SXF4

- In a distributed link fragmentation and interleaving over ATM (dLFIoATM) configuration, packets ingressing on an ATM FlexWAN interface with ATM Cell Loss Priority (CLP) will not be decoded correctly. This situation requires that the packets to be routed in software on the MSFC instead of being Layer 3 switched in hardware. This problem is resolved in Release 12.2(18)SXF4. (CSCsb97950)
- FlexWAN modules might reload on a system that is configured with Modular QoS CLI (MQC). This problem occurs when the physical interface is in the UP state and the following conditions occur:
  - An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
  - You remove the policy map from the PVC and attach the same policy map to the main interface.
  - You remove the policy map from the main interface.

All FlexWAN modules will reload even though there is no traffic processing when these conditions occur. This problem is resolved in Release 12.2(18)SXF4. (CSCsb12969)
- When you enter the **fair-queue** command for a FlexWAN interface, the command is not saved in the running configuration and is lost after a reload. This problem is resolved in Release 12.2(18)SXF4. (CSCee58986)
- A link to an EIGRP neighbor established over an ATM IMA interface might fail because of an authentication failure even though EIGRP authentication is not configured. This problem is resolved in Release 12.2(18)SXF4. (CSCeg77104)

- ATM OAM PVCs on a FlexWAN module or an Enhanced FlexWAN module might fail to transmit packets after a reload of the system or an OIR of the switching module. This situation occurs because the OAM packets are not processed and remain in the output queues. This problem occurs with a PA-A3-OC3 port adapter that is configured with a service policy. This problem is resolved in Release 12.2(18)SXF4. (CSCsd71119)

### Resolved FlexWAN Caveats in Release 12.2(18)SXF3

- A FlexWAN module reloads continuously if it has a service policy that is attached to a Frame Relay data-link connection identifier (DLCI), and the service policy has fair queueing configured. This problem occurs on a system configured with Frame Relay fragmentation. This problem is resolved in Release 12.2(18)SXF3 (CSCsc95511)

### Resolved FlexWAN Caveats in Release 12.2(18)SXF2

- With a PA-MC-8E1 port adapter, performance might be impaired if you configure Real-Time Protocol (RTP) Header compression on multilink PPP interfaces. This problem is resolved in Release 12.2(18)SXF2. (CSCeg47659)
- ATM multipoint bridging might stop working when there is a mismatch in the FPD version of the Enhanced FlexWAN module ROMMON software. This problem is resolved in Release 12.2(18)SXF2. (CSCsb31368)
- The PA-T3+ or PA-2T3+ port adapters do not always correctly delay the signalling of errors on a link. A system will go down when it receives two Alarm Indication Signal (AIS) bursts of less than one second each, separated by less than one second. This problem is resolved in Release 12.2(18)SXF2. (CSCsb27358)
- ATOM packets with small frame replay packets (11 bytes) that are sent from an Enhanced FlexWAN module are dropped when sent to a WS-X6548-GE-TX or a WS-X6148-GE-TX. This problem is resolved in Release 12.2(18)SXF2. (CSCsb90472)
- With two FlexWAN ATM permanent virtual circuits (PVCs) configured, it might not be possible to send traffic at the contracted rate for both PVCs without packet drops occurring. This problem is resolved in Release 12.2(18)SXF2. (CSCec17185)
- A system configured with a FlexWAN or an Enhanced FlexWAN module might experience memory allocation errors if it has a large QoS configuration. This problem is resolved in Release 12.2(18)SXF2. (CSCsb80590)
- A memory leak occurs when a FlexWAN module equipped with an ATM PA-A3 port adapter is removed. If the module is reinstalled, the loss stops. Otherwise the system will eventually run out of memory and reload. This problem is resolved in Release 12.2(18)SXF2. (CSCsc44237)
- ATM protocol data units (PDUs) might stop ingressing over a WS-X6582-2PA Enhanced FlexWAN module. All of the VCs configured on the ATM interface lose connectivity. This problem is resolved in Release 12.2(18)SXF2. (CSCsb85049)

### Resolved FlexWAN Caveats in Release 12.2(18)SXF1

- A standby supervisor engine might reload during a switchover or bootup if distributed Network-Based Application Recognition (dNBAR) is configured on a FlexWAN interface. This problem is resolved in Release 12.2(18)SXF1. (CSCsc38127)
- FlexWAN modules might reload when you enter the **ip nbar protocol-discovery** command. This problem is resolved in Release 12.2(18)SXF1. (CSCeh88604)

- An Enhanced FlexWAN module might reload with VRF, MLPPP, and QoS configured. This problem is resolved in Release 12.2(18)SXF2. (CSCsc98510)

## Resolved FlexWAN Caveats in Release 12.2(18)SXF

- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the “admindown” state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.2(18)SXF. (CSCin78325)
- A FlexWAN module may reload and generate tracebacks when you perform an online insertion and removal (OIR) on the module. This symptom occurs on a system that is configured for Distributed Link Fragmentation and Interleaving (dLFI) and an MPLS VPN. This problem is resolved in Release 12.2(18)SXF. (CSCef07167)
- With Link Fragmentation and Interleaving configured on a port adapter, the FlexWAN module might reload if links go up and down while traffic is flowing. This problem is resolved in Release 12.2(18)SXF. (CSCin88026)
- When high traffic levels go through the FlexWAN module interfaces that are configured for Quality of Service (QoS), a Route Processor Redundancy Plus (RPR+) switchover may cause the module to pause indefinitely. This problem is resolved in Release 12.2(18)SXF. (CSCeh84740)
- When you attempt to bring up a multilink interface, the interface may go up and down continuously on one side. Also, when the master link of the Multilink PPP (MLP) bundle interface goes down, traffic may stop flowing through the multilink interface. This situation occurs on a system that has non-channelized serial port adapters, such as a 4-port enhanced serial port adapter (PA-4T+) or an 8-port serial port adapter (PA-8T), and that is configured for distributed MLP. This problem is resolved in Release 12.2(18)SXF. (CSCin44386)
- Incorrect reassembly drops might occur on a dMLP ingress interface that has interleaving configured. This situation occurs on a PA-MC-STM-1 port adapter when more than two DS0 members are part of an dMLP bundle that is configured for interleaving. This problem is resolved in Release 12.2(18)SXF. (CSCin91163)
- A FlexWAN module configured to support dMLFR may reload when you enter the **microcode reload** command in the global configuration mode. This problem is resolved in Release 12.2(18)SXF. (CSCin91381)
- A FlexWAN module configured with a PA-MC-8TE1 port adapter detects loss of signal (LOS) after a reload, and then does not recover. This problem is resolved in Release 12.2(18)SXF. (CSCsb21867)
- All low-priority traffic is dropped over a distributed Link Fragmentation and Interleaving over Frame Relay (dLFioFR) link on a system that is configured with an Enhanced FlexWAN module. This situation occurs when all of the traffic is flowing at the full line rate and some low-priority traffic has to be fragmented. This problem is resolved in Release 12.2(18)SXF. (CSCsb25607)
- With serial FlexWAN interfaces configured, you might see these messages and be unable to make a Telnet connection:
 

```
%SYS-3-CPUHOG: Task is running for (4984)msec more than (2000) msec (12/1),
process = Serial Background
Traceback= 402AA8DC 4029F00C 402AD7D0 419C81C0 41A25CF4 4002AE50
```

This problem is resolved in Release 12.2(18)SXF. (CSCeg04325)
- With Cisco IOS SLB configured, FlexWAN module ingress traffic is hardware switched instead of route-cache switched after a switchover. This problem is resolved in Release 12.2(18)SXF. (CSCsa43553)



- When an MFR bundle goes down and up, all links associated with the bundle fail to recover line protocol. This problem occurs in a configuration that includes a PA-8T-V35 2 port adapter. The output of the **show frame-relay multilink** command displays port 0 as “HW state = up, link state = Add\_sent” and will never recovers. This problem is resolved in Release 12.2(18)SXF. (CSCsb48015)
- With a WS-X6182-2PA FlexWAN module installed, you might see messages similar to these about spurious accesses from the FlexWAN module:

```
SLOT 4/0: May 27 08:24:49: %ALIGN-3-SPURIOUS: Spurious memory access
made at 0x60336D
44 reading 0x44
SLOT 4/0: May 27 08:24:49: %ALIGN-3-TRACE: -Traceback= 60336D44
6021AFB0 6021C948 00000000 00000000 00000000 00000000 00000000
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb09250)

- After an OIR has been performed, the **show cef linecard** command might report an entry in the Forwarding Information Base (FIB) Table marked “table-disabled” for a FlexWAN module in slot 13. This problem is resolved in Release 12.2(18)SXF. (CSCsa70188)
- On a system configured with an Enhanced FlexWAN module and a PA-2CT3 port adapter, if the traffic rate becomes high enough to induce input overrun errors, the input rate degrades by approximately 50 percent. This problem is resolved in Release 12.2(18)SXF. (CSCei51155)
- A memory leak might occur on a Supervisor Engine 720 configured with a FlexWAN module that has synchronous transfer mode (STM) port adapters. This occurs when links on unused interfaces go up and down excessively. This problem is resolved in Release 12.2(18)SXF. (CSCsb64812)
- On an Enhanced FlexWAN module configured with a PA-MC-T3+ and PA-MC-2T3+ port adapter, traffic flow might be interrupted for 1 microsecond, followed by a display of this message:

```
%HYPERION-4-HYP_RESET: Hyperion Error Interrupt. Resetting ASIC.
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb07696)

- When NetFlow switching and AAA network security services are configured on a Supervisor Engine 720, memory fragmentation may occur in the I/O memory pool of the FlexWAN module. This problem is resolved in Release 12.2(18)SXF. (CSCsa70104)
- OSPF hello packets may not be received by an Enhanced FlexWAN Fast Ethernet port adapter interface after a peer’s interface has gone up and down. This situation occurs because the OSPF MAC entry is deleted during the link up and down event. This problem is resolved in Release 12.2(18)SXF. (CSCsb65340)
- A reload might occur on a system configured with a FlexWAN module with a channelized T1/E1 port adapter installed. This problem occurs after 5 or 6 hours of bidirectional voice over IP (VoIP) traffic through a multiple link point-to-point protocol (MLPPP) bundle link. A buffer leak eventually causes a memory allocation error to occur. This problem is resolved in Release 12.2(18)SXF. (CSCei86192)
- When IP RTP header-compression (IPHC) is configured on an interface on bay 1 of a FlexWAN or an Enhanced FlexWAN module, the IPHC counters do not update. This problem is resolved in Release 12.2(18)SXF. (CSCeh97017)
- The FIB table might become disabled or the output interface may become stop processing on an A3 ATM port adapter when six subinterfaces with six virtual templates are configured. The problem occurs in a distributed link fragmentation and interleaving over ATM (dLFIoATM) configuration.

**Workaround:** Reload the microcode or perform an OIR to recover the A3 ATM port adapter.

This problem is resolved in Release 12.2(18)SXF. (CSCei08458)

- An ATM interface on a FlexWAN or an Enhanced FlexWAN port adapter stops transmitting when you add or remove a QoS service policy on the interface. This problem is resolved in Release 12.2(18)SXF. (CSCsb01188)

## Service Module Caveats in Release 12.2(18)SXF and Rebuilds

- [Open Service Module Caveats in Release 12.2\(18\)SXF6, page 274](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF6, page 275](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF5, page 275](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF4, page 276](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF3, page 276](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF2, page 276](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF1, page 277](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXF, page 278](#)

### Open Service Module Caveats in Release 12.2(18)SXF6

- After two sequential NSF with SSO switchovers, a SPAN session configured to support a [WS-SVC-IDS-M2-K9](#) disappears from the configuration.  
**Workaround:** Reenter the configuration. (CSCsd66276)
- After a [distributed EtherChannel \(DEC\)](#) has been configured and removed from the configuration, the show monitor command does not display any SPAN sessions that you configure for a service module.  
**Workaround:** Reset the service module to show the SPAN session. (CSCeh03911)
- With a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)), a memory leak might occur when thousands of VPN clients are connecting and disconnecting at the same time. (CSCee25454)
- When you upgrade Cisco IOS software on the supervisor engine, and then you enter the Wireless Services Module (WiSM) module commands for the allowed VLANs, continuous tracebacks might display on the active and the standby consoles:  

```
1d21h: %NETWORK_RF_API-STDBY-3-FAILDECODEDATADESC: Cannot decode data descriptor for
an interface or controller because the sync header cannot be decoded, descriptor
type=3000
-Traceback= 40CCAAEC 40CCAC48 40CCAF58 403962E4 40394468 403950E0 40391514 4038C568
```

  
(CSCse53484)
- When you enter manual **wism** commands to configure individual WiSM Gigabit Ethernet interfaces, invalid and inconsistent configurations might result if the system is using automatic WiSM link aggregation (LAG) configuration commands.  
**Workaround:** Use manual configuration commands on individual WiSM interfaces or automatic WiSM LAG configuration commands, but not both. (CSCse53499)
- When you enter **wism** commands to configure WiSM interfaces, you might see tracebacks after a switchover. These tracebacks have no impact on the performance of the switchover or the WiSM. (CSCse53517)

- When you enter the WiSM controller commands to remove the allowed and native VLANs, the channel group configuration is not removed. You can verify that the channel group configuration still exists by entering the **show etherchannel summary** command or the **show run interface** commands. (CSCse60251)
- On a system configured with a WiSM, you can ping the management interface and pass traffic over it before the link aggregation (LAG) channels are configured. This situation occurs before you configure the allowed VLANs on the WiSM interfaces or assign a native VLAN to the WiSM controller. (CSCse51226)

### Resolved Service Module Caveats in Release 12.2(18)SXF6

- An SNMP walk does not find Content Services Gateway (CSG) user information for a CSG module installed in slot 1. If you add a second user group and an accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server statistics properly either with a manual MIB walk or with SNMP messaging for a CSG module installed in slot 1. This situation occurs with all the quota servers that are configured on both of the configured user groups. This problem is resolved in Release 12.2(18)SXF6. (CSCsa95306)
- The differentiated services code point (DSCP) bits in a packet traversing a Firewall Services Module (FWSM) might get overwritten. This problem is resolved in Release 12.2(18)SXF6. (CSCsd64103)
- When you use the **retcode imap rc-start rc-end** command to configure Content Services Gateway (CSG) refunding, and then you enter a command to write the startup-config and the running-config files, the **retcode rc-start rc-end** command is saved in the startup-config and the running-config files. This configuration can only be removed with the **no retcode imap rc-start rc-end** command. You cannot delete it with the **no retcode rc-start rc-end** command. You cannot overwrite the configuration with a new **retcode** command for imap. After a reload, the whole configuration is missing in the running-config file, and refunding is not configured for IMAP. This problem is resolved in Release 12.2(18)SXF6. (CSCse69748)
- A configuration synchronization check for active and standby CSMs might fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands and then you change configurations only in the active or the standby CSM, the module might incorrectly display synchronized configurations as being out of synchronization, and display configurations that are out of synchronization as being synchronized. This problem is resolved in Release 12.2(18)SXF6. (CSCek22782)
- High CPU utilization, excessive memory consumption, and a reload all might occur after reloading a wireless LAN services module (WLSM). This problem occurs when a large number of mobile nodes are registered to the WLSM and multipoint generic routing encapsulation (MGRE) tunnel interfaces are configured with at least 300 access points. This problem is resolved in Release 12.2(18)SXF6. (CSCse59777)

### Resolved Service Module Caveats in Release 12.2(18)SXF5

- Unnecessary reloads of a CSM might occur under heavy traffic when the CSM does not respond to ICP keepalive messages. ICP keepalives are sent every two seconds, and the CSM is reloaded if it does not respond to three ICP messages. The fix is to reload the CSM if it does not respond to six ICP messages.

**Workaround:** No workaround. ICP keepalives are not configurable.

This problem is resolved in Release 12.2(18)SXF5. (CSCek28863)

- When Unicast Flood Protection (UFP) is enabled, CSM redundancy between devices will periodically transition without any connectivity loss between the devices. This problem is resolved in Release 12.2(18)SXF5. (CSCsc51357)
- The online diagnostics that are performed on the WS-SVC-WISM-1-K9 Wireless Services Module (WiSM) are not performed on the daughtercard. The **diagnostic start module *mod\_num* test 1 port *port\_num*** command only does a MAC loopback test on the WiSM for the specified port number. This problem is resolved in Release 12.2(18)SXF5. (CSCek37181)
- Thermal warnings do not occur for the [WS-SVC-IDS2-K9](#) intrusion detection system module and the [WS-SVC-NAM-2](#) and [WS-SVC-NAM-1](#) network analysis modules (NAMs). This problem is resolved in Release 12.2(18)SXF5. (CSCse11333)
- A configuration synchronization on a CSM might fail and print a time-out message. This problem occurs when the CSM is processing slow path traffic. This problem is resolved in Release 12.2(18)SXF5. (CSCse54041)

### Resolved Service Module Caveats in Release 12.2(18)SXF4

- When you enter the **mls qos** command on a system configured with a [WS-SVC-SSL-1](#) service module, type of service (ToS) information is removed from unencrypted GET packets that pass from the service module to the SSL server. This problem disables the ToS carryover feature on the [WS-SVC-SSL-1](#). This problem is resolved in Release 12.2(18)SXF4. (CSCsc46105)
- Packets larger than 1526 bytes get dropped when passing from the supervisor engine to the Cisco Multiprocessor WAN Application Module (MWAM), regardless of the configured MTU size. This problem is resolved in Release 12.2(18)SXF4. (CSCsb61514)
- You might be unable to access an Multi-Processor WAN Application Module (MWAM) through a console or Telnet session for 10 minutes after the module has been reloaded.

**Workaround:** Configure the **ip rcmd rcp-enabled** command.

This problem is resolved in Release 12.2(18)SXF4. (CSCsa50215)

### Resolved Service Module Caveats in Release 12.2(18)SXF3

- For a topology configured for Firewall Service Module (FWSM) inter-chassis failover, if a manual failover is initiated, and the system is operating in bus mode, inter-chassis failover fails to execute with a status of normal (waiting). This problem occurs when you use a [distributed EtherChannel \(DEC\)](#) between the two chassis where the FWSM is installed, and the devices are forced to operate in bus mode. This problem is resolved in Release 12.2(18)SXF3. (CSCsc57156)

### Resolved Service Module Caveats in Release 12.2(18)SXF2

- Layer 2 and Layer 3 packets that are sourced by a NAM service module and that require recirculation are getting dropped when the fabric switching mode for the service module is crossbar-enabled mode. This problem is resolved in Release 12.2(18)SXF2. (CSCsc03864)
- A reload might occur when you enter the **clear counters** command. This problem occurs if the system is configured with a CSM module that has gone down, and an Remote Procedure Call (RPC) from the supervisor engine has timed out. This problem is resolved in Release 12.2(18)SXF2. (CSCsb79031)
- After a reload, URL match statements are missing from the CSG configuration. When you enter the **ip csg map *map-name* url** command. This problem is resolved in Release 12.2(18)SXF2. (CSCsb66799)

- The sticky database is corrupted if you use the same cookie name when you change the CSM sticky cookie insert configuration, for a virtual server, from dynamic cookie to cookie insert. A corrupted sticky database only partially displays when you enter the **show module csm slot sticky [groups | client ip\_address]** command, and session persistency cannot continue. To correct this problem, all configurations related to the sticky group must be removed and the CSM must be rebooted. This problem is resolved in Release 12.2(18)SXF2. (CSCsc05838)
- A reload might occur when you enter a **hw-module reset** command for a wireless LAN service module, and the DHCP snooping is enabled globally. This problem is resolved in Release 12.2(18)SXF2. (CSCsa58710)
- If a service module goes down, the module sends a message to the supervisor engine requesting an image download so that it can reinitialize. The supervisor engine ignores the message, does not notice that the service module is down for 180 seconds, and then downloads the image. This problem is resolved in Release 12.2(18)SXF2. (CSCei37672)
- A high CPU load might cause the IP Communications (IPC) ports on the MSFC to fail to open. This situation prevents communication between the Cisco Express Forwarding (CEF) and a service module. A FIBDISABLE error message is displayed. This problem is resolved in Release 12.2(18)SXF2. (CSCsb44220)
- On a system configured with a wireless LAN services module (WLSM), these messages might be displayed, and a reload might occur during normal operation:

```
UTIL-3-TREE: Data structure error--attempt to re-add a node to a tree
L3MM-4-MN_IPDB_ADD: Failed to add MN to MN DB
```

This problem occurs when databases that are used to collect IP binding information become inconsistent. This problem is resolved in Release 12.2(18)SXF2. (CSCsa93545)

- If you configure remote console and logging on an Cisco Multiprocessor WAN Application Module (MWAM) service module, you might see this message:

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
```

This problem is resolved in Release 12.2(18)SXF2. (CSCsc08498)

- With redundant CSMs, the CSM with the largest priority value is the primary CSM in the fault-tolerant pair when the modules are both operating. That priority is based on whether certain CSMs interfaces are available. The availability of those interfaces is monitored through a process called interface tracking. In some cases, the hardware interface descriptor block (HWIDB) is not updated. This situation causes the priority value of a CSM to not be adjusted even when a tracked interface goes down. This problem occurs when a link associated with that interface goes up and down several times very quickly. This problem is resolved in Release 12.2(18)SXF2. (CSCsb43860)
- The **hw-module csm standby config-sync** command might time out without synchronizing the CSM configuration from the active CSM to the standby CSM. The problem occurs in large configurations that have many VLANs configured with gateways. This problem is resolved in Release 12.2(18)SXF2. (CSCej00341 and CSCej32688)
- The VPN service module and the IPsec SPA do not generate messages in the date time format. If you enter the **service timestamps debug datetime msec localtime show-timezone** command and the **service timestamps log datetime msec localtime show-timezone** command, this problem still occurs. This problem is resolved in Release 12.2(18)SXF2. (CSCsb02848)

## Resolved Service Module Caveats in Release 12.2(18)SXF1

None.

## Resolved Service Module Caveats in Release 12.2(18)SXF

- VPN client authentication fails when you attempt to use New personal identification number (PIN) mode or Next Token mode. Authentication is successful if you avoid New PIN mode and Next Token mode. The problem occurs when you authenticate using Token card / ACE server through RADIUS in New PIN mode, or Next Token mode has been turned on because you entered an incorrect password, consecutively. This problem is resolved in Release 12.2(18)SXF. (CSCeh35849)
- When a router terminates 102,000 VPNv4 routes the route reflectors (RRs) report only a subset of the total number of routes. This problem is resolved in Release 12.2(18)SXF. (CSCeh33504)
- An IPsec VPN Service module inside a VLAN can not set up ISIS on an interface with a neighbor outside the VLAN. This problem is resolved in Release 12.2(18)SXF. (CSCei41653)
- Reverse route injection (RRI) routes are not reloaded immediately after a WS-SVC-IPSEC-1 IPsec VPN Acceleration Services Module (VPNSM) IPsec stateful failover. This symptom occurs when two systems are configured with VPNSMs, and one of the systems is configured for SSO. When a switchover occurs on the redundant system and the VPNSM reloads, the RRI routes are not reloaded until the VPNSM in the redundant system reloads. This problem is resolved in Release 12.2(18)SXF. (CSCsb38885)
- With a VPN Service Module (VPN-SM/WS-SVC-IPSEC-1) installed, large packet drops might occur when you configure the **ip mtu** command on a GRE IPsec tunnel interface. This problem is resolved in Release 12.2(18)SXF. (CSCsb12076)
- With a WS-SVC-NAM-2 or WS-SVC-NAM1 module installed, the following messages are displayed when you run the **redund reload shelf** command:

```
%CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 2 for software recovery,
Reason: Failed TestFabricChlHealth
SP: TestFabricChlHealth[2]: last_busy_percent[11%], Tx_Rate[476], Rx_Rate[0]
%CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 2 for software recovery,
Reason: Failed TestFabricChlHealth
SP: TestFabricChlHealth[2]: last_busy_percent[7%], Tx_Rate[453], Rx_Rate[0]
```

These errors are shown when the system is being reset. The module does not fail the diagnostics following a **reload** command. This problem is resolved in Release 12.2(18)SXF. (CSCsa92571)

- When configuring a new VLAN on a CSG, the VLAN may not be allowed on the trunk interface between the MSFC and the CSG until the CSG is reloaded. IP connectivity on the VLAN cannot be established towards the CSG before the reload. You can enter the **show interface trunk** command to verify whether or not the VLAN is allowed on the port channel interface associated with the CSG. This problem is resolved in Release 12.2(18)SXF. (CSCsb01086)
- An SNMP walk fails to find a value for the csgQuotaMgrStats MIB object. If you add a second user group and an accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server statistics by either a manual MIB walk or by SNMP messaging. This occurs with the quota servers that are configured in both of the configured user-groups. This problem is resolved in Release 12.2(18)SXF. (CSCsa95287)
- Some service modules do not have central rewrite capability but they generate Layer 3 packets that need to be recirculated (for example, packets that need to egress on a GRE tunnel). These packets are being dropped. [WS-SVC-IDSM2-K9](#) is the only service module impacted by this problem. This problem is resolved in Release 12.2(18)SXF. (CSCei64940)
- If you repeatedly use the **execute-on** command a memory depletion and an eventual reload might occur. This problem is resolved in Release 12.2(18)SXF. (CSCei67673)
- When you attempt to apply a service rule to a billing plan, an error message is displayed. If you enter the **show module csg all billing plan** command the display shows that the service rule is not present. This problem is resolved in Release 12.2(18)SXF. (CSCeh19465)

- The **show module csm slot sticky** command corrupts the display of the real server IP address. This problem is resolved in Release 12.2(18)SXF. (CSCsa77410)
- With a Supervisor Engine 720, a Cisco Multiprocessor WAN Application Module (MWAM) might experience connectivity problems if there are any Layer 2 [distributed EtherChannels \(DECs\)](#) configured. This problem is resolved in Release 12.2(18)SXF (CSCsb50559)

## OSM Caveats in Release 12.2(18)SXF and Rebuilds

- [Open OSM Caveats in Release 12.2\(18\)SXF6, page 279](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF6, page 279](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF5, page 280](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF4, page 280](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF3, page 280](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF2, page 280](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF1, page 280](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXF, page 281](#)

### Open OSM Caveats in Release 12.2(18)SXF6

None.

### Resolved OSM Caveats in Release 12.2(18)SXF6

- A GE-WAN subinterface might drop packets at a high-traffic rate when you enter the **shutdown** command or the **no shutdown** command on another subinterface of the same physical interface. This problem occurs in an OSPF configuration.  
**Workaround:** Enter the **no negotiation auto** command on the GE-WAN port.  
This problem is resolved in Release 12.2(18)SXF6. (CSCse26606)
- An egress Customer Edge (CE) router might not appear in a traceroute that traverses an MPLS Virtual Private Network (VPN). This problem occurs when an egress PE router sends core MPLS interfaces through an OSM module. This problem is resolved in Release 12.2(18)SXF6. (CSCee93983)
- There is an unacceptable mismatch between the change that occurs to the SNMP 64-bit high capacity (HC) input traffic counter of an OSM Frame Relay physical interface, and the total changes that occur to the HC input traffic counters of the subinterfaces. This problem is resolved in Release 12.2(18)SXF6. (CSCsd80632)
- When you apply an output service policy to a Gigabit Ethernet WAN (GE-WAN) interface, the policy might be rejected without explanation. This problem occurs when you have used the **set ip dscp** command to configure the output service policy. This problem is resolved in Release 12.2(18)SXF6. (CSCsc25952)
- A DS3 interface configured on an [OSM-12CT3/T1](#) remains in a line up state and protocol up state after receiving a **loopback remote line** command from an adjacent router. The interface should go into a line up state and protocol down state. This problem is resolved in Release 12.2(18)SXF6. (CSCsd46882)

## Resolved OSM Caveats in Release 12.2(18)SXF5

- Minimum and maximum Weighted Random Early Detection (WRED) threshold values for default differentiated services code point (DSCP) do not change when new values are configured. This problem occurs when an OSM is configured with quality of service (QoS) and WRED. This problem is resolved in Release 12.2(18)SXF5. (CSCsd90501)
- When using a service policy on an OSM-POS port, some MIB objects have the wrong values:
  - The TX cbQosCMPPrePolicyByte64 counter is always 0. It is not incremented with traffic.
  - The TX cbQosCMDropByte64 counter is always 0 even when the policer is dropping traffic.
  - The class-default counters for RX and TX (cbQosCMPPostPolicyByte, cbQosCMPPrePolicyByte, cbQosCMDropByte) are not incrementing even when traffic is sent in this class.

This problem is resolved in Release 12.2(18)SXF5. (CSCsd05513)

- An MPLS table entry on an MSFC might get out of synchronization with the supervisor engine when an OSM goes down. This problem occurs on a system configured with two OSMs, which is facing the MPLS core, and with multiple load-sharing paths to the MPLS core configured. This problem is resolved in Release 12.2(18)SXF5. (CSCsd41981)
- The OSM-2+4GE-WAN+ module might drop packets if you create or delete on it. This problem occurs when the subinterface belongs to a physical interface on the switching module that is currently passing traffic. This problem is resolved in Release 12.2(18)SXF5. (CSCse05336)
- On [OSM-1OC48-POS-SS+, -SI+, -SL+](#) enhanced POS OSMs, aggregate packet counters and rate counters are inaccurate when the traffic rate is more than 2 gigabits per second. This problem is resolved in Release 12.2(18)SXF5. (CSCsb64975)
- GE-WAN subinterfaces might report incorrect SNMP ifIndex values in NetFlow Data Export (NDE) packets after the module is reloaded. If the reported SNMP ifIndex values are zero, the subinterfaces will not be registered at all. This problem is resolved in Release 12.2(18)SXF5. (CSCsc69537)

## Resolved OSM Caveats in Release 12.2(18)SXF4

None.

## Resolved OSM Caveats in Release 12.2(18)SXF3

None.

## Resolved OSM Caveats in Release 12.2(18)SXF2

- On a Supervisor Engine 2, RSPAN does not work when configured on OSM Gigabit Ethernet LAN ports. This problem is resolved in Release 12.2(18)SXF2. (CSCsc24089)
- Spurious accesses are displayed during initialization of an OSM. This problem is resolved in Release 12.2(18)SXF2. (CSCsc18551)

## Resolved OSM Caveats in Release 12.2(18)SXF1

- A Supervisor Engine 720 configured with an OSM POS interface might experience the following ASIC error, and then the OSM POS interface might stop passing traffic:

```
UTC: %CWTLC-3-DMA_ENGINE_ASIC_ERR: DMA Engine Asic [0] error: SRIC packet data CRC error
UTC: %CWTLC-3-CONST_SWITCHING_BUS_INTERFACE_ASIC_ERR: Constellation Switching Bus Interface Asic [0] error: TXIF: RXPB bad packet len (low)
```



This problem occurs when MPLS is configured on an OSM. This problem is resolved in Release 12.2(18)SXF1. (CSCsc73288)

## Resolved OSM Caveats in Release 12.2(18)SXF

- With a Supervisor Engine 720, Layer 3 virtual private network (L3VPN) packets are dropped on the OSM Spatial Reuse Protocol (SRP) interfaces if the interfaces face CE routers. This problem is resolved in Release 12.2(18)SXF. (CSCei20996)
- In rare situations, a reload might occur if you modify an existing PVC. This problem is resolved in Release 12.2(18)SXF. (CSCed29265)
- If you configure or reconfigure the Content Services Gateway (CSG) service module accounting type, the CSG content configuration is erased from the service. This problem is resolved in Release 12.2(18)SXF. (CSCeh62562)
- The SNMP dot3StatsTable MIB object does not support the Gigabit Ethernet WAN modules (OSM-4GE-WAN-GBIC and OSM-2+4GE-WAN+). If you poll the SNMP dot3StatsTable MIB object for a Gigabit Ethernet WAN module, you might see ALIGN-3-SPURIOUS messages and a traceback. This problem is resolved in Release 12.2(18)SXF. (CSCsa71875)
- Images in the Release 12.2(18)SXE1IP Services Secure Shell (SSH) Feature Set do not support the Content Services Gateway (CSG) service module. This problem is resolved in Release 12.2(18)SXF. (CSCeh85135)
- Images in the Release 12.2(18)SXE1IP Services Secure Shell (SSH) Feature Set do not support the Content Services Gateway (CSG) service module. This problem is resolved in Release 12.2(18)SXF. (CSCeh85135)
- On an OSM-2+4GE-WAN+ module, if you replace a physical IEEE 802.1Q tunneling (QinQ) configuration with a QinQ EtherChannel configuration without any member ports, and later add member ports, the EtherChannel might not pass any traffic. This problem is resolved in Release 12.2(18)SXF. (CSCeh55293)
- Changing the encapsulation of an OSM POS interface from HDLC to PPP or from PPP to HDLC causes the link to go down.

**Workaround:** Power cycle the OSM by entering the **no power enable module slot** command and then the **power enable module slot** command.

This problem is resolved in Release 12.2(18)SXF. (CSCeh31691)

- A system configured with a POS OSM may experience the following ASIC error, and the POS interface may later stop passing traffic:

```
UTC: %CWTLC-3-DMA_ENGINE_ASIC_ERR: DMA Engine Asic [0] error: SRIC packet data
CRC error
UTC: %CWTLC-3-CONST_SWITCHING_BUS_INTERFACE_ASIC_ERR: Constellation Switching
Bus Interface Asic [0] error: TXIF: RXPB bad packet len (low)
```

This problem is resolved in Release 12.2(18)SXF. (CSCsb15183)

- The OSM-1OC48-POS-SS+ module occasionally fails to transport specifically crafted packets correctly. This situation causes them to be signalled as output drops on the POS interface. This problem is resolved in Release 12.2(18)SXF. (CSCsa95421)
- The **show mls multicast** command displays incorrect Local Target Logic (LTL) multicast levels for an OSM module. This problem is resolved in Release 12.2(18)SXF. (CSCed52844)
- Following a reload with an OSM-2+4GE-WAN+ or a POS OSM installed, traffic shaping configured on an SVI does not work. This problem is resolved in Release 12.2(18)SXF. (CSCsb24320)

- After an SSO switchover, a OSM-1CHOC12 service module that is channelized to DS0, might reload and cause an APS switchover. This problem is resolved in Release 12.2(18)SXF. (CSCei10228)
- When Weighted Random Early Detection (WRED) is configured on an OSM module, and the input queue limit is set to 2048 packets, the queue does not perform random drops before the limit is reached. All new packets are dropped when the queue reaches 2048 packets. User defined minimum and maximum WRED threshold values are displayed incorrectly as zeroes when you enter the **show policymap** interface command. This problem occurs when an OSM-2+4GE-WAN+ or an enhanced POS OSM is configured with quality of service (QoS) and WRED.

**Workaround:** You must explicitly configure WRED with a queue limit of 128. Random drops will occur in the range of 128 to 2048 packets.

This problem is resolved in Release 12.2(18)SXF. (CSCeh42348)

## SPA Caveats in Release 12.2(18)SXF and Rebuilds

- [Open SPA Caveats in Release 12.2\(18\)SXF6, page 282](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF6, page 282](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF5, page 283](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF4, page 284](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF3, page 284](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF2, page 284](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF1, page 285](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXF, page 285](#)

### Open SPA Caveats in Release 12.2(18)SXF6

- With a CT3 SPA in a SIP-200 configured with multiple DS0 links that are part of multilink bundles, these messages do not indicate a problem that affects traffic:

```
SLOT slot_num: 06:46:34: %INTR_MGR-3-INTR: SPA-4XCT3/DS0[slot_num/bay_num] EFC Parity Error
06:46:34: %Fatal Error: Hardware error (EFC Parity Error) detected for SPA
slot_num/bay_num
```

**Workaround:** None. (CSCeh52330)

- With a CT3 SPA, traffic loss occurs on multilink interfaces that have a differential delay larger than 70 milliseconds.

**Workaround:** None. (CSCef82225)

### Resolved SPA Caveats in Release 12.2(18)SXF6

- The system does not report the cause of an error when an ATM SPA does not initialize because of hardware calibration failures. This problem is resolved in Release 12.2(18)SXF6. (CSCek50720)
- An OC3 ATM SPA that detects CRC errors might send giant packets marked as aborted to a SIP-200 module. The SIP-200 erroneously will cause a %C7600\_SIP200\_SPIRX-3-SPI4\_LINKERROR error message to be displayed. This problem is resolved in Release 12.2(18)SXF6. (CSCeh52424)

- An Ethernet over Multiprotocol Label Switching (EoMPLS) virtual circuit (VC) does not initialize on a two-port POS SPA installed in a SIP-200. This problem occurs when the two-port POS SPA is used as an MPLS core-facing interface. This problem is resolved in Release 12.2(18)SXF6. (CSCek36288)
- Periods of high latency might occur on a Multilink PPP interface, and the interface might stop passing traffic. This problem occurs when the Multilink PPP interface is configured on a SPA-8XCHT1/E1 port adapter that is installed in a SIP-200.

**Workarounds:**

- Configure Multilink PPP interfaces on non-SIP boards.
- Configure IP load balancing by using two separate E1 links (that is, do not use Multilink PPP interfaces).

This problem is resolved in Release 12.2(18)SXF6. (CSCse50607)

- ISIS information does not update when FrameRelay encapsulation is configured on a POS SPA in a SIP-400. This problem is resolved in Release 12.2(18)SXF6. (CSCse29001)

## Resolved SPA Caveats in Release 12.2(18)SXF5

- A Field Programmable Device (FPD) error might occur when you do a SPA FPD upgrade on a SIP1 hardware revision 2.x module if you are using an old FPD bundle. This problem is resolved in Release 12.2(18)SXF5. (CSCek42027)
- Interfaces configured on an ATM SPA that is installed in a SIP-200 might fail to ping if the fabric channel had a synchronization failure during initialization of the SIP-200. This synchronization failure is verified in the output of the **show logging** command:

```
00:00:43: Serial Primary Channel SYNC FAILED!
```

This problem is resolved in Release 12.2(18)SXF5. (CSCsc43862)

- A T3 line might go up and down on a SPA. This problem occurs when the T3 SPAs are configured in channelized mode, the T1 interfaces are configured as Extended Super Frame (ESF) framing, and the T1 interfaces on the far end are configured to send T1 facilities data link (FDL) ANSI reports. This problem is resolved in Release 12.2(18)SXF5. (CSCsd94541)
- Tracebacks might occur when you upgrade the Field Programmable Device (FPD) image on a SIP-400. This situation has no functional impact. This problem is resolved in Release 12.2(18)SXF5. (CSCsc86540)
- An ingress VLAN-ACL service policy on a SPA-10X1GE interface fails to police traffic when you enter the **no xconnect vfi vfi\_name** command for the same VLAN interface. This problem is resolved in Release 12.2(18)SXF5. (CSCsd16407)
- A reload might occur if you remove and replace a 7600-SIP-600 while it is supporting egress traffic on an EtherChannel configured as an IEEE 802.1Q tunnel. This problem is resolved in Release 12.2(18)SXF5. (CSCsd01719)
- For MFR interfaces on channelized SPAs, the line protocol may remain in the down state for about 10 minutes after an RPR+ switchover.

**Workaround:** You can manually enter the **shutdown** command, and then the **no shutdown** command on the MFR interface.

This problem is resolved in Release 12.2(18)SXF5. (CSCek32555)

- When a large number of port channel interfaces are defined on SPAs that are installed in a 7600-SIP-200, all interfaces on the 7600-SIP-200 might go down. When this problem occurs, the RX IPC FIFO FULL error message and heart beat failure messages are displayed on the console. This problem occurs at maximum traffic rate with small packet sizes. This problem is resolved in Release 12.2(18)SXF5. (CSCsd75069)
- The CLASS-BASED-QOS-MIB counters cbQosCMPrePolicyByte64 and cbQosCMPPostPolicyByte64 in the output direction and cbQosCMDropByte64 in the input direction are incorrect. This problem occurs for 10 GE SPAs that are installed in a SIP-600. This problem is resolved in Release 12.2(18)SXF5. (CSCse15495)

#### Resolved SPA Caveats in Release 12.2(18)SXF4

- An ATM virtual path might fail to initialize when a large number of ATM virtual paths are configured on an ATM SPA interface and the interface goes up and down several times. This problem is resolved in Release 12.2(18)SXF4. (CSCek26186)
- The SNMP MIB counters for ATM subinterfaces on OC12 ATM SPA ports in a 7600-SIP-400 do not update. This problem is resolved in Release 12.2(18)SXF4. (CSCsc86600)
- An ATM permanent virtual circuit (PVC) may go down on a SIP1 that has RFC1483 ATM Routed Bridge Encapsulation (RBE) and ATM operation, administration and maintenance (OAM) enabled. This problem is resolved in Release 12.2(18)SXF4. (CSCsb94412)

#### Resolved SPA Caveats in Release 12.2(18)SXF3

- On a system configured with a SIP-200, Network Node Interface (NNI) Frame Relay subinterfaces might end up in a down/down state even though the Frame Relay permanent virtual circuits (PVCs) and a Frame Relay local management interface (LMI) are in an up/active state. This problem is resolved in Release 12.2(18)SXF3. (CSCsc86344)
- A 7600-SIP-400 might drop bursty egress traffic. This problem is resolved in Release 12.2(18)SXF3. (CSCsc68250)

#### Resolved SPA Caveats in Release 12.2(18)SXF2

- On a [SPA-2XCT3/DS0](#) or [SPA-4XCT3/DS0](#), you might see C7600\_SIP200\_SPITX-3-EFC\_QUEUE\_STUCK messages if you add a multilink bundle member that is already a member of one multilink bundle to a second multilink bundle. This problem is resolved in Release 12.2(18)SXF2. (CSCsa80620)
- T3 clear-channel interface performance degrades 40 percent when there are more than 400 low speed NxDS0 (N=1 or N=2) channels configured on the same CT3 SPA with the T3 clear-channel interface. This problem is resolved in Release 12.2(18)SXF2. (CSCed14809)
- A SPA goes out of service when thousands of multilink frame-relay (MFR) data-link connection identifiers (DLCIs) are configured. This problem is resolved in Release 12.2(18)SXF2. (CSCei72033)
- When a hierarchical QOS policy map is applied on a SIP-400 ATM virtual circuit (VC) in the output direction, it will be rejected. This problem is resolved in Release 12.2(18)SXF2. (CSCsb85229)
- Child classes from a hierarchical service policy might not receive minimum guaranteed bandwidth if the parent class is continuously oversubscribed. The following conditions must occur to reproduce this problem:
  - A hierarchical policy map is configured with shaping at the parent and child layers
  - The parent policy's shaping rate is continuously oversubscribed.

- Some classes in the child policy are continuously oversubscribed based on their shaping rate.
- The shaping rates of the affected classes are approximately twice the rates of the classes' guaranteed minimum bandwidth, whether explicitly defined or calculated based on the parent shaping rate.

This problem is resolved in Release 12.2(18)SXF2. (CSCsb62773)

- If you enter the **no aps protect circuit-number ip-address** command from an ATM SPA interface, the console connected to the standby supervisor engine locks for a few minutes. This problem is resolved in Release 12.2(18)SXF2. (CSCej21520)
- ATM SPA SRAM parity errors or SDRAM ECC errors may occur if a SPA is exposed to a significant change in temperature. If SRAM parity errors occur, the SPA will reset. If ECC errors occur, the corrupted packet will be dropped and the SPA will continue operating normally. This problem is resolved by adjusting some hardware settings to allow for fluctuation caused by temperature extremes. This problem is resolved in Release 12.2(18)SXF2. (CSCej21515)
- With an IPsec SPA, Internet Key Exchange (IKE) negotiation might fail if certificate authentication is used and the certificates used are issued by an Entrust Certificate Authority (CA) server. This problem is resolved in Release 12.2(18)SXF2. (CSCsc80822)
- A T1 line on a SPA-2XCT3/DS0 or SPA-4XCT3/DS0 goes down if you configure bit error rate testing (BERT) on a time slot or channel group of the T1. This problem is resolved in Release 12.2(18)SXF2. (CSCsc52645)

## Resolved SPA Caveats in Release 12.2(18)SXF1

None.

## Resolved SPA Caveats in Release 12.2(18)SXF

- On a SPA configured with a POS interface, the APS states on the standby supervisor engine might become inconsistent with the active supervisor engine. After an SSO switchover, this situation might result in incorrect output of the **show aps** command. This problem is resolved in Release 12.2(18)SXF. (CSCei39181)
- With 10 multilink bundles, each with 12 member links, configured from a SPA to a remote router, if you reload the remote router, you might see SPA\_CHOC\_DSX-3-HDLC\_CTRL\_ERR and "Overflow events on HDLC Controller were encountered" messages. This problem is resolved in Release 12.2(18)SXF. (CSCsa70494)
- A SIP-200 with an ATM shared port adapter (SPA) that has a policy map configured might reload when sending ATM Adaptation Layer 5 over MPLS (AAL5oMPLS) traffic. This problem is resolved in Release 12.2(18)SXF. (CSCei24139)
- If multiple FR DLCIs are configured for distributed traffic shaping (dTS) using modular QoS CLI (MQC), some DLCIs might be lost if you enter the **bandwidth n** command on the physical interface.  
**Workaround:** You can reapply the QoS configuration after the bandwidth change. This problem is resolved in Release 12.2(18)SXF. (CSCsb36818)
- With redundant supervisor engines, if you OIR a SPA, and then a switchover occurs, traffic stops over that SPA's interface. This problem is resolved in Release 12.2(18)SXF. (CSCin96328)
- A traceback occurs when you OIR a SIP-400 with an OC-48 ATM SPA. This problem is resolved in Release 12.2(18)SXF. (CSCei21293)
- If you enter the **card type** command for a SPA-8XCHT1/E1, hardware version 2.0 or greater, the command displays a message and fails. This problem is resolved in Release 12.2(18)SXF. (CSCei93397)

- When two interfaces with different encapsulations are configured for IPHC, some cRTP VoIP packets may be dropped on an ingress T3 SPA in a SIP-200 by IPHC as error packets. This problem is resolved in Release 12.2(18)SXF. (CSCei30999)
- MFR bundles configured on a channelized T3 SPA module remains down after a system reload or a reload of the SPA. This problem is resolved in Release 12.2(18)SXF. (CSCei48635)
- A CT3 SPA controller on the near end of a link goes down when the remote end of the link goes down and up. This problem occurs when T1 FDL transmission is started. This problem is resolved in Release 12.2(18)SXF. (CSCei33598)
- When a T3 line goes up and down, the serial interface configured on a T1 channel group over the T3 line fails to come up and stays in the Line Protocol down state. This problem occurs when the link is configured over a SPA-CT3 or a SPA-CHOC-STM1 port adapter. This problem is resolved in Release 12.2(18)SXF. (CSCeh80649)
- The output from the **show mod** command might indicate that a SIP module has an unknown line diagnostics status. This problem occurs after a switchover. The SIP module functions normally and there is no impact to data.

**Workaround:** Enter the **hw-module module num reset** command to reload the SIP module.

This problem is resolved in Release 12.2(18)SXF. (CSCsa71295)

## Caveats in Release 12.2(18)SXE and Rebuilds

- [General Caveats in Release 12.2\(18\)SXE and Rebuilds, page 286](#)
- [FlexWAN Caveats in Release 12.2\(18\)SXE and Rebuilds, page 319](#)
- [Service Module Caveats in Release 12.2\(18\)SXE and Rebuilds, page 323](#)
- [OSM Caveats in Release 12.2\(18\)SXE and Rebuilds, page 327](#)
- [SPA Caveats in Release 12.2\(18\)SXE and Rebuilds, page 330](#)



### Note

- Caveats resolved in Release 12.2(18)SXD4 and earlier releases and Release 12.2(17d)SXB7 and earlier releases are resolved in Release 12.2(18)SXE.
- The caveat information for Release 12.2(18)SXE is being updated frequently.

## General Caveats in Release 12.2(18)SXE and Rebuilds

- [Open General Caveats in Release 12.2\(18\)SXE6a, page 287](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE6a, page 287](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE6, page 287](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE5, page 292](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE4, page 299](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE3, page 307](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE2, page 307](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE1, page 310](#)
- [Resolved General Caveats in Release 12.2\(18\)SXE, page 311](#)

## Open General Caveats in Release 12.2(18)SXE6a

- If you configure the QoS policing violate action to be the same as the exceed action, after a reload, the violate action is drop instead of the configured action.

**Workaround:** None. This problem is resolved in Release 12.2(18)SXF. (CSCsa87178)

- In rare situations, a reload might occur if you make QoS configuration changes to a range of interfaces when a large QoS policy that has 63 microflow policers is attached to the interfaces.

**Workaround:** Reduce the size of the QoS policy or apply the QoS configuration changes to interfaces individually. This problem is resolved in Release 12.2(18)SXF. (CSCsa57222)

- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

## Resolved General Caveats in Release 12.2(18)SXE6a

- A Supervisor Engine 720 might reload when you install a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE6a. (CSCse73539)

## Resolved General Caveats in Release 12.2(18)SXE6

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

Conditions: The packets must be received on a trunk enabled port.

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXE6. (CSCsd34759)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXE6. (CSCsd34855)

- With SNMP ciscoEnvMonTemperature traps enabled, you might see these symptoms:
  - Multiple identical ciscoEnvMonTempStatusChangeNotif traps at the same time with these values:
 

ciscoEnvMonTemperatureStatusDescr.433 (OctetString): module 13 VDB inlet temperature

ciscoEnvMonTemperatureStatusValue.433 (Gauge): 19

ciscoEnvMonTemperatureState.433 (Integer): normal(1)
  - Between 20 through 60 seconds later, multiple identical traps with these values:
 

ciscoEnvMonTemperatureStatusDescr.433 (OctetString): module 13 VDB inlet temperature

ciscoEnvMonTemperatureStatusValue.433 (Gauge): 0

ciscoEnvMonTemperatureState.433 (Integer): notPresent(5)

This problem is resolved in Release 12.2(18)SXE6. (CSCsa87388)

- If you enter the **ip default-network** command, the **show ip route** command does not display the default gateway. This problem is resolved in Release 12.2(18)SXE6. (CSCed87897)
- When an MWAM service module or an OSM is installed, a reload might occur in a low memory configuration or when allocating a large amount of memory. This problem is resolved in Release 12.2(18)SXE6. (CSCef11195)
- When a Multicast-VPN (MVPN) PE router has two entries of the VPNv4-based multicast distribution tree (MDT) in the VPNv4 BGP table that are reflected by redundant route reflectors (RRs), and the current best VPNv4 MDT is withdrawn by one RR, BGP does not inform Protocol Independent Multicast (PIM) of the presence of the new best VPNv4 MDT. The corresponding (S,G) is pruned immediately and left in the pruned state, and then deleted. This problem is resolved in Release 12.2(18)SXE6. (CSCef35386)
- Higher than normal CPU utilization might be experienced in the BGP I/O process if BGP neighbors go up and down and generate a high volume of BGP updates. This problem is resolved in Release 12.2(18)SXE6. (CSCeg07274)
- A tcb\_isvalid traceback might occur in the TCP remote shell process for a link from a remote shell (RSH) or a remote copy protocol (RCP) server to an RSH or an RCP client. This problem is resolved in Release 12.2(18)SXE6. (CSCeg61169)



- When the SNMP ifOperStatus MIB object for an interface that is a member of a multilink group is placed in the down state, the ifStackStatus entry that links the interface to the multilink group interface is removed from the IF-MIB. This problem is resolved in Release 12.2(18)SXE6. (CSCeh62084)
- A system configured with a provider edge (PE) interface fails to resend routes to a reloaded BGP peer. This problem is resolved in Release 12.2(18)SXE6. (CSCei26899)
- A reload might occur when the output of the **show ip pim mdt bgp** command is being displayed. This problem occurs when withdraws for a MDT source group are received by PIM from BGP and you enter the **show ip pim mdt bgp** command. This problem is resolved in Release 12.2(18)SXE6. (CSCei27448)
- This DDTS documents changes in how Cisco IOS software handles packets destined to the router. This problem is resolved in Release 12.2(18)SXE6. (CSCek26492)
- A reload might occur when a certificate revocation list (CRL) expires that has been downloaded and stored in the local cache. This problem is resolved in Release 12.2(18)SXE6. (CSCsa63387)
- When you have MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) routers, a routing loop may occur between the MPLS VPN core and the CEs. This situation occurs if a route is learned from two paths and one path has cost community and the other path does not. This problem is resolved in Release 12.2(18)SXE6 (CSCsa81039)
- A system may display many CPUHOG error messages and then a reload because of a watchdog timeout. This problem is resolved in Release 12.2(18)SXE6. (CSCsa85229)
- The SNMP ifAdminStatus state for the ATM layer or the ATM Adaptation Layer 5 (AAL5) of an ATM interface or subinterface might go down. This situation can occur without entering a **shutdown** command, and prevents SNMP from monitoring the proper status of the ATM interfaces. This problem is resolved in Release 12.2(18)SXE6. (CSCsb12329)
- In GRE-based forwarding mode, WCCP unnecessarily uses a software cache that increases MSFC CPU utilization. This problem is resolved in Release 12.2(18)SXE6. (CSCsb18740)
- A reload might occur during BGP convergence when MVPNs are configured. This problem occurs after a duplicate BGP MDT extended community message is received that specifies a different route descriptor (RD) for an MDT that already exists for the specified MDT source and group address. This problem is resolved in Release 12.2(18)SXE6. (CSCsb33258)
- When you enter the **no mls ip slb search icmp** command, ICMP packets that are not destined for a vserver IP address are still handled by Cisco IOS SLB in the MSFC. These packets should be hardware switched. This problem is resolved in Release 12.2(18)SXE6. (CSCsb80141)
- The Cisco IOS Authentication, Authorization, and Accounting (AAA) user database connection count might not include a VPN client session that is abnormally terminated and then reconnected. This can cause problems in accuracy when the maximum login value is used to track connected users. This problem is resolved in Release 12.2(18)SXE6. (CSCsc65256)
- High CPU usage might occur and the BGP table versions of BGP peers are reset to zero. This problem occurs when you update a complex policy when there is a complex configuration of BGP peers present. This problem is resolved in Release 12.2(18)SXE6. (CSCsc73436)

- When a VRF route is redistributed into the MP-BGP cloud, a routing loop may occur for the prefix that represents the VRF route between the EIGRP cloud and the MP-BGP cloud. This problem occurs on a device that functions as a PE router when the following conditions are present:
  - The router has EIGRP configured on the link to a CE router.
  - The router has a static VRF route that is redistributed into the configuration that is defined by the **address-family vrf vrf-name** command and that is part of the BGP routing process.

This problem is resolved in Release 12.2(18)SXE6. (CSCsc76327)

- During the initialization of a VPN client session, if the Extended Authentication (Xauth) first is successful, and then the session is unsuccessful, the user might be suspended in the local database. This situation can cause problems when the **max-logins** configuration command is used, because a user is included in the count but is no longer active. This problem is resolved in Release 12.2(18)SXE6. (CSCsc91075)
- Power may be incorrectly applied to the wrong port of a WS-X6148-21AF or a switching module equipped with a PoE daughter card, when the module is reset. A device that cannot tolerate inline power might get damaged if you plug it into this port. This problem is resolved in Release 12.2(18)SXE6. (CSCsc92114)
- On a system configured with MPLS-VPN, some of the sham-links might not come up. This problem is resolved in Release 12.2(18)SXE6. (CSCsd12904)
- When a QoS policy map has more than one priority queue attached to more than one ATM VC or ATM LFI VC, traffic might stop flowing in the priority queues or a reload might occur. This problem is resolved in Release 12.2(18)SXE6. (CSCsd19203)
- When a system receives an Multicast Listener Discovery (MLD) report for an IPv6 multicast group, the IPv6 MFIB entry for the group is updated on the MSFC but the MFIB entry on the supervisor engine is not updated for several seconds. This situation delays the start of multicast forwarding. This problem occurs when a receiver joins and leaves a multicast group several times. This problem is resolved in Release 12.2(18)SXE6. (CSCsb91644)
- A Hot Standby Router Protocol (HSRP) active router does not respond to an ARP request for a virtual IP address. This problem might occur when the same HSRP virtual IP address is misconfigured on different HSRP groups on different routers. This problem is resolved in Release 12.2(18)SXE6 (CSCsd80754)
- High CPU utilization occurs while processing ingress IPv6 traffic. This problem occurs under the following conditions:
  - There are no forwarding entries corresponding to the destination addresses of the IPv6 multicast traffic.
  - The destination MAC address is 3333.0000.0001, 3333.0000.000d or 3333.0000.0016.
  - The ingress port is a routed port.

This problem is resolved in Release 12.2(18)SXE6. (CSCsd25532)

- A security violation might occur when a port security-enabled trunk port receives a Cisco Discovery Protocol (CDP) packet. This problem is resolved in Release 12.2(18)SXE6 (CSCsa86954)

- A Frame Relay interface might change the encapsulation on Frame Relay (FR) frames from Internet Engineering Task Force (IETF) encapsulation to Cisco encapsulation under these conditions:
  - Network Address Translation (NAT) or a reflexive ACL is configured on a Frame Relay permanent virtual circuit (FR PVC).
  - There is ingress and egress TCP traffic.

In an FRF.8 environment, this change in the encapsulation causes end-to-end TCP sessions to fail because an intermediate device drops the Cisco-encapsulated Frame Relay frames. This problem is resolved in Release 12.2(18)SXE6. (CSCsd58552)

- Memory leaks might occur in the Internet Key Management Protocol (IKMP) process when using Internet Security Association and Key Management Protocol (ISAKMP) certificates for peer authentication. This problem is resolved in Release 12.2(18)SXE6. (CSCsd45167, CSCsd49723, CSCsd49767)
- If you use Secure Copy to copy a configuration file, a bus error and a reload occurs. This problem is resolved in Release 12.2(18)SXE6. (CSCse12154)
- A reload might occur when the OSPF-MIB table ospfExtLsdbTable is queried with an SNMP walk. Alignment errors might occur when you enter the **show alignment** command because of this same problem. This problem is resolved in Release 12.2(18)SXE6. (CSCef11304)
- Memory leaks occur when a Certification Authority (CA) digital certificate has the serial number as an attribute in the subject name. This problem is resolved in Release 12.2(18)SXE6. (CSCsd43903)
- An established Point to Point Tunneling Protocol (PPTP) connection fails when Network Address Translation (NAT) or Port Address Translation (PAT) translates a new PPTP Call ID incorrectly. This problem occurs when NAT dynamic overload is configured. This problem is resolved in Release 12.2(18)SXE6. (CSCeh35083, CSCsd56549)
- A system might not withdraw a BGP route from an iBGP peer. This problem occurs when you enter the BGP neighbor-specific **clear ip bgp neighbor-address soft out** command for a member of the system's peer group, and then changes occur to the outbound policy of that member.

**Workaround:** You can use the peer group-specific **clear ip bgp peer-group-name soft out** command instead of the BGP neighbor-specific command.

This problem is resolved in Release 12.2(18)SXE6. (CSCeg52659)

- A native VLAN mismatch might go undetected. This situation might cause a forwarding loop. This problem is resolved in Release 12.2(18)SXE6. (CSCsc75381)
- Outbound ACLs that are applied to SVIs have no affect on traffic from Layer 3 interfaces. This problem is resolved in Release 12.2(18)SXE6. (CSCsd03882)
- A large memory leak might occur on a Supervisor Engine 720 when a VLAN, a portchannel, or an individual interface goes down. This problem occurs when the system is in egress replication mode and there are no DFCs present. The interface that goes down must be an outgoing interface of a multicast entry in the hardware. The memory leak is proportional to the number of multicast entries that apply to this interface.

**Workaround:** Put the system in ingress replication mode by entering the **mls ip multicast replication-mode ingress** global configuration command or install a DFC with the system in egress replication mode.

This problem is resolved in Release 12.2(18)SXE6. (CSCsd98887)

- With VRF-aware IPsec configured on a VPN Services Module (VPNSM) or an IPsec SPA, the system does not send the peer device IKE DELETE NOTIFY message when it receives an IPsec packet that has an invalid Security Parameter Index (SPI). This situation causes loss of encrypted traffic. This problem is resolved in Release 12.2(18)SXE6. (CSCse15728)

- When you enter the **show vlans** *vlanID* command, the counters do not display the same values as the SNMP counters. This problem is resolved in Release 12.2(18)SXE6. (CSCsd94687)
- The port ASIC ISR message rate limiter is set to an inappropriate value and allows high CPU usage. This problem is resolved in Release 12.2(18)SXE6. (CSCsb60409)
- When a peer has invalid certificates on an IPSec IKE responder, failed IKE sessions may not be deleted. These failed sessions may accumulate and eventually cause router instability. These failed sessions are displayed in the output of the **show crypto isakmp sa** command. The sessions fail when receiving a bad IKE certificate. This problem occurs when RSA signatures are used as the authentication method.

**Workaround:** You can remove the IKE sessions manually. You also can enter the **shutdown** command followed by the **no shutdown** command on the interface that is used for the IKE sessions. This action brings down all IKE sessions, including any active sessions. You also can reapply the crypto map to this interface. This action brings down all IKE sessions, including any active sessions. This problem is resolved in Release 12.2(18)SXE6. (CSCeh78411, CSCsd68605)

- A DHCP snooping-enabled system can include information about itself in client-originated DHCP packets that the system forwards to a DHCP server. The system accomplishes this by using the Dynamic Host Configuration Protocol (DHCP) relay agent information option (option 82). If the DHCP server does not handle the option 82 data properly, and sends a DHCP reply with malformed option 82 data, the DHCP snooping-enabled system might reload. This problem is resolved in Release 12.2(18)SXE6. (CSCeh21210)
- When you enter the **show crypto ca timers** command, the RENEW time displayed in the output never changes. This problem is resolved in Release 12.2(18)SXE6. (CSCse11457)
- With the Cisco IOS Firewall CBAC feature enabled, if a client opens a connection to a server, which causes a firewall session to be created, and the connection is terminated on both the client and the server, the firewall session may never time out. This problem occurs with applications that use fixed source and destination ports. This problem is resolved in Release 12.2(18)SXE6. (CSCsc72722)

## Resolved General Caveats in Release 12.2(18)SXE5

- The Multiprotocol Border Gateway Protocol (MP-BGP) network entries counter increases above the actual number of reachable networks.

This problem occurs in a nonconverged environment. The correct number of network entries is restored when there is a period of BGP stability that lasts for approximately 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is continuous churning and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the actual number of reachable networks. This problem is resolved in Release 12.2(18)SXE5. (CSCeh16989)

- A reload might occur when a standby supervisor engine is inserted. This problem occurs with the following conditions: SNMP MIB notifications are enabled, the notification log is configured, and the redundancy mode SSO is configured. This problem is resolved in Release 12.2(18)SXE5. (CSCej08355)
- Occasionally in an IGMP multicast configuration, the PFC or DFC FIFO stops processing, and this message is displayed:

```
EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
```

This problem is resolved in Release 12.2(18)SXE5. (CSCej21698)

- Duplicate interface index numbers might be assigned to tunnel interfaces when Protocol Independent Multicast (PIM) and multicast distribution tree (MDT) tunnels are created. These duplicate interface index numbers might prevent traffic from being forwarded from these multicast interfaces. This situation might cause a bus error and a reload when these tunnels are deleted and recreated. This problem is resolved in Release 12.2(18)SXE5. (CSCei80699)
- The **clear ip bgp update-group** [*index-group* | *ip-address*] command clears all the Border Gateway Protocol (BGP) peers, including members of other update groups. This problem is resolved in Release 12.2(18)SXE5. (CSCsb24535)
- A reload might occur after upgrading the Erasable Programmable Logic Device (EPLD) image file on a WS-X6548-GE-TX module in accordance with Field Notice: FN - 29407. The reload also causes the EPLD upgrade to fail. This problem is resolved in Release 12.2(18)SXE5. (CSCsb49326)
- With Cisco IOS SLB and VRF configured, when traffic is fragmented, if a trailing fragment arrives before the leading fragment within a VRF, the trailing fragment is dropped by the supervisor engine. This problem occurs with Cisco IOS SLB enabled. This problem is resolved in Release 12.2(18)SXE5. (CSCsb70996)
- If a service module is installed instead of a redundant supervisor engine, and you change the redundancy mode, this message displays continuously, and then eventually the service module reloads:

```
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR
```

This problem is resolved in Release 12.2(18)SXE5. (CSCsc03429)

- In certain LAN topologies, the PIM assert mechanism can cause an upstream router to erroneously remove downstream interfaces from output interface lists. When this situation occurs, it causes multicast traffic to be dropped. This problem occurs when two or more upstream routers with routes to the same rendezvous point or traffic source are connected to the same LAN segment as two different downstream routers. The problem occurs when the two downstream routers select different upstream routers as their next hop. This problem is resolved in Release 12.2(18)SXE5. (CSCeh17756)
- After an SSO switchover, some SPAN destination ports of RSPAN sessions might stop monitoring traffic. This problem is resolved in Release 12.2(18)SXE5. (CSCsb34213)
- If you enter the **channel-group** command or the **pri-group** command issued in a T1/E1 interface controller mode or a similar configuration to create interfaces, and then you enter the **channel-group** command or the **pri-group** command to unconfigure or reconfigure these interfaces, a Network Time Protocol (NTP) server receiving NTP requests through these interfaces will stop synchronizing with a NTP client. When this problem occurs, the NTP application stops functioning instead of changing interfaces and maintaining synchronization. This problem is resolved in Release 12.2(18)SXE5. (CSCeh48548)
- The global IP address instead of the IP address of the VPN of the egress PE router is displayed in a traceroute VRF. This problem occurs under the following conditions:
  - The egress PE router is configured with a Supervisor Engine 720.
  - The **mls qos** command is configured on the egress PE router.
  - A service policy is configured on the egress PE router.
  - The **no mpls ip propagate-ttl** command is configured on the ingress PE router.
  - The outgoing label on the egress PE router is an aggregate label.

The problem also occurs under these conditions:

- The egress PE router is configured with Supervisor Engine 720.
- The **no mpls ip propagate-ttl** command is configured on the ingress PE router.
- The outgoing label on the egress PE router is an aggregate label.
- Recirculation of MPLS packets with an aggregate label is turned on (using the **mls mpls recir-agg** command).

This problem is resolved in Release 12.2(18)SXE5. (CSCsb80866)

- Egress multicast replication traffic for an outgoing interface (OIF) might be dropped. The supervisor engine generates this replication traffic to synchronize its copy of the multicast expansion table (MET) with the copy on a DFC. If this replication traffic is dropped, it is never resent and the synchronization is never attempted again. This problem is resolved in Release 12.2(18)SXE5. (CSCsb67152)
- A standby supervisor engine in SSO mode might reload. This problem occurs when SNMP fills a data structure, and overwrites a byte of memory after the data structure. This problem is resolved in Release 12.2(18)SXE5. (CSCsc07793)
- In a Gateway Load Balancing Protocol (GLBP) configuration, when the static router address for a SVI is configured on two different Layer 2 addresses for dual ASICs on the same forwarding card, the MAC address for one of the ASICs is not removed from the forwarding table if you enter the **shutdown** command on this SVI. The forwarding cards that feature dual ASICs are the WS-F6700-DFC3A, WS-F6700-DFC3B and the WS-F6700-DFC3BXL. This problem is resolved in Release 12.2(18)SXE5. (CSCsc26490)
- If the software accesses an ARP table that is corrupted, a bus error and a reload might occur. The ARP table gets corrupted when a process accessing the table is suspended and then resumed. This problem is resolved in Release 12.2(18)SXE5. (CSCea34586)
- The SNMP monitor application constantly sends messages indicating that the ifOperStatus of the control plane interface is down. This situation occurs because the control plane interface does not support SNMP. To prevent these messages, the control plane interface has been removed from the list of interfaces in the MIB database. This problem is resolved in Release 12.2(18)SXE5. (CSCej57810)
- A message sent to add an SFP entity into the ENTITY-MIB tree sometimes is not processed. Because the SFP entity has not been added to the ENTITY-MIB tree, the SFP entity will not be displayed when you enter the **show inventory** command. This problem is resolved in Release 12.2(18)SXE5. (CSCsc05500)
- Internet Key Exchange (IKE) security associations (SAs) are not replicated to the standby supervisor engine. This problem is resolved in Release 12.2(18)SXE5. (CSCsc59207)
- The achieved bandwidth of policed egress Ethernet over Multiprotocol Label Switching (EoMPLS) traffic is much lower than the policing value when there is also ingress EoMPLS traffic on the same port whose destination is not the source MAC address of the egress EoMPLS traffic. This problem is resolved in Release 12.2(18)SXE5. (CSCsc13720)
- An OSPF autonomous system boundary router (ASBR) configured with the **area area-id nssa default-information originate** command might continue to advertise a default route on a not-so-stubby area (NSSA) even after the default BGP route has been withdrawn and removed from the routing table. This problem is resolved in Release 12.2(18)SXE5. (CSCsc03828)

- A reload might occur with memory corruption when a SPAN session is removed from service modules. This problem does not occur when the SPAN session is removed from all service modules configured on the system at once. This problem occurs when you enter the **no monitor session servicemodule module 3-4** command and slots 3 and 4 were occupied by Firewall service modules. This problem is resolved in Release 12.2(18)SXE5. (CSCsc06620)
- BGP updategroup selection for peers that are in nonprivate autonomous systems that use the remove-private-as features, needs to be improved to optimize convergence time and flexibility of neighbor configuration. This problem is resolved in Release 12.2(18)SXE5. (CSCei53226)
- A memory leak occurs on a Supervisor Engine 720 when a console session is opened. This problem is resolved in Release 12.2(18)SXE5. (CSCsc08741)
- When a parallel link comes up between two routers running OSPF that have iSPF enabled, routes may not be installed over this new added parallel link. This problem is resolved in Release 12.2(18)SXE5. (CSCsa79783)
- IP multicast streams can be interrupted when IGMP snooping receives an IGMP leave for a group while another leave from the same group and from the same port is already being processed. This problem is resolved in Release 12.2(18)SXE5. (CSCsc32198)
- A memory leak might occur on a system configured with an IPsec VPN SM or an IPsec SPA. A large memory leak might occur on an aggregator or a hub for a large number of spokes, or in configurations where Dead Peer Detections (DPDs) are enabled and the IPsec SA lifetime is a small value (for example, 120 seconds). This problem is resolved in Release 12.2(18)SXE5. (CSCsc52105)
- In a redundant topology with SONET controllers present and configured with Multi-router automatic protection switching (APS), while protection is active, an SSO switchover might cause an inconsistent state for a packet-over-SONET (POS) APS interface. When you enter the **show aps** command, the status for the interface changes from inactive on the slave to interface down after the switchover. This problem is resolved in Release 12.2(18)SXE5. (CSCin46297)
- A loopback interface in a VRF cannot be routed when there is a nonhost static route pointing to the loopback interface in the global routing table. This problem occurs in a VRF-lite configuration. This problem is resolved in Release 12.2(18)SXE5. (CSCsc50692)
- A system configured with an IPsec VPN SM or an IPsec SPA might reload when GRE and IPsec fragmentation occur on the same packet. This problem occurs when 1,000 packets that are the appropriate size are transmitted with the MTU size set to require both GRE and IPsec fragmentation. This problem is resolved in Release 12.2(18)SXE5. (CSCek03772)
- CPU utilization might be high when an existing ARP entry that was learned on an MPLS-enabled interface is updated. This problem occurs if the IP address for that interface is also currently being used with a different ARP entry, for an adjacency pointer. This problem is resolved in Release 12.2(18)SXE5. (CSCsb16512)
- When querying the cbQosCMStatsTable of the CISCO-CLASS-BASED-QOS-MIB, values returned for byte and bit rate statistics are always zero. The output of the **show policy-map interface** command indicates that these statistics are not zero. This problem occurs on FlexWAN, Enhanced FlexWAN and SPA port adapters. This problem is resolved in Release 12.2(18)SXE5. (CSCsc04015)
- Passwords and other sensitive information should not be sent to Access Control Server (ACS) logs. When command accounting is enabled, the full text of each command is sent to an ACS server. This information is sent to the server encrypted, but the server decrypts the packets and logs these commands in plain text. This problem is resolved in Release 12.2(17d)SXE5. (CSCed09685)
- A reload might occur when there is heavy traffic on an IPsec SPA or VPN SM configured with IKE Dead Peer Detection (DPD). This problem is resolved in Release 12.2(18)SXE5. (CSCee86692)

- An LSP ping reports that an LSP is functioning correctly although the LSP cannot carry MPLS payloads such as VPN traffic. This occurs when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1. With this fix, an LSP ping can detect LSP breakages that are caused by untagged interfaces. This problem is resolved in Release 12.2(18)SXE5. (CSCee93598)
- Cisco Express Forwarding (CEF) may not be correctly updated with a route change when the route type changes from interior Border Gateway Protocol (iBGP) to exterior Border Gateway Protocol (eBGP) or vice versa. This symptom occurs when running IPv6 BGP. This problem is resolved in Release 12.2(18)SXE5. (CSCef61721)

- An SNMP walk might fail, and then display these messages:

```
transmission.dsl.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
19.7 119
transmission.dsl.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
19.8 119
transmission.dsl.dsxlFarEndIntervalTable.dsxlFarEndIntervalEntry.dsxlFar
EndIntervalIndex.1
19.9 119
. . .
```

This problem is resolved in Release 12.2(18)SXE5. (CSCeg39518)

- On a Supervisor Engine 720, when you enter the **show version** command, the wrong reason is displayed for a system reload after recovery. This problem is resolved in Release 12.2(18)SXE5. (CSCeh49742)
- A stale non-best path multipath remains in the Routing Information Base (RIB) after the path information changes, and BGP does not consider the stale path part of the multipath. This problem occurs on a system that has the soft-reconfiguration inbound command enabled and only when BGP Multipath Loadsharing is enabled for three or more paths (the number-of-paths argument of the maximum-paths number-of-paths command has a value of three or more).

**Workaround:** Disable the soft-reconfiguration inbound command for the neighbor sessions for which BGP Multipath Loadsharing is enabled or reduce the maximum number of paths for BGP Multipath Loadsharing to two paths.

This problem is resolved in Release 12.2(18)SXE5. (CSCeh53906)

- With a complex VRF configuration that is processing a large amount of routing information, you might see messages similar to these after an SSO switchover:

```
02:12:34: %FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
02:12:36: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
(272/145),process = IPC LC Message Handler.
-Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093
100 410932B8
```

This problem is resolved in Release 12.2(18)SXE5. (CSCei07805)

- Multicast virtual private network (MVPN) tunnels may be mapped to an incorrect VRF forwarding table. This problem has been observed in systems that are configured for data multicast distribution tree (MDT) groups. This problem is resolved in Release 12.2(18)SXE5. (CSCei22697)
- A PE router that is configured with 100 or more multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF. Also, a tunnel may be a duplicate of another mVRF. This problem occurs when you reload a PE router that is configured for MVPN. This problem is resolved in Release 12.2(18)SXE5. (CSCei30764)



- A VRF forwarding entry is not removed when you enter the **no interface vlan** *vlan\_num* command. This problem is resolved in Release 12.2(18)SXE5. (CSCe138036)
- OSPFv3 may write zeros into incorrect memory locations. Depending on where this memory is, the symptom may be a reload or a warning. This problem occurs when you unconfigure an OSPFv3 area or use the **clear ipv6 ospf process** command. The area being removed or the process being cleared must contain one or more non-self-originated type-4 LSAs, and the system must not have an intra-area path to the autonomous system boundary router (ASBR) described by the type-4 LSA. This problem is resolved in Release 12.2(18)SXE5. (CSCe175375)
- Packets generated on a system might not be classified on a FlexWAN, Enhanced FlexWAN or SPA for dMLP or dMLFR interfaces. This problem is resolved in Release 12.2(18)SXE5. (CSCsa56959)
- When a policy is applied on 300 VLANs, the standby supervisor engine displays error messages and the policy is not programmed on the standby supervisor engine. After an SSO switchover, the policy does not exist on the new active supervisor engine. This problem is resolved in Release 12.2(18)SXE5. (CSCsa83541)
- A BGP speaker may fail to send all of its prefixes to a neighbor BGP speaker if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation may occur between any pair of BGP speakers. A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). This situation occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE. This problem is resolved in Release 12.2(18)SXE5. (CSCsa87473)
- The **mls acl team default-result permit** command does not work. Even if you configure the command, when you send traffic through an interface and make a change to the ACL applied to that interface, packets are dropped. This problem is resolved in Release 12.2(18)SXE5. (CSCsb01861)
- Members of a BGP update group might have different versions of BGP tables, which could prevent BGP from removing networks that do not have a path. This problem is resolved in Release 12.2(18)SXE5. (CSCsb09852)
- With QoS configured, a reload might occur if you enter the **show running-config** command or the **write memory** command after configuring the first cos-mutation map with default values. This problem is resolved in Release 12.2(18)SXE5. (CSCsb11224)
- On a system configured for VRF-lite, a reload occurs when you enter the **no ip vrf** *vrf-name* to remove the VRFs. This problem does not occur when BGP is configured. This problem is resolved in Release 12.2(18)SXE5 (CSCsb22489)
- If an intermittent multicast source is inactive for 3.5 minutes, (S,G) entries in the MSDP cache might become inconsistent with a neighbor's cache which can cause multicast packet loss. This problem is resolved in Release 12.2(18)SXE5. (CSCsb23433)
- The **clear ip bgp update-group** [*index-group* | *ip-address*] command clears all the Border Gateway Protocol (BGP) peers, including members of other update groups. This problem is resolved in Release 12.2(18)SXE5. (CSCsb24535)
- After an SSO switchover, some SPAN destination ports of RSPAN sessions might stop monitoring traffic. This problem is resolved in Release 12.2(18)SXE5. (CSCsb34213)
- A reload might occur after upgrading the Erasable Programmable Logic Device (EPLD) image file on a WS-X6548-GE-TX module in accordance with Field Notice: FN - 29407. The reload also causes the EPLD upgrade to fail. This problem is resolved in Release 12.2(18)SXE5. (CSCsb49326)
- If IEEE 802.1q encapsulation is configured on FlexWAN Ethernet interfaces or SPA Ethernet interfaces, routes might not propagate. If this situation occurs, when you enter the **show interface** command for these interfaces, giant packets are shown to have been received on these interfaces. This problem is resolved in Release 12.2(18)SXE5. (CSCsb54233)

- When a statically mapped rendezvous point is defined as an interface address and the interface is in the down/down state, the router can still attempt to become the rendezvous point for the defined groups. This problem occurs when the interface that reached the down/down state was not administratively brought down (for example, a cable was unplugged). This problem is resolved in Release 12.2(18)SXE5. (CSCsb64585)
- A reload might occur with a breakpoint exception (signal=5). This problem can occur in any release that contains the fix for CSCee28288 when a 32-bit counter continues to increment until it wraps around to 0. In most cases approximately 40 to 50 weeks of continuous uptime elapses before this problem is observed. This problem is resolved in Release 12.2(18)SXE5. (CSCsb98702)
- CPUHOG messages might be displayed if PIM snooping is enabled on several VLANs. This problem is resolved in Release 12.2(18)SXE5. (CSCsc26048)
- A system configured with IPsec stateful failover with a large number of Internet Key Exchange (IKE) security associations (SAs) might reload because of memory corruption. The crashinfo file might display the following messages:

```
%SYS-3-BADFREEPTRS:
%SYS-6-BLKINFO: Corrupted previous pointer in next of freed block
```

This problem is resolved in Release 12.2(18)SXE5. (CSCsc94266)

- If SNMP sets an ERSPAN crcERSpanIFTTable MIB object entry to not-in-service, and the status does not change for 50 minutes, a memory corruption occurs. This problem is resolved in Release 12.2(18)SXE5. (CSCej87462)
- A serial interface might remain configured in an MFR bundle link after the serial interface has been removed. This problem is resolved in Release 12.2(18)SXE5. (CSCsb67941)
- A bus error and a reload might occur on a system configured with SNMP views. This problem occurs if the views are being polled by SNMP while they are being changed or updated, which happens when the running configuration is updated. This problem is resolved in Release 12.2(18)SXE5. (CSCsc82214)
- A memory leak might occur when you enter the **show mls nde** command. The leak will eventually disable Cisco Express Forwarding (CEF). This problem is resolved in Release 12.2(18)SXE5. (CSCsc89044)
- For a system configured as an IP HTTP server, tracebacks and a reload might occur during HTTP transactions with URL tokens greater than 128 characters long. A token is a string delimited by slashes in a URL. This problem is resolved in Release 12.2(18)SXE5. (CSCeg62070)
- A WS-X6548-GE-TX port might stop forwarding unicast traffic. This problem occurs when WS-X6548-GE-TX ports are configured as Layer 2 switch ports, are not part of an EtherChannel, and the LTL consistency checker is enabled, which is the default state.

**Workaround:** Disable the LTL consistency checker by entering the **no ip cef table consistency-check** command.

This problem is resolved in Release 12.2(18)SXE5. (CSCsb08512)

- In a topology with multiple multicast forwarding devices sharing the same physical medium, if one of the forwarding devices reloads, then a Catalyst 6500 switch or a Cisco 7600 router acting as the other forwarding device might fail to forward some traffic. This problem is resolved in Release 12.2(18)SXE5. (CSCei13579)
- A Supervisor Engine 720 configured with a WS-X67xx switching module might experience fabric receive errors on all fabric channels and frequent fabric synchronization errors during the initialization of the module. This problem is resolved in Release 12.2(18)SXE5. (CSCsc55949, CSCsd20092)

- An incoming differentiated services code point (DSCP) value is not trusted when packets arrive on a VLAN interface that is configured as a Layer 2 EtherChannel. This problem occurs when MLS QoS is enabled globally and the incoming DSCP is trusted by the VLAN-based QoS policy map attached on the interface. This problem is resolved in Release 12.2(18)SXE5. (CSCsc05210)
- A reload might occur because of a divide-by-zero exception. This problem occurs when you enter the **show policy-map interface interface-name output** command after removing a portion of a policy map that is configured with both a shaper and policer. This problem is resolved in Release 12.2(18)SXE5. (CSCsc25204)
- When a Reverse Path Forwarding (RPF) change affects approximately 30,000 multicast routes, a CPUHOG message might be displayed. This problem is resolved in Release 12.2(18)SXE5. (CSCek26627)
- A PA-A3 or PA-A6 port adapter in an Enhanced FlexWAN module, or an ATM SPA might not initialize correctly after a reload if it is configured for bridging using RFC1483 bridged routed encapsulation (BRE). The BRE Local Target Logic (LTL) is not populated properly and traffic does not pass from Ethernet to ATM on the BRE connection. This problem is resolved in Release 12.2(18)SXE5. (CSCsb89241)
- The **no mls qos mpls trust exp** command does not work after a reload. This problem is resolved in Release 12.2(18)SXE5. (CSCsc93283)
- A reload might occur when you remove a service policy after you enter the **mls qos mpls trust exp** command and then you enter the **no mls qos mpls trust exp** command. This problem is resolved in Release 12.2(18)SXE5. (CSCsc93607)

#### Resolved General Caveats in Release 12.2(18)SXE4

- A reload might occur if you reset an IPsec SPA or a IPsec VPNM that is supporting active IPsec tunnels. This problem is resolved in Release 12.2(18)SXE4. (CSCeh81794)
- An SVI for a VLAN carrying 1483 or 1490 multipoint bridging (MPB) traffic fails to forward multicast packets over a link in the VLAN. This problem occurs when the SVI is associated with a SPA or a port adapter on a FlexWAN module. This problem is resolved in Release 12.2(18)SXE4. (CSCei16701)
- Layer 3 traffic that ingresses over one port of a [distributed EtherChannel \(DEC\)](#), and then egressed over a different port in the same distributed EtherChannel, might cause continuous flooding after the first time the aging timer expires. This problem is resolved in Release 12.2(18)SXE4. (CSCsb38273)
- A system configured with Cisco IOS server load balancing (SLB) and multiple access interfaces might display several CPUHOG messages and suspend operations in the Cisco IOS SLB process. This problem is resolved in Release 12.2(18)SXE4. (CSCei01237)
- With Bridge Control Protocol (BCP) configured on a SIP-200 or a FlexWAN interface, the interface does not become part of STP after an OIR removal and reinsertion. This problem is resolved in Release 12.2(18)SXE4. (CSCei02695)
- Spurious memory accesses might occur on a SIP-200 module, a FlexWAN module, or an Enhanced FlexWAN module. This situation occurs when a service policy is attached to a Frame Relay serial interface containing at least one Data Link Control (DLC) connection with RFC 1490 bridging configured. This problem is resolved in Release 12.2(18)SXE4. (CSCei51175)

- The following log might appear when there is a switchover from the active to a standby supervisor engine:

```
00:10:45: %SYS-DFC-3-CPUHOG: Task is running for (4936)msecs, more than (2000)msecs
(0/0),process = SCP LC EVENT MGR.(c61c-sp-3-dso-b.so+0x76358)
```

This message is informational only; there are no other symptoms. This problem occurs on the WS-X6816-GBIC switching module only. This problem is resolved in Release 12.2(18)SXE4. (CSCsa82912)

- The Supervisor Engine 720 reloads after changing the spanning tree mode from per-VLAN spanning tree (PVST) to either Rapid Spanning Tree protocol (RSTP) or Multiple Spanning Tree (MST). This problem is resolved in Release 12.2(18)SXE4. (CSCsb04346)
- With BGP configured, a reload can occur after a switchover. This problem is resolved in Release 12.2(18)SXE4. (CSCsb69773)
- If you enter the **no ip vrf vrf\_name** command followed by any of the following commands, the supervisor engine reloads:
  - no ip multicast- routing**
  - no ip multicast-routing vrf vrf\_name**
  - no mls ip multicast**

This problem is resolved in Release 12.2(18)SXE4. (CSCsa95660)

- Traffic sent over a DEC, configured from a DFC-equipped module, to a WS-X67xx switching module can cause information to be lost about a MAC address learned over the DEC. This loss causes traffic from hosts that are connected from the DFC-equipped module to the MAC address to be flooded to all ports on the DEC. This problem is resolved in Release 12.2(18)SXE4. (CSCsb10662)
- IEEE 802.1x authentication takes approximately 150 seconds to authenticate 270 supplicants. This problem is resolved in Release 12.2(18)SXE4. (CSCsb29951)
- If a policy is configured with a no drop action, then no policer is allocated and no statistics are displayed even if you enter the **mls qos marking statistics** command.

**Workaround:** Because the policer with a no drop action is equivalent to a trust dscp action, you should configure the **trust dscp** command instead in software where this fix is not available. This problem is resolved in Release 12.2(18)SXE4. (CSCeh41511)

- ACL counters might display twice as many matches than actually exist. This problem occurs only when class maps are nested because the **rate-limit llq classify** command is configured along with class-based classification. When the ACL counters are used in policies with these class maps, the counts are included once for each of the classifications when displaying accounting output for the **show policy interface** command. Twice as many packets appear to have entered the network and are matched on these ACLs. This problem is resolved in Release 12.2(18)SXE4. (CSCee56209)
- When NHRP receives an invalid packet, it attempts to reply to the sender with an error message that contains part of the original packet. This situation might result in a large memory allocation and a traceback, memory alignment errors, address access errors, and possibly a system reload. This problem is resolved in Release 12.2(18)SXE4. (CSCin95836)

- A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

**Workaround:** Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL). By doing this, the offending router will not be able to participate within the mVPN data trees.

The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a rACL:

```
!
ip receive access-list 111
!
access-list 111 deny udp host <ip address of router sending malformed join
request> host 224.0.0.13 eq 3232
access-list 111 permit ip any any
!
```



**Note** Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to “Protecting Your Core: Infrastructure Protection Access Control Lists” at:

<http://www.cisco.com/warp/public/707/rACL.html>

This problem is resolved in Release 12.2(18)SXE4. (CSCsb52717)

- The following error messages might appear on the console and in the log:

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
-Process= "TTY Background", ipl= 6, pid= 20
-Traceback= 801BA4D4 801BA798 80114D94 801CEF34
```

This message indicates a situation that does not appear to affect any system service. The system generates these log messages when you enter the **terminal monitor** command and encounter excessive SSH traffic (such as debug messages). This problem is resolved in Release 12.2(18)SXE4. (CSCdy80670)

- Occasionally, the PS-Fan status in the **show power** command displays as n/a for a functional power supply. This problem is resolved in Release 12.2(18)SXE4. (CSCee01435)
- An attempt to make an active FTP connection to a Linux FTP server will fail and the following message will result:

```
425 Can't build data connection: connection refused.
```

This problem is resolved in Release 12.2(18)SXE4. (CSCeg06261)

- Some statics may not get redistributed into a VRF through RIPv2 protocol during a switchover. This problem is resolved in Release 12.2(18)SXE4. (CSCeh20051)
- The identification field in all TACACS+ packets is always 0 when the synchronize (SYN) flag is set and the TACACS+ packet goes through a firewall to the AAA server. The firewall interprets this 0 identification field as a Fragment Overlap Attack and drops additional new connections. This problem is resolved in Release 12.2(18)SXE4. (CSCeh48684)

- A reload might occur if you attempt to resequence an ACL. This problem occurs when you delete a few ACEs and then immediately enter the **ip access-list resequence** *access-list-name starting-sequence-number increment* command. This problem is resolved in Release 12.2(18)SXE4. (CSCsa50971)
- LSP ping packets or traceroute packets received with an untagged output interface are discarded. This situation causes the MPLS echo request packet to timeout while waiting for a reply. This problem is resolved in Release 12.2(18)SXE4. (CSCsa82640)
- A login authentication fails to appear as default after a VTY is configured. This problem is resolved in Release 12.2(18)SXE4. (CSCsa91175)
- In a multi-router automatic protection switching (APS) configuration with working routers and protect routers and traffic flowing through the active working router, if the working router is powered off, the protect becomes the active router and starts forwarding traffic with minimal packet loss. When the working router is reloaded, the protect router switches to the working router (before the working router's forwarding path is up), causing significant traffic loss. This problem is resolved in Release 12.2(18)SXE4. (CSCsa93725)
- You might see the following messages when configuring an EtherChannel on a WS-X6548-GE-TX module or a WS-X6548V-GE-TX module:

```
%CAPI_EC-4-RATE_LIMITED: Adding WS-X6548-GE-TX interfaces to an etherchannel will
limit channel throughput to 1 Gbps!
```

This problem is resolved in Release 12.2(18)SXE4. (CSCsb16475)

- On a provider edge (PE) router with multihop eBGP configured to the customer edge (CE) router, a per-VRF aggregate label might get deleted from the MPLS forwarding table. This problem occurs when a connected prefix comes up and when there is already a same prefix that is learned locally from eBGP or another PE-CE protocol. This problem is resolved in Release 12.2(18)SXE4. (CSCsb32695)
- If you attach QoS ACL to an interface that is in the MPLS to IP path, the ACL occasionally can cause traffic forwarding problems for the routes that use this path. This problem is resolved in Release 12.2(18)SXE4. (CSCsb33744)
- A DHCP client may fail to renew an IP address when DHCP snooping is enabled. This problem is resolved in Release 12.2(18)SXE4. (CSCsb36874)
- Some labels may be missing in the output of an LSP traceroute. This problem is resolved in Release 12.2(18)SXE4. (CSCsb38242)
- Network management systems (NMS) stations display an alert because a Supervisor Engine 720 control plane interface state is ifAdminStatus up but ifOperStatus is down. Also, when a switchover occurs, an SNMP trap (linkdown) is sent to the NMS. These problems are resolved in Release 12.2(18)SXE4. (CSCsb55343)
- A Supervisor Engine 720, configured for OSPF, EIGRP or BGP, may take up to two minutes for multicast RIP traffic to propagate on the first SSO switchover after a reload. The problem is isolated to a system operating in egress replication mode where the outgoing interfaces are local to DFC3B or DFC3A-equipped modules. This problem is resolved in Release 12.2(18)SXE4. (CSCsb71242)
- Spurious memory accesses might occur when the cbQosREDTailDropByte64 or cbQosREDRandomDropByte64 MIB objects (belonging to the CISCO-CLASS-BASED-QOS-MI) are polled using SNMP. This problem is resolved in Release 12.2(18)SXE4. (CSCdz84448)
- When a serial link is removed from a multilink bundle by entering the **no ppp multilink** command in the serial link configuration, the link remains at the line protocol down state and does not recover. This problem is resolved in Release 12.2(18)SXE4. (CSCei09755)

- The general packet radio service (GPRS) Tunneling Protocol (GTP) load-balancing feature that is configured for Intelligent Packet Solution (IPS) 2.0 stops functioning when the **mls ip slb search wildcard rp** command is entered.

The **mls ip slb search wildcard rp** command is recommended for IPS 2.0 because many Radius Load Balancer (RLB) and FireWall Load Balancer (FWLB) are configured as a part of the solution. Without this command, ternary content addressable memory (TCAM) capacity errors and other issues may be seen in the IPS 2.0 environment.

This problem is resolved in Release 12.2(18)SXE4. (CSCei37692)

- When the **crypto connect** mode is deconfigured, the interface defaults are updated to L3\_DENY in both the ingress and egress directions. This situation creates incorrect default results in the egress direction if the interface has been converted to a regular Layer 3 interface by configuring the ip address on this interface. This problem is resolved in Release 12.2(18)SXE4. (CSCei52441)
- A reload or spurious memory access occurs when HSRP rapidly changes states or goes up and down. This problem occurs with Cisco IOS SLB configured and with virtual servers that are monitoring these HSRP groups and probes that are configured on their server farms. This problem is resolved in Release 12.2(18)SXE4. (CSCin94752)
- When you use point-to-point GRE tunnels, non-RPF multicast traffic may get passed to the MSFC and forwarded to the network after an SSO switchover. This situation occurs for approximately 2 minutes after the switchover if the shared tree and the PIM shortest path tree have point-to-point GRE tunnels as incoming interfaces. This problem is resolved in Release 12.2(18)SXE4. (CSCsb02590)
- A system configured with MSDP does not send a triggered Source-Active (SA) message when it is the nondesignated router on a segment for a directly connected source. This situation can induce a delay in the start of the multicast stream for remote receivers. This problem is resolved in Release 12.2(18)SXE4. (CSCsb02976)
- When incremental shortest path first (iSPF) attaches a stub network to the shortest-path tree, it does not check for an existing transit network that describes the same network. This situation might cause a better route to be replaced by a worse route in the routing table. This problem is resolved in Release 12.2(18)SXE4. (CSCsb08380)
- An Cisco IOS SLB GTP virtual server may start rejecting calls when all the real servers in the server farm are in the MAXCONN state. This situation occurs under stress conditions when there are many simultaneous creations and deletions of sessions and when the sticky GTP international mobile subscriber identity (IMSI) feature is enabled on the server. No additional PDP contexts can be created through Cisco IOS SLB even though none of the GPRS Gateway Support Nodes (GGSNs) currently have any contexts. This problem is resolved in Release 12.2(18)SXE4. (CSCsb14175)
- A GTP Cisco IOS SLB server may reload when the GTP sticky IMSI feature is disabled while a Packet Data Protocol (PDP) context deletion is in progress. This problem is resolved in Release 12.2(18)SXE4. (CSCsb14306)
- A system that is configured with HSRP and proxy ARP, with no active HSRP groups, may respond to an ARP request with a MAC address of an HSRP group that is not configured. This problem is resolved in Release 12.2(18)SXE4. (CSCsb15224)
- Spurious memory accesses occur when a link goes down and up. This problem is resolved in Release 12.2(18)SXE4. (CSCsb23906)
- A reload may occur if IEEE 802.1X authentication is disabled and then reenabled while authentication is in progress. This problem is resolved in Release 12.2(18)SXE4. (CSCsb29783)

- The NetFlow process has excessive CPU utilization while NetFlow is enabled which continues after NetFlow is disabled. This problem was triggered by an Error-Correcting Code (ECC) correction of a hardware data error in the NetFlow table. This problem is resolved in Release 12.2(18)SXE4. (CSCsb34354)
- When all the GGSNs in a server farm send reassign notifications because of a call admission control failure, the Cisco IOS SLB maximum reassign counter may reach maximum value. If this situation occurs, Cisco IOS SLB fails to relay the create response back to the Serving GPRS Support Node (SGSN). This problem is resolved in Release 12.2(18)SXE4. (CSCsb37618)
- After a switchover, a reload may occur when you enter the **no snmp-server** command. This problem is resolved in Release 12.2(18)SXE4. (CSCsb44308)
- The **clear bgp ipv4 unicast \*** command clears IPv4 BGP peers from the routing table, but does not clear BGP routes from the routing table. The **clear bgp ipv6 unicast \*** command clears IPv6 BGP peers from the routing table, but does not clear BGP routes from the routing table. This problem is resolved in Release 12.2(18)SXE4. (CSCsa87034)
- SNMP polling of the IPsec MIBS (ciscoIPsecMIB, ciscoIpSecFlowMonitorMIB, and ciscoIpSecPolMapMIB) results in memory being held indefinitely by the device. This problem is resolved in Release 12.2(18)SXE4. (CSCec64333)
- Unicast traffic floods continuously to all ports in the VLAN instead of being forwarded only to the EtherChannel member ports. This situation occurs if you shut down member ports in a [distributed EtherChannel \(DEC\)](#) and leave active only the member ports served by a single fabric connection. This problem is resolved in Release 12.2(18)SXE4. (CSCsb16396)
- When you change the Next Hop Resolution Protocol (NHRP) mapping configuration, an incorrect NHRP cache entry and incorrect crypto socket entry may occur. When you change the NHRP static mapping entry by entering the **ip nhrp map** command, the NHRP cache entry is not updated with the new mappings and the crypto socket entry is incorrect. This problem is resolved in Release 12.2(18)SXE4. (CSCsb03192)
- After a switchover, traffic for OSPF routes might be suspended for approximately 10 to 15 seconds. This problem is resolved in Release 12.2(18)SXE4. (CSCsa95973)
- On an EtherChannel IEEE 802.1q trunk that is configured with VLAN 1 as the native VLAN, connectivity is lost if you change the native VLAN. This problem is resolved in Release 12.2(18)SXE4. (CSCsa80358)
- With a large number of interfaces configured, you might see this type of message:  

```
Error adding idb to list_type idb list
```

(*list\_type* can be a list name, for example, macaddr). This problem is resolved in Release 12.2(18)SXE4. (CSCsa80223)
- Inter-Card Communication (ICC) gets blocked during bootup if the routed MAC aging time is set to 0 (no aging) or the aging time is set to 0. This problem is resolved in Release 12.2(18)SXE4. (CSCsa76812)
- A reload may occur during an LSP traceroute when a transit router responds with a downstream map Type-Length-Value (TLV) that contains a multipath length field that is set to 0, 1, 2, or 3. This reload occurs during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. All implementations of the draft version 3 will encode the length as four bytes and reply with a multipath length of four bytes.



When an LSP traceroute is invoked, a transit router replies with a downstream map TLV that contains a multipath length field which is set to a length shorter than four bytes. This situation causes memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet.

**Workaround:** If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value less than four, do not invoke an LSP traceroute.

The implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this problem.

This problem is resolved in Release 12.2(18)SXE4. (CSCsa70274)

- Control plane policing (CoPP) may fail to match packets that arrive tagged with the VPN aggregate MPLS label. This problem is resolved in Release 12.2(18)SXE4. (CSCsa69060)
- An ISIS routing protocol **redistribute** *protocol* command is not synchronized to a redundant MSFC, and routes that are dependent on this command fail after a switchover. This problem is resolved in Release 12.2(18)SXE4. (CSCin65241)
- With a Supervisor Engine 720 and DFC3A-equipped switching modules, a memory allocation failure and reload might occur if you configure SPAN. This problem is resolved in Release 12.2(18)SXE4. (CSCei20107)
- When Compressed Real-Time Protocol (cRTP) errors occur, half of the cRTP packets are dropped. These drops are counted as output drops on the interface. This problem is resolved in Release 12.2(18)SXE4. (CSCei02826)
- An update in a bidirectional rendezvous point (Bidir RP) cache during a designated forwarder (DF) election might result in an erroneous path cost. This problem is resolved in Release 12.2(18)SXE4. (CSCeh95160)
- BGP next-hop information is not redistributed as expected by the OSPF routing protocol. This problem is resolved in Release 12.2(18)SXE4. (CSCeh92012)
- Unicast traffic carried by a [distributed EtherChannel \(DEC\)](#) can be transmitted from different member ports. When the DEC selects a member port supported by one DFC to transmit a packet, and reverse traffic of the same flow is being received by another member port supported by another DFC, the unicast traffic is flooded if the Layer 2 MAC address has aged out on the DFC that is transmitting the packet. This problem is resolved in Release 12.2(18)SXE4. (CSCeh73110)
- During a Non-Stop Forwarding (NSF) MSFC switchover, open shortest path first (OSPF) convergence may be delayed up to 5 minutes. This problem occurs when an OSPF Database Description (DBD) exchange error occurs while the adjacency is brought up. This problem is resolved in Release 12.2(18)SXE4. (CSCeh09588)
- When a VPN client acquires a login popup window and attempts to log in, the following popup windows are not displayed after the username and password. This problem is resolved in Release 12.2(18)SXE4. (CSCef07048)
- A supervisor engine may reload while a multiple number of ATM commands are being executed simultaneously on one ATM Virtual Circuit (VC) from different sessions. This problem occurs in a large configuration and is resolved in Release 12.2(18)SXE4. (CSCdw25402)
- With multiple equal-cost routes exiting on different interfaces, a Resource ReSerVation Protocol (RSVP) reservation may initially be made on the wrong interface. This problem is resolved in Release 12.2(18)SXE4. (CSCdt12296)
- Closing an existing Telnet session may cause the system to reset. This problem is resolved in Release 12.2(18)SXE4. (CSCds33629)

- With a large number of multicast routes being carried by GRE tunnels, a bus error and a reload might occur if the GRE tunnel interfaces go up and down frequently. This problem is resolved in Release 12.2(18)SXE4. (CSCsb95851)
- When there is a sticky International Mobile Subscriber ID (IMSI) object for an alternate GPRS Support Node (GGSN), a create request from a packet radio service (GPRS) Tunneling Protocol (GTP) server load balancer that is received after the GTP session times out might be forwarded to the alternate GGSN. This problem is resolved in Release 12.2(18)SXE4. (CSCsb48739)
- Memory corruption might cause a reload if you query the entire ciscoCBQos MIB object or if you poll the cbQosQueueingStatsTable MIB object or the cbQosPoliceStatsTable MIB object. This problem is resolved in Release 12.2(18)SXE4. (CSCeg03733)
- After you disable multicast VPN (MVPN) on a VRF interface, CPU utilization increases to 99 or 100 percent and remains at that level; or with a VRF interface configured, a reload might occur when you remove an MDT group from a remote PE router. These problems are resolved in Release 12.2(18)SXE4. (CSCeh61467)
- With a Supervisor Engine 720, egress traffic loss might occur if you configure the **wrr queue-limit** and **wrr random-detect max-threshold** commands to nondefault values. This problem is resolved in Release 12.2(18)SXE4. (CSCei33393)
- Reverse route injection (RRI) might incorrectly delete all routes to a remote proxy, including routes to different remote peers. This problem is resolved in Release 12.2(18)SXE4. (CSCei80006)
- IGMP snooping report suppression was inadvertently disabled. This problem is resolved in Release 12.2(18)SXE4. (CSCsb70973)
- When a Multiple Spanning Tree (MST) designated port receives a topology change (TC) from another MST region, it does not become a boundary port and it flushes only the internal spanning tree (IST) instance. This situation causes traffic loss in topologies that have VLANs mapped to instances other than the IST. This problem is resolved in Release 12.2(18)SXE4. (CSCsb79590)
- A traceback might occur after you enter the **hw-module module slot\_number reset** command. This problem is resolved in Release 12.2(18)SXE4. (CSCsb84998)
- If a switchover occurs on a Supervisor Engine 720 because of a fabric error, the system log does not indicate that the active fabric has been disabled because of the error. You can display this log by entering the **show svlog** command. This problem is resolved in Release 12.2(18)SXE4. (CSCsb60453)
- When a Reverse Path Forwarding (RPF) change occurs, a bidirectional PIM convergence may take up to 10 seconds. This problem is resolved in Release 12.2(18)SXE4. (CSCeh93087)
- A reload might occur when you enter the **default-information originate** RIP routing information command and you enter the **clear ip route EXEC** command. This problem is resolved in Release 12.2(18)SXE4. (CSCej21891)
- If IEEE 802.1X authentication is in progress on multiple ports and a link goes up and down, or if a module is removed or disabled, a memory corruption might occur, which could cause a reload. This problem is resolved in Release 12.2(18)SXE4. (CSCsb77716)
- If differentiated services code point (DSCP) mutation is configured on a switching module, and you OIR the module, DSCP mutation will no longer be configured. This problem might occur with IPv4 or IPv6 traffic. This problem is resolved in Release 12.2(18)SXE4. (CSCsb84405)
- A Telnet, SSH, or console session might suspend operation when you enter the **show policy-map** command or the **show class-map** command, or while configuring various modular QoS features. This problem occurs when one terminal session leaves these commands at the More prompt. Other

terminal sessions may suspend operation while configuring modular QOS features or executing other **show policy-map** or **show class-map** commands before the command in the original session has completed. This problem is resolved in Release 12.2(18)SXE4. (CSCed71844)

### Resolved General Caveats in Release 12.2(18)SXE3

- Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

This problem is resolved in Release 12.2(18)SXE3. (CSCeh73049)

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

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

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

This problem is resolved in Release 12.2(18)SXE3. (CSCei61732)

- When Multiprotocol Label Switching (MPLS) learns routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled, a label forwarding table entry might be missed. This problem can be seen in the output of the **show tag-switching forwarding-table EXEC** command for the missing entry and in the output of the **show ip cef detail EXEC** command for the prefix. This problem is resolved in Release 12.2(18)SXE3. (CSCsb09190)

### Resolved General Caveats in Release 12.2(18)SXE2

- Multicast Source Discovery Protocol (MSDP) does not create an (S,G) state and does not trigger (S,G) joins for the relevant entries in the MSDP cache when Internet Group Management Protocol (IGMP) modifies the (\*,G) o-list from null to non-null. This problem is resolved in Release 12.2(18)SXE2. (CSCeh01390)
- The multicast rate counter is not updated properly in the **show ip mroute active** command output. This problem is resolved in Release 12.2(18)SXE2. (CSCsa94063)
- The **ip routing protocol purge interface** command is not configurable. This problem is resolved in Release 12.2(18)SXE2. (CSCsb18066)
- The **ip igmp snooping source-only-learning age-timer 0** command does not disable source-only flooding. This problem is resolved in Release 12.2(18)SXE2. (CSCsb17320)
- Receipt of a Border Gateway Protocol (BGP) autonomous system (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.2(18)SXE2. (CSCeh13489)

- Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected.

Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

See the Security Advisory at the following URL for more details

<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

This problem is resolved in Release 12.2(18)SXE2. (CSCee45312)

- With MPLS configured, a reload might occur if there is a 0/0 entry in the routing table. This problem is resolved in Release 12.2(18)SXE2. (CSCsa91749)
- A reload occurs if you enter the **show platform tech-support ipmulticast** command. This problem is resolved in Release 12.2(18)SXE2. (CSCsb01729)
- With SSO redundancy mode and **snmp mib notification-log** commands configured, a reload occurs when you insert a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE2. (CSCsa98777)
- Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers in this situation:
  - At least two border routers are eBGP-connected to another autonomous system
  - The two border routers receive the same prefix over these connections
  - The two border routers redistribute the prefix into OSPF

Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer goes up and down, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers. This problem is resolved in Release 12.2(18)SXE2. (CSCsa98059)

- Erroneous “notPresent Temperature StatusValue Value =0” SNMP traps might be generated. This problem is resolved in Release 12.2(18)SXE2. (CSCsa91816)
- WCCP ingress-redirection traffic uses the NetFlow table for hardware switching when the Cache Engine is configured for GRE forwarding with the mask assignment mode. This situation causes WCCP ingress redirection to fail when the NetFlow table is full. This problem is resolved in Release 12.2(18)SXE2. (CSCsa90830)
- You cannot configure two different general packet radio service (GPRS) tunneling protocol (GTP) service virtual servers in the same sticky group. This problem is resolved in Release 12.2(18)SXE2. (CSCsa91166)
- Occasionally, the BGP-allocated per-VRF aggregate tag is not present in the label forwarding information base (LFIB). This situation causes destinations to be unreachable. This problem is resolved in Release 12.2(18)SXE2. (CSCsa85588)

- The IntMacTx-Err counter in the **show interface interface\_type counter error** command output might increment when there are no errors. This problem is resolved in Release 12.2(18)SXE2. (CSCsa77084)
- A reload might occur when the Resource ReSerVation Protocol (RSVP) MIB object is polled. This problem is resolved in Release 12.2(18)SXE2. (CSCsa57101)
- A crashinfo file generated as the result of communication failure between the MSFC and the supervisor engine does not contain sufficient diagnostic information. This problem is resolved in Release 12.2(18)SXE2. (CSCei18018)
- A reload might occur if a module resets during FPD image upgrade. This problem is resolved in Release 12.2(18)SXE2. (CSCeh82971)
- The online diagnostic TestL3VlanMet and TestIngressSpan tests fail on switching modules that have power-over-Ethernet (PoE) daughtercards installed, unless inline power support has been explicitly disabled on the first port on the module that passes the TestPortLoopback test. This problem is resolved in Release 12.2(18)SXE2. (CSCeh65615)
- At boot time, online diagnostics assume that the ASICs on switching modules are synchronized when they are not. This situation can cause the TestL3VlanMet, TestIngressSpan, and TestEgressSpan tests to fail on WS-6548-GE-TX and WS-6516A-GBIC switching modules. This problem is resolved in Release 12.2(18)SXE2. (CSCeh56398)
- Upon receipt of a Gateway General Packet Radio System (GPRS) Support Node (GGSN) reassign notification, Cisco IOS Server Load Balancing (SLB) might ignore a sticky database object for one GGSN and reassign the session to another alternate GGSN. This problem is resolved in Release 12.2(18)SXE2. (CSCeh54217)
- The order in which tests are run when complete diagnostics are enabled causes some tests to interfere with other tests and fail. This problem is resolved in Release 12.2(18)SXE2. (CSCeh51894)
- The source MAC addresses of traffic received on a Layer 2 **distributed EtherChannel (DEC)** might be learned in multiple VLANs. This problem is resolved in Release 12.2(18)SXE2. (CSCeh40945)
- The source MAC addresses of Layer 3-switched traffic received on a Layer 2 **distributed EtherChannel (DEC)** might be learned in multiple VLANs. This problem is resolved in Release 12.2(18)SXE2. (CSCei16381)
- With fast reroute (FRR) and VPN support configured, a reload might occur when a fast reroute happens. This problem is resolved in Release 12.2(18)SXE2. (CSCeh05594)
- When a PIM neighbor expires that is the designated forwarder (DF) for multiple rendezvous points (RPs), the DF election is triggered only for the first RP on the list and does not occur for all the other RPs. This problem is resolved in Release 12.2(18)SXE2. (CSCeg83460)
- The Resource ReSerVation Protocol (RSVP) reservation state of an MPLS Traffic Engineering (TE) Label Distribution Protocol (LDP) tunnel is not removed immediately when you shut down the outbound tunnel interface. This problem is resolved in Release 12.2(18)SXE2. (CSCef87449)
- If the configuration of a Cisco IOS SLB virtual server or firewall farm contains the **replicate slave** command but not the **replicate casa** command, a reload might occur when an HSRP group that is being monitored by the virtual server changes state. This problem is resolved in Release 12.2(18)SXE2. (CSCee58827)
- With the **tunnel key** command configured on a tunnel interface, any input ACLs on the tunnel interface are ignored. This problem is resolved in Release 12.2(18)SXE2. (CSCeb47225)

- These features do not support the RPR+ redundancy mode:
  - [DHCP snooping](#)
  - [Dynamic ARP inspection \(DAI\)](#)
  - [VACL Logging](#)
  - IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#))

This problem is resolved in Release 12.2(18)SXE2. (CSCsa87127)

- A reload might occur if you enter the **tfoot-server** command with a file name that is longer than 67 characters. This problem is resolved in Release 12.2(18)SXE2. (CSCsa82886)
- With Border Gateway Protocol (BGP) route redistribution configured to an Interior Gateway Protocol (for example, OSPF or EIGRP), routes might not be properly removed when a BGP-learned route is withdrawn. This situation might cause a control plane inconsistency and data plane forwarding loops. This problem is resolved in Release 12.2(18)SXE2. (CSCsa80861)
- A small memory leak occurs when you configure PIM on a point-to-point tunnel interface. This problem is resolved in Release 12.2(18)SXE2. (CSCsa78705)
- Following an NSF with SSO switchover with OSPF NSF configured, OSPF traffic loss occurs for a few seconds because neighboring OSPF routers withdraw the OSPF routes. This problem is resolved in Release 12.2(18)SXE2. (CSCsa74271)
- With the default flow control configuration, the ports in an unstable link between a Supervisor Engine 720 equipped with a copper SFP and a port in a chassis with a Supervisor Engine 2 remain in the “up/down” state. This problem is resolved in Release 12.2(18)SXE2. (CSCsa61788)
- IGMP snooping does not constrain multicast traffic for multicast group addresses in the range x.128-255.x.x until a receiver joins the multicast group. This problem is resolved in Release 12.2(18)SXE2. (CSCeh62522)
- With Cisco IOS SLB configured, hardware-accelerated egress IOS ACLs configured on a VLAN interface might be applied to ingress bridged traffic. This problem is resolved in Release 12.2(18)SXE2. (CSCeh54533)
- [PA-MC-8TE1+](#) port adapters fail to check and drop invalid packets with a datagram size of one byte. This problem is resolved in Release 12.2(18)SXE2. (CSCin78324)

## Resolved General Caveats in Release 12.2(18)SXE1

- There is reduced performance for traffic between non-DFC-equipped switching modules and DFC-equipped switching modules, and some additional Layer 2-traffic flooding occurs. This problem is resolved in Release 12.2(18)SXE1. (CSCsa76290)
- The system resets because of a TestSPRPInbandPing failure after QoS is enabled and is incorrectly applied to the traffic. This problem is resolved in Release 12.2(17d)SXE1. (CSCsa63184)
- On a Supervisor Engine 2, MAC addresses unnecessarily age out every 4 seconds. This problem is resolved in Release 12.2(18)SXE1. (CSCef66632)
- When an EtherChannel trunk is configured to carry many VLANs, traffic pauses for as much as several seconds when you add or remove member ports from the EtherChannel. This problem is resolved in Release 12.2(17d)SXE1. (CSCef33051)
- In VTP transparent mode, the VLAN database might be lost after a VTP configuration error occurs. This problem is resolved in Release 12.2(18)SXE1. (CSCef47414)



## Resolved General Caveats in Release 12.2(18)SXE

- Multiple Cisco products contain vulnerabilities in the processing of IPsec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for IPsec and can be repeatedly exploited to produce a denial of service.

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

This advisory is posted at

<http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml>.

This problem is resolved in Release 12.2(18)SXE. (CSCed94829)

- In releases where [CSCdz75507](#) is resolved, you cannot configure fall-back bridging on any subinterface under a physical interface where MPLS is configured on another subinterface. This problem is resolved for ATM interfaces in Release 12.2(18)SXE. (CSCeb87433; also see resolved caveat [CSCee00239](#))
- In releases where [CSCdz75507](#) is resolved, you cannot configure fall-back bridging on any subinterface under a physical interface where MPLS is configured on another subinterface. This problem is resolved for Frame Relay interfaces in Release 12.1(23)E. (CSCee00239; also see resolved caveat [CSCeb87433](#))
- If you enter the **ip verify unicast reverse-path** interface configuration command on ATM subinterfaces, some ingress traffic is dropped. This problem is resolved in Release 12.2(18)SXE. (CSCdt51547)
- If you enter a **write memory** command, the module in the redundant supervisor engine slot reloads, and you might see one of the following messages:

```
CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 6 for software recovery, Reason: Failed
TestMacNotification
CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 6 for software recovery, Reason: Failed
TestFabricCh0Health
```

This problem occurs where there is either a redundant supervisor engine or a DFC-equipped module in the redundant supervisor engine slot. This problem is resolved in Release 12.2(18)SXE. (CSCeg29451)

- Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

This problem is resolved in Release 12.2(18)SXE. (CSCef68324)

- Ports on a [WS-X6748-GE-TX](#) switching module, hardware revision 2.1, stop sending traffic when configured to operate only at 10 Mbps or only at 100 Mbps. This problem is resolved in Release 12.2(18)SXE. (CSCsa76031)
- After switchover to a redundant supervisor engine with EIGRP stub routing configured, EIGRP neighbors do not see routes. This problem is resolved in Release 12.2(18)SXE. (CSCin84644)

- A reload might fail because the software image does not decompress. This problem is resolved in Release 12.2(18)SXE. (CSCin53807)
- In egress multicast replication mode, after online insertion or removal (OIR) of a module, some fabric channel utilization might be higher than normal because some multicast traffic is sent across the switch fabric more than often than is necessary. This problem is resolved in Release 12.2(18)SXE. (CSCeg28814)
- In rare situations, a ROMMON upgrade for these modules might fail:
  - [WS-X6704-10GE](#)
  - [WS-X6748-SFP](#)
  - [WS-X6724-SFP](#)
  - [WS-X6748-GE-TX](#)

This problem is resolved in Release 12.2(18)SXE. (CSCee37771)

- The SNMP ifInDiscards value incorrectly resets to zero. This problem is resolved in Release 12.2(18)SXE. (CSCef76161)
- If you configure multiple IP service level agreement (SLA) jitter probes to send packets to the same destination IP address and port number, and you turn the responder router off and back on, the probes show traffic loss (displayed as the packetMIA value) that is equal to the probe's number of packets minus one. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg64124)
- Several MIB entity tables share one entCacheFlag and under rare circumstances, accessing the MIB entity tables might cause an entCacheFlag state that is not valid for all the MIB entity tables and a reload might occur. This problem is resolved in Release 12.2(18)SXE. (CSCeg19038)
- In a configuration with many routes and many routing changes, you might see IPC-3-NOBUFF messages indicating that the IPC message header cache is exhausted and a reload might occur. This problem is resolved in Release 12.2(18)SXE. (CSCeg08562)
- Modifying the configuration of statically configured bidirectional PIM rendezvous points (RPs) can cause very high CPU utilization. This problem is resolved in Release 12.2(18)SXE. (CSCef36367)
- With OSPF routing configured, and with default routes learned from multiple autonomous system boundary routers (ASBRs) as equal cost paths, reconfiguring the cost of one of the interfaces for the default routes does not correctly update the routing table. This problem is resolved in Release 12.2(18)SXE. (CSCee16068)
- After a reload of a Supervisor Engine 2 with DFC-equipped switching modules, Gateway Load Balancing Protocol (GLBP) traffic might be routed in software on the MSFC2, because the GLBP virtual MAC address might not be enabled. This problem is resolved in Release 12.2(18)SXE. (CSCee70075)
- On a Supervisor Engine 720, the **show version** command might display an incorrect cause for a reload. This problem is resolved in Release 12.2(18)SXE. (CSCef80423)
- With redundant Supervisor Engine 720s configured to support NSF and multicast, multicast groups with a large number of output interfaces (for example, more than 170) that are being Layer 3 switched in hardware are routed in software after an NSF with SSO switchover. This problem is resolved in Release 12.2(18)SXE. (CSCee79348)
- When the FIB TCAM is full, CPU utilization might be unacceptably high. This problem is resolved in Release 12.2(18)SXE. (CSCeb85827, CSCeb29888, CSCec14802, CSCec42634, CSCed58661, CSCee00311, CSCee22821, CSCin77977, CSCin78030, CSCin80590)



- Subinterfaces on these ports do not provide hardware switching for IPv4 multicast traffic:
  - Ethernet1/1
  - FastEthernet1/1
  - GigabitEthernet1/1
  - TenGigabitEthernet1/1

This problem is resolved in Release 12.2(18)SXE. (CSCec77178, CSCed26629, CSCef91498)

- With a PFC3, on Layer 3 interfaces that are configured to support IPX routing, but which are not configured with an IP address, the **mls rate-limit** commands incorrectly limit IPX traffic. This problem is resolved in Release 12.2(18)SXE. (CSCee09692)
- With RPR+ redundancy mode configured, the supervisor engine might fail bootup diagnostics with an “AclPermit” test failure and a reload. This problem is resolved in Release 12.2(18)SXE. (CSCef20654)
- You might see “Port Manager Internal Software Error” messages and tracebacks on the console of a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE. (CSCef50171)
- Ignore “Cannot encode data descriptor LI-Null0” messages on the console of a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE. (CSCef72939)
- If you enter the **no ip vrf vrf\_name** command in one administrative session, a reload might occur if you enter the **ip vrf vrf\_name** command for the same VRF in another administrative session before the deletion process completes. This problem is resolved in Release 12.2(18)SXE. (CSCeg51793)
- While the output of the **show ip mroute vrf vrf\_name** command is being displayed in one administrative session, a reload might occur if you enter the **no ip vrf vrf\_name** command for the same VRF in another administrative session. This problem is resolved in Release 12.2(18)SXE. (CSCeg52076, CSCeg55595)
- When two ports in the same VLAN on different DFC-equipped switching modules send bidirectional traffic to each other, and you configure one of the ports as an egress SPAN source port, then the traffic sent to that port is flooded to all the ports in the VLAN. This problem is resolved in Release 12.2(18)SXE. (CSCin78242)
- With a Supervisor Engine 720, if you enter the **mls ip cef load-sharing simple** command, traffic might be lost that uses MPLS adjacencies for routes that have a next hop that is reachable through an MPLS cloud. This problem is resolved in Release 12.2(18)SXE. (CSCsa50071, CSCeg71317)
- With RPR+ mode configured, after you enter the **clear cef linecard** command, RPR+ information might not be displayed correctly in the output of the **show cef linecard** command. This problem is resolved in Release 12.2(18)SXE. (CSCuk41411)
- Ignore spurious memory access errors during an SSO switchover. This problem is resolved in Release 12.2(18)SXE. (CSCuk49384, CSCed64648, CSCeb55269, CSCed44945, CSCed47559, CSCed50801, CSCed51914, CSCed64843, CSCed80188, CSCed88244, CSCee10565, CSCee19150, CSCee32558, CSCee42141, CSCee56069, CSCee59872, CSCin70853, CSCin72244)
- With policy-based routing (PBR) configured, you might see “ALIGN-3-SPURIOUS” and “ALIGN-3-TRACE” messages. This problem is resolved in Release 12.2(18)SXE. (CSCef70083)
- A reload might occur when you enter the **shutdown** and **no shutdown** interface configuration command for the interface that connects to an IP EIGRP neighbor, and then you enter the **show ip eigrp neighbors EXEC** command. This problem is resolved in Release 12.2(18)SXE. (CSCdu59038)
- The **show interface summary** command might truncate some of the final characters of an interface name. This problem is resolved in Release 12.2(18)SXE. (CSCdx62060)

- You might see high CPU utilization if you enter the logging synchronous command for line con 0. This problem is resolved in Release 12.2(18)SXE. (CSCdy01705)
- With a Y-cable Automatic Protection Switching (APS) configuration, there might be 30 to 45 seconds of traffic loss following an APS switchover. This problem is resolved in Release 12.2(18)SXE. (CSCdz66609)
- Cisco IOS software does not prevent simultaneous **erase nvram:** and **write memory** commands from different Telnet or console sessions. This problem is resolved in Release 12.2(18)SXE. (CSCea20169)
- Routing Information Protocol version 2 (RIPv2) routes get stuck in the routing table, even if the next hop interface is down. This problem is resolved in Release 12.2(18)SXE. (CSCea47597)
- With MD5 password encryption configured, the software does not correctly verify that all configured TCP options can be sent in a TCP packet, which can cause this message to be displayed:  

```
%TCP-6-TOOBIG: Tty0, too many bytes of options (44)
```

This problem is resolved in Release 12.2(18)SXE. (CSCeb07106)

- The “Do Not Learn” bit is not set in Layer 2 traffic processed by bridge groups on the MSFC. This problem is resolved in Release 12.2(18)SXE. (CSCeb56814)
- The BGP **set community none** command does not work; prefixes are not advertised to external peers. This problem is resolved in Release 12.2(18)SXE. (CSCeb69972)
- With Multicast Source Discovery Protocol (MSDP) configured, a reload might occur if you enter the **show ip msdp peer ip\_address advertised-SAs** command. This problem is resolved in Release 12.2(18)SXE. (CSCec23559)
- In a PIM dense mode environment, a forwarding interface might be pruned because join messages are delayed. This problem is resolved in Release 12.2(18)SXE. (CSCec37022)
- Because the WCCP service group list is scanned in the order in which service groups are created, rather than by priority, with multiple dynamic WCCP services defined, traffic that matches the selection criteria for more than one service group is not redirected to the service group with the highest priority. This problem is resolved in Release 12.2(18)SXE. (CSCec55429)
- In an SSM/IGMPv3 environment under a topology where a non-designated router (non-DR), but not the designated router (DR), is in the Shortest Path Tree (SPT), it may take the non-DR up to 3-1/2 minutes to prune and time-out its outgoing interface when all interested receivers have left an (s,g) group. This problem is resolved in Release 12.2(18)SXE. (CSCed12688)
- If you enable PIM on a VLAN interface and configure a bridge group on the VLAN interface, and then remove the PIM configuration from the VLAN interface, EIGRP neighborships are lost. This problem is resolved in Release 12.2(18)SXE. (CSCed12722)
- Configuration of fair queuing fails on virtual-template interfaces. This problem is resolved in Release 12.2(18)SXE. (CSCed54330)
- When an OSPF external route has a forwarding address with a next hop address in the routing table, the next hop address does not get updated in the type 5 link-state advertisement (LSA) when the forwarding address gets a more specific entry in the routing table with a different next hop address. This problem is resolved in Release 12.2(18)SXE. (CSCed59370)
- After you configure a tunnel to support DECnet with assigned DECnet cost and then delete the tunnel configuration, a reload might occur if you disable DECnet routing. This problem is resolved in Release 12.2(18)SXE. (CSCed88563)
- In a topology with overlapping networks, EIGRP might incorrectly remove a connected route if you add a new **network** command before you remove the old one. This problem is resolved in Release 12.2(18)SXE. (CSCed93804)

- HSRP tracking might incorrectly track two instances of the same interface, stating that one instance is down while the other is up. This situation causes the HSRP priority to be decremented by 10. This problem is resolved in Release 12.2(18)SXE. (CSCed95701)
- When an OSPF neighbor on a local IP segment has multiple interfaces on that IP segment, OSPF installs only a single next-hop entry to routes reachable through the OSPF neighbor, instead of multiple next-hop entries, as required by RFC 2328. This problem is resolved in Release 12.2(18)SXE. (CSCee21928)
- With Cisco IOS SLB configured, a reload might occur if you remove the Cisco IOS SLB configuration while the Cisco IOS SLB virtual servers are handling traffic. This problem is resolved in Release 12.2(18)SXE. (CSCee23087)
- If you enter the **debug ip slb connections acl** command, the debugging output might consume all available resources. This problem is resolved in Release 12.2(18)SXE with the **debug ip slb connections [state] [acl\_name]** command. (CSCee33923)
- If you enter the **attach** command through the Cisco IOS web browser interface, a reload might occur. This problem is resolved in Release 12.2(18)SXE. (CSCee56618)
- With policy-based routing (PBR) and an input ACL configured on the same interface, if you enter the **clear arp-cache** command, PBR is done in software instead of hardware. This problem is resolved in Release 12.2(18)SXE. (CSCee58127)
- A reload might occur when a distance vector multicast routing protocol (DVMRP) tunnel is configured and routing information is being redistributed between DVMRP and MBGP. This problem is resolved in Release 12.2(18)SXE. (CSCee66936)
- Policing might not be accurate for packets smaller than 82 bytes. This problem is resolved in Release 12.2(18)SXE. (CSCee78451)
- The maximum value displayed for VRF multicast route uptime is seven weeks. This problem is resolved in Release 12.2(18)SXE. (CSCee84457)
- Spurious memory accesses might occur if you remove DECnet configuration commands associated with a tunnel interface. This problem is resolved in Release 12.2(18)SXE. (CSCee88936)
- When you configure a static PIM rendezvous point (RP) IP address with an ACL that specifies the groups for the RP, and there is also another RP IP address configured without an ACL, you cannot remove the first RP IP address from the configuration. This problem is resolved in Release 12.2(18)SXE. (CSCee93574)
- When configured as an IEEE 802.1Q trunk, ports on these modules might drop all native VLAN traffic:
  - Supervisor Engine 2
  - [WS-X6408-GBIC](#)
  - [WS-X6408A-GBIC](#)
  - [WS-X6416-GE-MT](#)
  - [WS-X6416-GBIC](#)
  - [WS-X6516-GBIC](#)
  - [WS-X6516A-GBIC](#)
  - [WS-X6816-GBIC](#)
  - [WS-X6316-GE-TX](#)
  - [WS-X6516-GE-TX](#)

This problem is resolved in Release 12.2(18)SXE. (CSCef23302)

- If you configure a SPAN destination port on any of these modules, and the SPAN destination port goes down and comes back up, ingress traffic through other ports on the same port ASIC as the SPAN destination port might experience high latency:
  - Supervisor Engine 2
  - [WS-X6408-GBIC](#)
  - [WS-X6408A-GBIC](#)
  - [WS-X6416-GE-MT](#)
  - [WS-X6416-GBIC](#)
  - [WS-X6516-GBIC](#)
  - [WS-X6516A-GBIC](#)
  - [WS-X6816-GBIC](#)
  - [WS-X6316-GE-TX](#)
  - [WS-X6516-GE-TX](#)

This problem is resolved in Release 12.2(18)SXE. (CSCef32513)

- Following a reload when multicast routing and PIM are configured, the **no mls ip multicast non-rpf cef** command appears in the configuration file. This problem is resolved in Release 12.2(18)SXE. (CSCef36986)
- With power supplies of significantly different wattages in an [OSR-7609](#) or [WS-C6509-NEB](#) chassis, a reload might occur when a module powers up. This problem is resolved in Release 12.2(18)SXE. (CSCef62539)
- The SNMP portEntPhysicalIndex MIB object is not implemented for the [WS-X6316-GE-TX](#) switching module. This problem is resolved in Release 12.2(18)SXE. (CSCef83162)
- The BPDU guard feature does not work on an access port when you configure a voice VLAN unless either the voice VLAN or the access VLAN is VLAN 1. This problem is resolved in Release 12.2(18)SXE. (CSCef93371)
- The hardware switching information for (\*,G) multicast traffic might not be consistent with the software routing table. This problem is resolved in Release 12.2(18)SXE. (CSCeg13661)
- When you reconfigure the forwarding method for a cache engine service from Layer 2 redirection to GRE tunneling, the MLS flow mask is not amended appropriately. This situation might cause suboptimal performance. This problem is resolved in Release 12.2(18)SXE. (CSCin79644)
- The **interface range** command syntax requires spaces. This problem is resolved in Release 12.2(18)SXE. (CSCin82081)
- After a reload, multicast sources in secondary IP subnets cannot register immediately. This problem is resolved in Release 12.2(18)SXE. (CSCsa39767)
- In a release where caveat [CSCec55429](#) is resolved, after a number of Web Cache Communication Protocol (WCCP) “cache lost” and “cache found” events have occurred for all the caches in a service group, spurious memory accesses might occur, the addition and deletion of WCCP services might fail, and the **show ip wccp** command displays the WCCP service, but the output of the **show ip wccp service\_number** command does not show the WCCP service. This problem is resolved in Release 12.2(18)SXE. (CSCuk50878)
- The system resets because of a TestSPRPInbandPing failure after QoS is enabled and is incorrectly applied to the traffic. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa63184)
- On a Supervisor Engine 2, MAC addresses unnecessarily age out every 4 seconds. This problem is resolved in Release 12.2(18)SXE. (CSCef66632)

- When an EtherChannel trunk is configured to carry many VLANs, traffic pauses for as much as several seconds when you add or remove member ports from the EtherChannel. This problem is resolved in Release 12.2(18)SXE. (CSCef33051)
- In VTP transparent mode, the VLAN database might be lost after a VTP configuration error occurs. This problem is resolved in Release 12.2(18)SXE. (CSCef47414)
- When the *keep-exchanges* argument in the **frame-relay lmi-n391dte** command has a value that is lower than 3, Frame Relay autosensing does not function. This problem is resolved in Release 12.2(18)SXE. (CSCea30197)
- When you enter the **show controllers pos slot-number pm time-interval** command SONET statistics for POS interfaces are not displayed in the correct order in the output. The order of display should be the most recent first. This problem is resolved in Release 12.2(18)SXE. (CSCea70822)
- When using the **no ip-next-hop-self** setting, EIGRP routes in the routing table state might retain old information even though the EIGRP topology database has been updated. This problem is resolved in Release 12.2(18)SXE. (CSCee19880)
- If you configure fallback bridging on a Layer 3 LAN port, established OSPF neighbors might be put into the INIT state. This problem is resolved in Release 12.2(18)SXE. (CSCef66899)
- With a Supervisor Engine 2, QoS does not preserve the CoS value derived from IP precedence in traffic that originates on the MSFC2. This problem is resolved in Release 12.2(18)SXE. (CSCef68801)
- When you use an **snmpget** command for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the system responds with the following information:

```
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such Instance.
```

However, an **snmpwalk** executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6. This problem is resolved in Release 12.2(18)SXE. (CSCef79968)

- With Per-VLAN-Spanning Tree (PVST) configured, if you remove a DFC-equipped switching module, other DFC-equipped switching modules might retain some Layer 2 address entries for the removed module. Traffic loss occurs when the remaining DFC-equipped switching modules send traffic to the removed module. This problem is resolved in Release 12.2(18)SXE. (CSCef84129)
- Layer 2 EtherChannels configured with ports on different DFC-equipped switching modules periodically purge and refresh their Layer 2 address tables. Typically, the refresh takes a few seconds as the EtherChannel learns the destination MAC addresses, during which time the EtherChannel floods all egress traffic to other ports in the VLAN as unknown unicast traffic. With a Layer 2 EtherChannel configured with ports on different DFC-equipped switching modules, the EtherChannel might flood traffic for several minutes. This problem is resolved in Release 12.2(18)SXE. (CSCeg39091)
- If you insert a CSM in a running system, and then reset the module by entering the **hw-module module module slot number reset** command, the active supervisor engine resets. This problem is resolved in Release 12.2(18)SXE. (CSCeg77264)
- A reload might occur when PIM traffic is on the network. This problem will probably occur during initialization, but could occur anytime an interface goes up and down while receiving PIM traffic. This problem is resolved in Release 12.2(18)SXE. (CSCeh15639)
- A routing table entry for a Cisco IOS Server Load Balancing (SLB) virtual server is removed when the IP address of the virtual server is advertised as active for the host route and the backup server farm takes over. As a result, connectivity is lost to the backup server farm virtual server and its real servers. This problem is resolved in Release 12.2(18)SXE. (CSCeh17417)

- A system may stop receiving multicast traffic. This problem occurs rarely during convergence when a system receives a Join message on an Reverse Path Forwarding (RPF) interface and when a downstream router converges faster than the first router that receives the Join message.

In this situation, the system does not populate the RPF interface into the outgoing interface list (OIL) (the OIL remains null) because the old SP tree has already been pruned by the downstream router. When the RPF interface of the system changes to the new path later, it does not trigger a Join message toward the multicast source until the system receives the next periodic Join message from the downstream router and populates the OIL. Multicast traffic stops temporarily but no longer than the periodic Join message interval.

This problem is resolved in Release 12.2(18)SXE. (CSCeh47667)

- When you configure a Gigabit Ethernet interface with the **mode dot1q-in-dot1q access-gateway** interface configuration command, you might experience a halt in traffic on the subinterface if you also use the **encapsulation dot1q** *vlan* command to change the trunk VLAN while the **bridge-domain** *vlan* command is configured. This problem is resolved in Release 12.2(18)SXE. (CSCeh51395)
- With a Supervisor Engine 2, a memory leak might occur in the medium buffers. This problem is resolved in Release 12.2(18)SXE. (CSCsa47573)
- The system may reset if it receives a invalid VTP packet. The invalid VTP packet must be received on a port configured for ISL or 802.1q trunking and must correctly match the VTP domain name. This problem does not affect switch ports configured for the voice VLAN. This problem is resolved in Release 12.2(18)SXE. (CSCsa67294)
- Incoming MPLS packets that exit on a non-MPLS interface (tag to IP path) on which some output feature is configured (for example, egress ACL or egress WCCP) might not have the output features applied. This problem occurs because the output ACL lookup is bypassed. This problem is resolved in Release 12.2(18)SXE. (CSCsa67611)
- The SVI interface input buffer stops processing when the traffic generated by a directly connected network scanner fills the input buffer to capacity with accounting-request or access-request packets. Overflowing this buffer causes the new ingress traffic to be routed in software on the MSFC. The packets in the input buffer are no longer processed. This problem is resolved in Release 12.2(18)SXE. (CSCsa74002)
- With OSPF and MPLS traffic engineering configured, a reload might occur that is related to MPLS TE bandwidth management. This problem occurs on a system in which the interfaces, OSPF adjacencies, and TE tunnels are going up and down and more than 300 OSPF interfaces exist (in any state including admin down) in the OSPF area that is configured for MPLS traffic engineering. This problem is resolved in Release 12.2(18)SXE. (CSCsa77411)
- A CPUHOG message might display when the system is configured with 200 multicast groups and processing traffic from 2000 hosts. This problem does not affect performance. This problem is resolved in Release 12.2(18)SXE. (CSCdy64412)
- The output counters in the **show frame-relay pvc** *maplist* command are not being updated for either IP traffic or MPLS traffic. This problem is resolved in Release 12.2(18)SXE. (CSCec08821)
- In rare circumstances, a group of four ports (1 to 4, 5 to 8, 9- to 12, or 13 to 16) on the WS-X6516-GE-TX module may experience connectivity problems. If this problem occurs, the following syslog messages might be seen:

```
%PM_SCP-SP-6-LCP_FW_ERR_INFORM: Module 4 is experiencing the following error:
Pinnacle #0 Frames with Bad Packet CRC Error (PI_CI_S_PKT_CRC_ERR - 0xC7) = 110
```

This problem is resolved in Release 12.2(18)SXE. (CSCef46923)

## FlexWAN Caveats in Release 12.2(18)SXE and Rebuilds

- [Open FlexWAN Caveats in Release 12.2\(18\)SXE6a, page 319](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE6a, page 319](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE6, page 319](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE5, page 319](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE4, page 320](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE3, page 321](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE2, page 322](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE1, page 322](#)
- [Resolved FlexWAN Caveats in Release 12.2\(18\)SXE, page 322](#)

### Open FlexWAN Caveats in Release 12.2(18)SXE6a

None.

### Resolved FlexWAN Caveats in Release 12.2(18)SXE6a

None.

### Resolved FlexWAN Caveats in Release 12.2(18)SXE6

- A link to an EIGRP neighbor established over an ATM IMA interface might fail because of an authentication failure even though EIGRP authentication is not configured. This problem is resolved in Release 12.2(18)SXE6. (CSCeg77104)
- ATM OAM PVCs on a FlexWAN module or an Enhanced FlexWAN module might fail to transmit packets after a reload of the system or an OIR of the switching module. This situation occurs because the OAM packets are not processed and remain in the output queues. This problem occurs with a PA-A3-OC3 port adapter that is configured with a service policy. This problem is resolved in Release 12.2(18)SXE6. (CSCsd71119)
- The alarm LED on the PA-MC-8TE1+ stays on even if all the ports on the PA are shutdown. This problem is resolved in Release 12.2(18)SXE6. (CSCsd14307)

### Resolved FlexWAN Caveats in Release 12.2(18)SXE5

- With a PA-MC-8E1 port adapter, performance might be impaired if you configure Real-Time Protocol (RTP) Header compression on multilink PPP interfaces. This problem is resolved in Release 12.2(18)SXE5. (CSCeg47659)
- ATM multipoint bridging might stop working when there is a mismatch in the FPD version of the Enhanced FlexWAN module ROMMON software. This problem is resolved in Release 12.2(18)SXE5. (CSCsb31368)
- A system configured with a FlexWAN or an Enhanced FlexWAN module might experience memory allocation errors if it has a large QoS configuration. This problem is resolved in Release 12.2(18)SXE5. (CSCsb80590)
- A memory leak occurs when a FlexWAN module equipped with an ATM PA-A3 port adapter is removed. If the module is reinstalled, the loss stops. Otherwise the system will eventually run out of memory and reload. This problem is resolved in Release 12.2(18)SXE5. (CSCsc44237)

- A reload might occur on a system configured with a FlexWAN module with a channelized T1/E1 port adapter installed. This problem occurs after 5 or 6 hours of bidirectional voice over IP (VoIP) traffic through a multiple link point-to-point protocol (MLPPP) bundle link. A buffer leak eventually causes a memory allocation error to occur. This problem is resolved in Release 12.2(18)SXE5. (CSCei86192)
- When you attempt to bring up a multilink interface, the interface may go up and down continuously on one side. Also, when the master link of the Multilink PPP (MLP) bundle interface goes down, traffic may stop flowing through the multilink interface. This situation occurs on a system that has non-channelized serial port adapters, such as a 4-port enhanced serial port adapter (PA-4T+) or an 8-port serial port adapter (PA-8T), and that is configured for distributed MLP. This problem is resolved in Release 12.2(18)SXE5 (CSCin44386)
- In a distributed link fragmentation and interleaving over ATM (dLFIoATM) configuration, packets ingressing on an ATM FlexWAN interface with ATM Cell Loss Priority (CLP) will not be decoded correctly. This situation requires that the packets to be routed in software on the MSFC instead of being Layer 3 switched in hardware. This problem is resolved in Release 12.2(18)SXE5. (CSCsb97950)
- When you enter the **fair-queue** command for a FlexWAN interface, the command is not saved in the running configuration and is lost after a reload. This problem is resolved in Release 12.2(18)SXE5. (CSCee58986)
- ATM protocol data units (PDUs) might stop ingressing over a WS-X6582-2PA Enhanced FlexWAN module. All of the VCs configured on the ATM interface lose connectivity. This problem is resolved in Release 12.2(18)SXE5. (CSCsb85049)
- A FlexWAN module reloads continuously if it has a service policy that is attached to a Frame Relay data-link connection identifier (DLCI), and the service policy has fair queueing configured. This problem occurs on a system configured with Frame Relay fragmentation. This problem is resolved in Release 12.2(18)SXE5 (CSCsc95511)
- FlexWAN modules might reload on a system that is configured with Modular QoS CLI (MQC). This problem occurs when the physical interface is in the UP state and the following conditions occur:
  - An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
  - You remove the policy map from the PVC and attach the same policy map to the main interface.
  - You remove the policy map from the main interface.

All FlexWAN modules will reload even though there is no traffic processing when these conditions occur. This problem is resolved in Release 12.2(18)SXE5. (CSCsb12969)

#### Resolved FlexWAN Caveats in Release 12.2(18)SXE4

- When IP RTP header-compression (IPHC) is configured on an interface on bay 1 of a FlexWAN or an Enhanced FlexWAN module, the IPHC counters do not update. This problem is resolved in Release 12.2(18)SXE4. (CSCeh97017)
- A Supervisor Engine 720 configured with a FlexWAN module that has synchronous transfer mode (STM) port adapters might fail to release memory. This occurs when links on unused interfaces go up and down excessively. This problem is resolved in Release 12.2(18)SXE4. (CSCsb64812)
- On a system configured with an Enhanced FlexWAN module and a PA-2CT3 port adapter, if the traffic rate becomes high enough to induce input overrun errors, the input rate degrades by approximately 50 percent. This problem is resolved in Release 12.2(18)SXE4. (CSCei51155)



- With a WS-X6182-2PA FlexWAN module installed, you might see messages similar to these about spurious accesses from the FlexWAN module:

```
SLOT 4/0: May 27 08:24:49: %ALIGN-3-SPURIOUS: Spurious memory access
made at 0x60336D
44 reading 0x44
SLOT 4/0: May 27 08:24:49: %ALIGN-3-TRACE: -Traceback= 60336D44
6021AFB0 6021C948 00000000 00000000 00000000 00000000 00000000
```

This problem is resolved in Release 12.2(18)SXE4. (CSCsb09250)

- With serial FlexWAN interfaces configured, you might see these messages and be unable to make a Telnet connection:

```
%SYS-3-CPUHOG: Task is running for (4984)msec more than (2000) msec (12/1),
process = Serial Background
Traceback= 402AA8DC 4029F00C 402AD7D0 419C81C0 41A25CF4 4002AE50
```

This problem is resolved in Release 12.2(18)SXE4. (CSCeg04325)

- With Cisco IOS SLB configured, FlexWAN module ingress traffic is hardware switched instead of route-cache switched after a switchover. This problem is resolved in Release 12.2(18)SXE4. (CSCsa43553)
- All low-priority traffic is dropped over a distributed Link Fragmentation and Interleaving over Frame Relay (dLFIoFR) link on a system that is configured with an Enhanced FlexWAN module. This situation occurs when all of the traffic is flowing at the full line rate and some low-priority traffic has to be fragmented. This problem is resolved in Release 12.2(18)SXE4. (CSCsb25607)
- When an MFR bundle goes down and up, all links associated with the bundle fail to recover line protocol. This problem occurs in a configuration that includes a PA-8T-V35 2 port adapter. The output of the **show frame-relay multilink** command displays port 0 as “HW state = up, link state = Add\_sent” and will never recovers. This problem is resolved in Release 12.2(18)SXE4. (CSCsb48015)
- A FlexWAN module configured with a PA-MC-8TE1 port adapter detects loss of signal (LOS) after a reload, and then does not recover. This problem is resolved in Release 12.2(18)SXE4. (CSCsb21867)
- A FlexWAN module might reload if you apply a Frame Relay map class configured with a **frame relay fragment** command to the Frame Relay data-link connection identifier (DLCI) on a multilink Frame Relay (MFR) interface created from a serial port adapter interface. To resolve this problem, the **frame relay fragment** command has been disabled in Release 12.2(18)SXE4. (CSCsb70335)
- FlexWAN egress multicast traffic loss occurs on a permanent virtual circuit (PVC) bundle if any of the PVCs in the bundle is down. This problem is resolved in Release 12.2(18)SXE4. (CSCsb86675)
- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the “admindown” state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.2(18)SXE4. (CSCin78325)
- An ATM interface on a FlexWAN or an Enhanced FlexWAN port adapter stops transmitting when you add or remove a QoS service policy on the interface. This problem is resolved in Release 12.2(18)SXE4. (CSCsb01188)

### Resolved FlexWAN Caveats in Release 12.2(18)SXE3

None.

## Resolved FlexWAN Caveats in Release 12.2(18)SXE2

- Intermediate System-to-Intermediate System (IS-IS) multicast frames destined to MAC addresses 01:80:C2:00:00:14-15 that are received by a FlexWAN module interface as bridged ATM PVC traffic are classified as BPDUs and dropped. This situation prevents IS-IS adjacency establishment. (CSCsb09997)
- When configured to support Frame Relay with Internet Engineering Task Force (IETF) encapsulation, a FlexWAN module interface might corrupt OSPF Database Description (DBD) packets. This problem is resolved in Release 12.2(18)SXE2. (CSCeh68965)
- After online insertion and removal (OIR) of a FlexWAN module, these port adapters stop passing traffic if they are configured for Frame Relay encapsulation:
  - [PA-MC-2E1/120](#)
  - [PA-MC-8T1](#)
  - [PA-MC-8E1/120](#)
  - [PA-MC-2T1](#)
  - [PA-MC-4T1](#)
  - [PA-MC-8TE1+](#)

This problem is resolved in Release 12.2(18)SXE. (CSCei12574)

## Resolved FlexWAN Caveats in Release 12.2(18)SXE1

None.

## Resolved FlexWAN Caveats in Release 12.2(18)SXE

- Under a high traffic load, a [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) port adapter might display an increasing rx\_no\_buffer counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter might stop receiving traffic. This problem is resolved in Release 12.2(18)SXE. (CSCin77553)
- Following a reload, the **vbr-nrt** command might be missing from inverse multiplexing over ATM (IMA) interfaces. This problem is resolved in Release 12.2(18)SXE. (CSCec51408)
- With non-real time variable bit rate (VBR-nrt) shaping configured on more than one permanent virtual circuit (PVC) defined under the same physical ATM interface on a [PA-A3-8E1IMA](#) or [PA-A3-8T1IMA](#) port adapter, when the load is equal to or greater than the maximum configured VBR-nrt value on at least two PVCs, not all of the PVCs achieve the configured VBR-nrt value. This problem is resolved in Release 12.2(18)SXE. (CSCef55463)
- With an E3 serial port adapter, when you enter the **dsu bandwidth kbps\_rate** command, the DSU bandwidth might not change. This problem is resolved in Release 12.2(18)SXE. (CSCef73120)
- With more than 38 multilink bundles configured on a port adapter, a reload might occur if CEF switching is disabled. This problem is resolved in Release 12.2(18)SXE. (CSCef94525)
- The SNMP ifAdminStatus MIB object does not support ATM subinterfaces. This problem is resolved in Release 12.2(18)SXE. (CSCeg03153)
- If you perform an OIR on a PA-MC-STM-1 port adapter that is configured to support automatic protection switching (APS), a CBUS-3-CCBCMDFAIL1 message might display. This problem is resolved in Release 12.2(18)SXE. (CSCeg06570)

- A reload might occur during heavy traffic over FlexWAN channelized port adapters and the port adapters go up and down. This problem occurs when the port adapters are configured with MFR. This problem is resolved in Release 12.2(18)SXE. (CSCeh34067)
- When you use the **show controller** command to display the serial interface counters, they may stop incrementing for the input and output rate and the input and output packet counts. This problem occurs on a system configured with a PA-MC-E3 or a PA-MC-8E1 port adapter. The problem does not effect traffic flow. This problem is resolved in Release 12.2(18)SXE. (CSCsa46643)

## Service Module Caveats in Release 12.2(18)SXE and Rebuilds

- [Open Service Module Caveats in Release 12.2\(18\)SXE6a, page 323](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE6a, page 323](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE6, page 323](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE5, page 323](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE4, page 324](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE3, page 325](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE2, page 325](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE1, page 326](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXE, page 326](#)

### Open Service Module Caveats in Release 12.2(18)SXE6a

- With an IPsec VPN Acceleration services module (**WS-SVC-IPSEC-1**), a memory leak might occur when thousands of VPN clients are connecting and disconnecting at the same time. (CSCee25454)

### Resolved Service Module Caveats in Release 12.2(18)SXE6a

None.

### Resolved Service Module Caveats in Release 12.2(18)SXE6

- You might be unable to access an Multi-Processor WAN Application Module (MWAM) through a console or Telnet session for 10 minutes after the module has been reloaded.

**Workaround:** Configure the **ip rcmd rcp-enabled** command.

This problem is resolved in Release 12.2(18)SXE6. (CSCsa50215)

### Resolved Service Module Caveats in Release 12.2(18)SXE5

- Layer 2 and Layer 3 packets that are sourced by a NAM service module and that require recirculation are getting dropped when the fabric switching mode for the service module is crossbar-enabled mode. This problem is resolved in Release 12.2(18)SXE5. (CSCsc03864)
- A reload might occur when you enter the **clear counters** command. This problem occurs if the system is configured with a CSM module that has gone down, and an Remote Procedure Call (RPC) from the supervisor engine has timed out. This problem is resolved in Release 12.2(18)SXE5. (CSCsb79031)

- The sticky database is corrupted if you use the same cookie name when you change the CSM sticky cookie insert configuration, for a virtual server, from dynamic cookie to cookie insert. A corrupted sticky database only partially displays when you enter the **show module csm slot sticky [groups | client ip\_address]** command, and session persistency cannot continue. To correct this problem, all configurations related to the sticky group must be removed and the CSM must be rebooted. This problem is resolved in Release 12.2(18)SXE5. (CSCsc05838)
- If a service module goes down, the module sends a message to the supervisor engine requesting an image download so that it can reinitialize. The supervisor engine ignores the message, does not notice that the service module is down for 180 seconds, and then downloads the image. This problem is resolved in Release 12.2(18)SXE5. (CSCei37672)
- If you repeatedly use the **execute-on** command a memory depletion and an eventual reload might occur. This problem is resolved in Release 12.2(18)SXE5. (CSCei67673)
- When you enroll a Supervisor Engine 2 with a certification authority (CA) server and you request that the serial number be included with the subject name of the certificate, the serial number is incorrect in the certificate-signing request (CSR) and in the certificate. This problem is resolved in Release 12.2(17d)SXE5. (CSCsa67272)
- With a Supervisor Engine 720, a Cisco Multiprocessor WAN Application Module (MWAM) might experience connectivity problems if there are any Layer 2 [distributed EtherChannels \(DECs\)](#) configured. This problem is resolved in Release 12.2(18)SXE5 (CSCsb50559)
- After a reload, URL match statements are missing from the CSG configuration. When you enter the **ip csg map map-name url** command. This problem is resolved in Release 12.2(18)SXE5. (CSCsb66799)
- For a topology configured for Firewall Service Module (FWSM) inter-chassis failover, if a manual failover is initiated, and the system is operating in bus mode, inter-chassis failover fails to execute with a status of normal (waiting). This problem occurs when you use a distributed EtherChannel (DEC) between the two chassis where the FWSM is installed, and the devices are forced to operate in bus mode. This problem is resolved in Release 12.2(18)SXE5. (CSCsc57156)

#### Resolved Service Module Caveats in Release 12.2(18)SXE4

- Some service modules do not have central rewrite capability but they generate Layer 3 packets that need to be recirculated (for example, packets that need to egress on a GRE tunnel). These packets are being dropped. [WS-SVC-IDSM2-K9](#) is the only service module impacted by this problem. This problem is resolved in Release 12.2(18)SXE4. (CSCei64940)
- An SNMP walk fails to find a value for the csgQuotaMgrStats MIB object. If you add a second user group and an accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server statistics by either a manual MIB walk or by SNMP messaging. This occurs with the quota servers that are configured in both of the configured user-groups. This problem is resolved in Release 12.2(18)SXE4. (CSCsa95287)
- When configuring a new VLAN on a CSG, the VLAN may not be allowed on the trunk interface between the MSFC and the CSG until the CSG is reloaded. IP connectivity on the VLAN cannot be established towards the CSG before the reload. You can enter the **show interface trunk** command to verify whether or not the VLAN is allowed on the port channel interface associated with the CSG. This problem is resolved in Release 12.2(18)SXE4. (CSCsb01086)

- A system that is configured with Dynamic Multipoint VPN (DMVPN) tunnels might reload during DMVPN deployment with the following bus error:

```
SYS-2-FREEBAD: Attempted to free memory at 41D7A6E4, not part of buffer pool
-Traceback= 40E93794 41CDF084 41CD7CD0 41CBD568 41CBD884 41CBF070 41CC10F0
41CC2068
```

```
0x40E93794:free(0x40e936f0)+0xa4
0x41CDF084:ace_polo_send_hapi(0x41cdeb40)+0x544
...
```

This problem is resolved in Release 12.2(18)SXE4. (CSCsb16146)

- With a VPN Service Module (VPN-SM/WS-SVC-IPSEC-1) installed, large packet drops might occur when you configure the **ip mtu** command on a GRE IPsec tunnel interface. This problem is resolved in Release 12.2(18)SXE4. (CSCsb12076)
- Reverse route injection (RRI) routes are not reloaded immediately after a WS-SVC-IPSEC-1 IPsec VPN Acceleration Services Module (VPNSM) IPsec stateful failover. This symptom occurs when two systems are configured with VPNSMs, and one of the systems is configured for SSO. When a switchover occurs on the redundant system and the VPNSM reloads, the RRI routes are not reloaded until the VPNSM in the redundant system reloads. This problem is resolved in Release 12.2(18)SXE4. (CSCsb38885)
- VPN client authentication fails when you attempt to use New personal identification number (PIN) mode or Next Token mode. Authentication is successful if you avoid New PIN mode and Next Token mode. The problem occurs when you authenticate using Token card / ACE server through RADIUS in New PIN mode, or Next Token mode has been turned on because you entered an incorrect password, consecutively. This problem is resolved in Release 12.2(18)SXE4. (CSCeh35849)
- With redundant Supervisor Engine 720s and redundant IPsec VPN Acceleration Services Modules (VPNSMs), a reload occurs if you remove an ACL that is part of the VPNSM configuration. This problem is resolved in Release 12.2(18)SXE4. (CSCsb77592)

### Resolved Service Module Caveats in Release 12.2(18)SXE3

None.

### Resolved Service Module Caveats in Release 12.2(18)SXE2

- In rare circumstances, if maximum capacity traffic is flowing bidirectionally through the IPsec VPN Acceleration services module (VPN SM; [WS-SVC-IPSEC-1](#)), packets flood on all VLANs that are allowed on the internal gigabit Ethernet interface of the VPN SM. This situation causes traffic to loop back to the VPN SM and the VPN SM must drop the looped traffic, which reduces the effective bandwidth of the VPN SM. This problem is resolved in Release 12.2(18)SXE2. (CSCeh65221)
- With a VPN SM, a reload might occur if you enter the **show crypto socket** command while a range of tunnel interfaces are in the process of shutting down. This problem is resolved in Release 12.2(18)SXE2. (CSCsa48259, CSCsb10226)
- Rivest, Shamir, and Adelman (RSA) signature authentication on the VPN SM does not support upper-case (A through Z) peer certificate URLs. This problem is resolved in Release 12.2(18)SXE2. (CSCsa81928)
- With a VPN SM configured for Rivest, Shamir, and Adelman (RSA) signature authentication, if the certificate distribution point (CDP) in the peer certificate does not have the hostname or IP address of the lightweight directory access protocol (LDAP) CRL server, all Internet Key Exchange (IKE)

negotiation fails and the Internet Key Management Protocol (IKMP) process might be blocked indefinitely because the CRL cannot be fetched. This problem is resolved in Release 12.2(18)SXE2. (CSCsa78580)

- When configured as a dynamic multipoint virtual private network (DMVPN) spoke router and when a VPN SM is providing IPsec acceleration, a reload might occur if you enter a **no shutdown** command on a multipoint generic routing encapsulation (MGRE) tunnel interface that is in the administrative “reset” state and the operational “down” state. This problem is resolved in Release 12.2(18)SXE2. (CSCeh71584)
- When configured as a dynamic multipoint virtual private network (DMVPN) spoke router and when a VPN SM is providing IPsec acceleration, if there are IPsec failures when the dynamic spoke to spoke tunnels are built, a memory leak might occur in the I/O memory pool. This situation eventually causes I/O memory allocation failures. This problem is resolved in Release 12.2(18)SXE2. (CSCsa73843)

### Resolved Service Module Caveats in Release 12.2(18)SXE1

None.

### Resolved Service Module Caveats in Release 12.2(18)SXE

- When configured with a standby Content Switching Module (CSM), a bus error exception and a reload might occur if there is an SNMP request for the Cisco IOS SLB MIB for the standby CSM and the **hw-module csm slot\_num standby config-sync** command is entered on the active CSM. This problem is resolved in Release 12.2(18)SXE. (CSCsa74464)
- When the CSM Cisco IOS SLB mode is “RP”, a reload might occur if you enter the **ip slb mode csm** command and then enter the **show running-config** command. This problem is resolved in Release 12.2(18)SXE. (CSCef93632)
- The traffic counters displayed by the show interfaces tunnel command are incorrect for GRE IPsec tunnels on the IPsec VPN Acceleration services module (WS-SVC-IPSEC-1). This problem is resolved in Release 12.2(18)SXE. (CSCef56578)
- With a Rivest, Shamir, and Adelman signature (RSA-SIG) and Internet Key Management Protocol (IKMP) configured, a memory leak might occur. This problem is resolved in Release 12.2(18)SXE. (CSCec32184)
- With public key infrastructure (PKI) and Internet Key Management Protocol (IKMP) configured, a memory leak might occur. This problem is resolved in Release 12.2(18)SXE. (CSCec22308)
- With an IPsec VPN Acceleration Services Module, following a switchover to a redundant supervisor engine under heavy traffic conditions, traffic might stop flowing through IPsec and GRE IPsec tunnels that are configured for tunnel protection. This problem is resolved in Release 12.2(18)SXE. (CSCef75411)
- With an IPsec VPN Acceleration Services Module, if you change the ACL name in a **match address acl\_name** crypto-map command, the crypto-map is removed from the VPN module and is not sent to the VPN module with the new name. This problem is resolved in Release 12.2(18)SXE. (CSCef77822)
- The SNMP slbStickyObjectTableEntry MIB object is not supported. This problem is resolved in Release 12.2(18)SXE. (CSCef05643)
- The trunk connection to a WS-X6066-SLB-APC Content Switching Module (CSM) carries VLANs that are not used by the CSM. This problem is resolved in Release 12.2(18)SXE. (CSCeg41623)

- With a VPN Services Module (VPNSM) or an IPsec SPA, a dynamic crypto map and Dead Peer Detection (DPD) may reload when many IPsec tunnels are processed under heavy traffic. This problem is resolved in Release 12.2(18)SXE. (CSCeh43531)

## OSM Caveats in Release 12.2(18)SXE and Rebuilds

- [Open OSM Caveats in Release 12.2\(18\)SXE6a, page 327](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE6a, page 327](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE6, page 327](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE5, page 328](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE4, page 328](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE3, page 328](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE2, page 328](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE1, page 329](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXE, page 329](#)

### Open OSM Caveats in Release 12.2(18)SXE6a

None.

### Resolved OSM Caveats in Release 12.2(18)SXE6a

None.

### Resolved OSM Caveats in Release 12.2(18)SXE6

- When using a service policy on an OSM-POS port, some MIB objects have the wrong values:
  - The TX cbQosCMPrePolicyByte64 counter is always 0. It is not incremented with traffic.
  - The TX cbQosCMDropByte64 counter is always 0 even when the policer is dropping traffic.
  - The class-default counters for RX and TX (cbQosCMPPostPolicyByte, cbQosCMPrePolicyByte, cbQosCMDropByte) are not incrementing even when traffic is sent in this class.

This problem is resolved in Release 12.2(18)SXE6. (CSCsd05513)

- An MPLS table entry on an MSFC might get out of synchronization with the supervisor engine when an OSM goes down. This problem occurs on a system configured with two OSMs, which is facing the MPLS core, and with multiple load-sharing paths to the MPLS core configured. This problem is resolved in Release 12.2(18)SXE6. (CSCsd41981)
- The OSM-2+4GE-WAN+ module might drop packets if you create or delete on it. This problem occurs when the subinterface belongs to a physical interface on the switching module that is currently passing traffic. This problem is resolved in Release 12.2(18)SXE6. (CSCse05336)
- Minimum and maximum Weighted Random Early Detection (WRED) threshold values for default differentiated services code point (DSCP) do not change when new values are configured. This problem occurs when an OSM is configured with quality of service (QoS) and WRED. This problem is resolved in Release 12.2(18)SXE6. (CSCsd90501)



## Resolved OSM Caveats in Release 12.2(18)SXE5

- A Supervisor Engine 720 configured with an OSM POS interface might experience the following ASIC error, and then the OSM POS interface might stop passing traffic:

```
UTC: %CWTLC-3-DMA_ENGINE_ASIC_ERR: DMA Engine Asic [0] error: SRIC packet data CRC error
UTC: %CWTLC-3-CONST_SWITCHING_BUS_INTERFACE_ASIC_ERR: Constellation Switching Bus Interface Asic [0] error: TXIF: RXPB bad packet len (low)
```

This problem occurs when MPLS is configured on an OSM. This problem is resolved in Release 12.2(18)SXE5. (CSCsc73288)

- After an SSO switchover, a OSM-1CHOC12 service module that is channelized to DS0, might reload and cause an APS switchover. This problem is resolved in Release 12.2(18)SXE5. (CSCei10228)
- The Virtual Container 12 (VC-12) RFI bit is undefined in the International Telecommunication Union (ITU) G.707/Y.1322 standard. Instead of ignoring the VC-12 RFI bit, an [OSM-1CHOC12/T1-SI](#) reports a Remote Fault Indication (RFI) for VC-12 and shuts down its E1 interfaces if it is connected to a synchronous digital hierarchy (SDH) switch that has the VC-12 RFI bit set. This problem is resolved in Release 12.2(18)SXE5. (CSCsa85123)

## Resolved OSM Caveats in Release 12.2(18)SXE4

- Following a reload with an OSM-2+4GE-WAN+ or a POS OSM installed, traffic shaping configured on an SVI does not work. This problem is resolved in Release 12.2(18)SXE4. (CSCsb24320)
- A system configured with a POS OSM may experience the following ASIC error, and the POS interface may later stop passing traffic:

```
UTC: %CWTLC-3-DMA_ENGINE_ASIC_ERR: DMA Engine Asic [0] error: SRIC packet data CRC error
UTC: %CWTLC-3-CONST_SWITCHING_BUS_INTERFACE_ASIC_ERR: Constellation Switching Bus Interface Asic [0] error: TXIF: RXPB bad packet len (low)
```

This problem is resolved in Release 12.2(18)SXE4. (CSCsb15183)

- On an OSM-2+4GE-WAN+ module, if you replace a physical IEEE 802.1Q tunneling (QinQ) configuration with a QinQ EtherChannel configuration without any member ports, and later add member ports, the EtherChannel might not pass any traffic. This problem is resolved in Release 12.2(18)SXE4. (CSCeh55293)
- With a Supervisor Engine 720, Layer 3 virtual private network (L3VPN) packets are dropped on the OSM Spatial Reuse Protocol (SRP) interfaces if the interfaces face CE routers. This problem is resolved in Release 12.2(18)SXE4. (CSCei20996)

## Resolved OSM Caveats in Release 12.2(18)SXE3

None.

## Resolved OSM Caveats in Release 12.2(18)SXE2

- [OSM-2+4GE-WAN+](#) ports do not automatically adjust the MTU size to accommodate tagged traffic. Ingress tagged packets destined for the MSFC are dropped if the packet size is larger than the ingress interface MTU size. This problem is resolved in Release 12.2(18)SXD. (CSCsb13441)



- An OSM that has more than 4 ports might reset if you attach either of these to port 5 or higher:
  - A nonhierarchical policy map that configures strict priority queuing
  - A hierarchical policy map that configures strict priority queuing at the child level and does not configure shaping at the parent level

This problem is resolved in Release 12.2(18)SXE2. (CSCei00856)

### Resolved OSM Caveats in Release 12.2(18)SXE1

None.

### Resolved OSM Caveats in Release 12.2(18)SXE

- When autonegotiation is disabled on a dense wavelength-division multiplexing (DWDM) link between two GE-WAN ports, connectivity is lost after you enter **shutdown** and **no shutdown** commands on one of the OSMs. This problem is resolved in Release 12.2(18)SXE. (CSCef12304)
- Changing the MTU size on a port might not change the MPLS MTU size. This problem is resolved in Release 12.2(18)SXE. (CSCed17226, CSCed33822)
- If you enter the **encapsulation dot1q vlan\_id** command on an OSM Gigabit Ethernet WAN port with the VLAN ID of an internal VLAN, the port does not forward traffic. This problem is resolved in Release 12.2(18)SXE. (CSCef08790)
- The SNMP ifHCOutOctets and ifHCInOctets MIB objects always have a value of zero. This problem is resolved in Release 12.2(18)SXE. (CSCef42133)
- On a channelized OSM, after you enter the **aps force** command to change the status of an automatic protection switching (APS) interface from protect to working, IP routing is not notified of the status change. This problem is resolved in Release 12.2(18)SXE. (CSCef45881)
- OSM ATM interfaces do not support unspecified bit rate plus (UBR+) virtual circuit (VC) class maps, but you can apply UBR+ VC class maps to VC subinterfaces. This problem is resolved in Release 12.2(18)SXE. (CSCec31381)
- OSM ATM interfaces do not support the SNMP lowerLayerDown value defined in RFC 2863. This problem is resolved in Release 12.2(18)SXE. (CSCee56269)
- On a channelized OSM, after a reload, some of the links in a multilink interface might not come up. This problem is resolved in Release 12.2(18)SXE. (CSCef78798)
- On a channelized OSM, after a reload, the clock source might be incorrect. This problem is resolved in Release 12.2(18)SXE. (CSCef79815)
- On an [OSM-1CHOC12/T1-SI](#), when modifying a configuration from E3 to E1, the newly configured E1s stay down. This problem is resolved in Release 12.2(18)SXE. (CSCsa43724)
- With QoS configured on an OSM multilink interface, a reload might occur if the multilink interface becomes unstable. This problem is resolved in Release 12.2(18)SXE. (CSCsa44933)

- MPLS traffic from the MSFC, for example, ping or Service Assurance Agent (SAA) traffic, is not enqueued correctly on [OSM-2+4GE-WAN+](#) egress ports. Because the traffic is not in the correct egress queue, incorrect QoS policies are applied to the traffic. This problem is resolved in Release 12.2(18)SXE. (CSCeg77503)

## SPA Caveats in Release 12.2(18)SXE and Rebuilds

- [Open SPA Caveats in Release 12.2\(18\)SXE6a, page 330](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE6a, page 330](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE6, page 330](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE5, page 331](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE4, page 332](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE3, page 332](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE2, page 332](#)
- [Resolved SPA Caveats in Release 12.2\(18\)SXE1, page 333](#)

### Open SPA Caveats in Release 12.2(18)SXE6a

- With a CT3 SPA in a SIP-200 configured with multiple DS0 links that are part of multilink bundles, these messages do not indicate a problem that affects traffic:

```
SLOT slot_num: 06:46:34: %INTR_MGR-3-INTR: SPA-4XCT3/DS0[slot_num/bay_num] EFC Parity Error
06:46:34: %Fatal Error: Hardware error (EFC Parity Error) detected for SPA
slot_num/bay_num
```

**Workaround:** None. (CSCeh52330)

- With a CT3 SPA, traffic loss occurs on multilink interfaces that have a differential delay larger than 70 milliseconds.

**Workaround:** None. (CSCef82225)

### Resolved SPA Caveats in Release 12.2(18)SXE6a

None.

### Resolved SPA Caveats in Release 12.2(18)SXE6

- An ATM virtual path might fail to initialize when a large number of ATM virtual paths are configured on an ATM SPA interface and the interface goes up and down several times. This problem is resolved in Release 12.2(18)SXE6. (CSCek26186)
- A Field Programmable Device (FPD) error might occur when you do a SPA FPD upgrade on a SIP1 hardware revision 2.x module if you are using an old FPD bundle. This problem is resolved in Release 12.2(18)SXE6. (CSCek42027)
- A T3 line might go up and down on a SPA. This problem occurs when the T3 SPAs are configured in channelized mode, the T1 interfaces are configured as Extended Super Frame (ESF) framing, and the T1 interfaces on the far end are configured to send T1 facilities data link (FDL) ANSI reports. This problem is resolved in Release 12.2(18)SXE6. (CSCsd94541)

- Interfaces configured on an ATM SPA that is installed in a SIP-200 might fail to ping if the fabric channel had a synchronization failure during initialization of the SIP-200. This synchronization failure is verified in the output of the **show logging** command:

```
00:00:43: Serial Primary Channel SYNC FAILED!
```

This problem is resolved in Release 12.2(18)SXE6. (CSCsc43862)

## Resolved SPA Caveats in Release 12.2(18)SXE5

- MFR bundles configured on a channelized T3 SPA module remains down after a system reload or a reload of the SPA. This problem is resolved in Release 12.2(18)SXE5. (CSCei48635)
- T3 clear-channel interface performance degrades 40 percent when there are more than 400 low speed NxDS0 (N=1 or N=2) channels configured on the same CT3 SPA with the T3 clear-channel interface. This problem is resolved in Release 12.2(18)SXE5. (CSCed14809)
- With 10 multilink bundles, each with 12 member links, configured from a SPA to a remote router, if you reload the remote router, you might see SPA\_CHOC\_DSX-3-HDLC\_CTRL\_ERR and “Overflow events on HDLC Controller were encountered” messages. This problem is resolved in Release 12.2(18)SXE5. (CSCsa70494)
- On a [SPA-2XCT3/DS0](#) or [SPA-4XCT3/DS0](#), you might see C7600\_SIP200\_SPITX-3-EFC\_QUEUE\_STUCK messages if you add a multilink bundle member that is already a member of one multilink bundle to a second multilink bundle. This problem is resolved in Release 12.2(18)SXE5. (CSCsa80620)
- T3 clear-channel interface performance degrades 40 percent when there are more than 400 low speed NxDS0 (N=1 or N=2) channels configured on the same CT3 SPA with the T3 clear-channel interface. This problem is resolved in Release 12.2(18)SXE5. (CSCed14809)
- When a T3 line goes up and down, the serial interface configured on a T1 channel group over the T3 line fails to come up and stays in the Line Protocol down state. This problem occurs when the link is configured over a SPA-CT3 or a SPA-CHOC-STM1 port adapter. This problem is resolved in Release 12.2(18)SXE5. (CSCeh80649)
- A traceback occurs when you OIR a SIP-400 with an OC-48 ATM SPA. This problem is resolved in Release 12.2(18)SXE5. (CSCei21293)
- A CT3 SPA controller on the near end of a link goes down when the remote end of the link goes down and up. This problem occurs when T1 FDL transmission is started. This problem is resolved in Release 12.2(18)SXE5. (CSCei33598)
- On a SPA configured with a POS interface, the APS states on the standby supervisor engine might become inconsistent with the active supervisor engine. After an SSO switchover, this situation might result in incorrect output of the **show aps** command. This problem is resolved in Release 12.2(18)SXE5. (CSCei39181)
- With redundant supervisor engines, if you OIR a SPA, and then a switchover occurs, traffic stops over that SPA’s interface. This problem is resolved in Release 12.2(18)SXE5. (CSCin96328)
- If multiple FR DLCIs are configured for distributed traffic shaping (dTS) using modular QoS CLI (MQC), some DLCIs might be lost if you enter the **bandwidth n** command on the physical interface.  
**Workaround:** You can reapply the QoS configuration after the bandwidth change. This problem is resolved in Release 12.2(18)SXE5. (CSCsb36818)
- A channelized T3 to DS0 SPA might stop processing traffic. This problem occurs when you configure a large number of T1 links in Super Frame (SF) framing mode simultaneously on two channelized T3 to DS0 SPAs that are connected back-to-back. This problem is resolved in Release 12.2(18)SXE5. (CSCsb00473)

- A 7600-SIP-400 might drop bursty egress traffic. This problem is resolved in Release 12.2(18)SXE5. (CSCsc68250)
- A T1 line on a SPA-2XCT3/DS0 or SPA-4XCT3/DS0 goes down if you configure bit error rate testing (BERT) on a time slot or channel group of the T1. This problem is resolved in Release 12.2(18)SXE5. (CSCsc52645)
- When a 2-port or 4-port channelized T3-to-DS0 SPA is configured with MFR subinterfaces, and when you enter the **shutdown** command followed by the **no shutdown** command on one of the subinterfaces, the subinterface does not come up. This problem is resolved in Release 12.2(18)SXE5. (CSCsb38396)

#### Resolved SPA Caveats in Release 12.2(18)SXE4

- When two interfaces with different encapsulations are configured for IPHC, some cRTP VoIP packets may be dropped on an ingress T3 SPA in a SIP-200 by IPHC as error packets. This problem is resolved in Release 12.2(18)SXE4. (CSCei30999)
- If you enter the **card type** command for a SPA-8XCHT1/E1, hardware version 2.0 or greater, the command displays a message and fails. This problem is resolved in Release 12.2(18)SXE4. (CSCei93397)
- A SIP-200 with an ATM shared port adapter (SPA) that has a policy map configured might reload when sending ATM Adaptation Layer 5 over MPLS (AAL5oMPLS) traffic. This problem is resolved in Release 12.2(18)SXE4. (CSCei24139)

#### Resolved SPA Caveats in Release 12.2(18)SXE3

None.

#### Resolved SPA Caveats in Release 12.2(18)SXE2

- A reload might occur if you enter the **show tech-support** command or the **show hw-module subslot** command with any of these SPAs installed:
  - [SPA-4XCT3/DS0](#)
  - [SPA-2XCT3/DS0](#)
  - [SPA-2XT3/E3](#)
  - [SPA-4XT3/E3](#)
  - [SPA-8XCHT1/E1](#)

This problem is resolved in Release 12.2(18)SXE2. (CSCeh62351)

- If you apply a WRED aggregate service policy to an ATM PVC on an ATM SPA with 7 user-defined subclass groups and no “leftover subclasses” in the default aggregate subclass group, a “maximum configurable WRED colors (7) exceeded” message is displayed, and the service policy is rejected. This problem is resolved in Release 12.2(18)SXE2. (CSCeh56439)
- A service policy attached to a Multilink Frame Relay (MFR) SPA interface on a [7600-SIP-200](#) might not classify traffic after an RPR+ switchover. This problem is resolved in Release 12.2(18)SXE2. (CSCeh41652)
- On an [ATM SPA](#), the random-detect policy-map class command does not work in policy maps applied to an ATM virtual circuit (VC) configured for distributed Link Fragmentation and Interleaving (dLFI). This problem is resolved in Release 12.2(18)SXE2. (CSCeh54083)

- Occasionally, after the system or the SIP or the SPA reloads, some of the channel interfaces on a [SPA-2XCT3/DS0](#) or [SPA-4XCT3/DS0](#) might not be able to transmit packets. This problem is resolved in Release 12.2(18)SXE2. (CSCeh42629)

### Resolved SPA Caveats in Release 12.2(18)SXE1

None.

## Caveats in Release 12.2(18)SXD and Rebuilds

- [General Caveats in Release 12.2\(18\)SXD and Rebuilds, page 333](#)
- [FlexWAN Module Caveats in Release 12.2\(18\)SXD and Rebuilds, page 357](#)
- [Service Module Caveats in Release 12.2\(18\)SXD and Rebuilds, page 361](#)
- [OSM Caveats in Release 12.2\(18\)SXD and Rebuilds, page 365](#)



#### Note

- 
- Caveats resolved in Release 12.2(17d)SXB2 and earlier releases are resolved in Release 12.2(18)SXD.
  - The caveat information for Release 12.2(18)SXD and rebuilds is being updated frequently.
- 

### General Caveats in Release 12.2(18)SXD and Rebuilds

- [Open General Caveats in Release 12.2\(18\)SXD7a, page 333](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD7a, page 335](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD7, page 337](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD6, page 337](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD5, page 338](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD4, page 340](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD3, page 343](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD2, page 346](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD1, page 347](#)
- [Resolved General Caveats in Release 12.2\(18\)SXD, page 351](#)

### Open General Caveats in Release 12.2(18)SXD7a

- Subinterfaces on these ports do not provide hardware switching for IPv4 multicast traffic:
  - Ethernet1/1
  - FastEthernet1/1
  - GigabitEthernet1/1
  - TenGigabitEthernet1/1

This problem is resolved in Release 12.2(18)SXE. (CSCec77178, CSCed26629, CSCef91498)

- With a Supervisor Engine 720, if you enter the **mls ip cef load-sharing simple** command, traffic might be lost that uses MPLS adjacencies for routes that have a next hop that is reachable through an MPLS cloud. This problem is resolved in Release 12.2(18)SXE. (CSCsa50071, CSCeg71317)
- If you enter the **no ip vrf vrf\_name** command in one administrative session, a reload might occur if you enter the **ip vrf vrf\_name** command for the same VRF in another administrative session before the deletion process completes. This problem is resolved in Release 12.2(18)SXE. (CSCeg51793)
- When two ports in the same VLAN on different DFC-equipped switching modules send bidirectional traffic to each other, and you configure one of the ports as an egress SPAN source port, then the traffic sent to that port is flooded to all the ports in the VLAN. This problem is resolved in Release 12.2(18)SXE. (CSCin78242)
- With RPR+ mode configured, the supervisor engine might fail bootup diagnostics with an “AclPermit” test failure and a reload. This problem is resolved in Release 12.2(18)SXE. (CSCef20654)
- When the FIB TCAM is full, CPU utilization might be unacceptably high. This problem is resolved in Release 12.2(18)SXE (CSCeb85827, CSCeb29888, CSCec14802, CSCec42634, CSCed58661, CSCee00311, CSCee22821, CSCin77977, CSCin78030, CSCin80590)
- With redundant Supervisor Engine 720s configured to support NSF and multicast, multicast groups with a large number of output interfaces (for example, more than 170) that are being Layer 3 switched in hardware are routed in software after an NSF with SSO switchover. This problem is resolved in Release 12.2(18)SXE. (CSCee79348)
- With RPR+ mode configured, after you enter the **clear cef linecard** command, RPR+ information might not be displayed correctly in the output of the **show cef linecard** command. This problem is resolved in Release 12.2(18)SXE. (CSCuk41411)
- Ignore “Cannot encode data descriptor LI-Null0” messages on the console of a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE. (CSCef72939)
- Ignore “Port Manager Internal Software Error” messages and tracebacks on the console of a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXE. (CSCef50171)
- After a reload of a Supervisor Engine 2 with DFC-equipped switching modules, Gateway Load Balancing Protocol (GLBP) traffic might be routed in software on the MSFC2, because the GLBP virtual MAC address might not be enabled. This problem is resolved in Release 12.2(18)SXE. (CSCee70075)
- Ignore spurious memory access errors during an SSO switchover. This problem is resolved in Release 12.2(18)SXE. (CSCuk49384, CSCed64648, CSCeb55269, CSCed44945, CSCed47559, CSCed50801, CSCed51914, CSCed64843, CSCed80188, CSCed88244, CSCee10565, CSCee19150, CSCee32558, CSCee42141, CSCee56069, CSCee59872, CSCin70853, CSCin72244)
- With a PFC3, on Layer 3 interfaces that are configured to support IPX routing, but which are not configured with an IP address, the **mls rate-limit** commands incorrectly limit IPX traffic.

**Workaround:** Configure an IP address on Layer 3 interfaces that are configured to support IPX routing. Use an IP address to which IP routing does not send any traffic. Configure an IP access list to drop IP ingress traffic. This problem is resolved in Release 12.2(18)SXE. (CSCee09692)

- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

- A large memory leak might occur on a Supervisor Engine 720 when a VLAN, a portchannel, or an individual interface goes down. This problem occurs when the system is in egress replication mode and there are no DFCs present. The interface that goes down must be an outgoing interface of a multicast entry in the hardware. The memory leak is proportional to the number of multicast entries that apply to this interface.

**Workaround:** Put the system in ingress replication mode by entering the **mls ip multicast replication-mode ingress** global configuration command or install a DFC with the system in egress replication mode.

This problem is resolved in Release 12.2(18)SXE6. (CSCsd98887)

## Resolved General Caveats in Release 12.2(18)SXD7a

- A Supervisor Engine 720 might reload when you install a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXD7a. (CSCse73539)
- Occasionally in an IGMP multicast configuration, the PFC or DFC FIFO stops processing, and this message is displayed:

```
EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
```

This problem is resolved in Release 12.2(17d)SXB11a. (CSCej21698)

- This DDTS documents changes in how Cisco IOS software handles packets destined to the router. This problem is resolved in Release 12.2(17d)SXB11a. (CSCek26492)
- Some UDP packets that have the Terminal Access Controller Access Control System (TACACS) port (49) as their destination might remain suspended in the interface queue. This problem occurs when TACACS+ is configured. This problem is resolved in Release 12.2(18)SXD7a. (CSCsb11698)
- A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

**Workaround:** Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL). By doing this, the offending router will not be able to participate within the mVPN data trees.

The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a rACL:

```
!
ip receive access-list 111
!
access-list 111 deny udp host <ip address of router sending malformed join
request> host 224.0.0.13 eq 3232
access-list 111 permit ip any any
!
```



**Note** Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to “Protecting Your Core: Infrastructure Protection Access Control Lists” at:

<http://www.cisco.com/warp/public/707/rACL.html>

This problem is resolved in Release 12.2(18)SXD7a. (CSCsb52717)

- With the Cisco IOS Firewall CBAC feature enabled, if a client opens a connection to a server, which causes a firewall session to be created, and the connection is terminated on both the client and the server, the firewall session may never time out. This problem occurs with applications that use fixed source and destination ports. This problem is resolved in Release 12.2(18)SXD7a. (CSCsc72722)
- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

Conditions: The packets must be received on a trunk enabled port.

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXD7a. (CSCsd34759)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

This problem is resolved in Release 12.2(18)SXD7a. (CSCsd34855)



## Resolved General Caveats in Release 12.2(18)SXD7

- Passwords and other sensitive information should not be sent to Access Control Server (ACS) logs. When command accounting is enabled, the full text of each command is sent to an ACS server. This information is sent to the server encrypted, but the server decrypts the packets and logs these commands in plain text. This problem is resolved in Release 12.2(18)SXD7. (CSCed09685)
- Multiple Cisco products contain vulnerabilities in the processing of IPsec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for IPsec and can be repeatedly exploited to produce a denial of service.

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

This advisory is posted at

<http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml>.

This problem is resolved in Release 12.2(18)SXD7. (CSCed94829)

- On a Supervisor Engine 2, MAC addresses unnecessarily age out every 4 seconds. This problem is resolved in Release 12.2(18)SXD7. (CSCef66632)
- When Multiprotocol Label Switching (MPLS) learns routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled, a label forwarding table entry might be missed. This problem can be seen in the output of the **show tag-switching forwarding-table EXEC** command for the missing entry and in the output of the **show ip cef detail EXEC** command for the prefix. This problem is resolved in Release 12.2(18)SXD7. (CSCsb09190)
- A reload might occur with a breakpoint exception (signal=5). This problem can occur in any release that contains the fix for CSCee28288 when a 32-bit counter continues to increment until it wraps around to 0. In most cases approximately 40 to 50 weeks of continuous uptime elapses before this problem is observed. This problem is resolved in Release 12.2(18)SXD7. (CSCsb98702)

## Resolved General Caveats in Release 12.2(18)SXD6

- Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **tcsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

This problem is resolved in Release 12.2(18)SXD6. (CSCeh73049)

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

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

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

This problem is resolved in Release 12.2(18)SXD6. (CSCei61732)

- With multiple equal-cost routes egressing on different interfaces, a Resource ReSerVation Protocol (RSVP) reservation may initially be made on the wrong interface. This problem is resolved in Release 12.2(18)SXD6. (CSCdt12296)

## Resolved General Caveats in Release 12.2(18)SXD5

- If two OSPF routing areas generate the same link-state advertisement (LSA) for a route and the route is known on the Area Border Router (ABR) as an intra-area route, a summary LSA might not be generated on the ABR if the route goes up and down. This problem is resolved in Release 12.2(18)SXD5. (CSCeg62496)
- Receipt of a Border Gateway Protocol (BGP) autonomous system (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.2(18)SXD5. (CSCeh13489)
- Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected.

Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

See the Security Advisory at the following URL for more details

<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

This problem is resolved in Release 12.2(18)SXD5. (CSCee45312)

- With SNMP ciscoEnvMonTemperature traps enabled, you might see these symptoms:
  - Multiple identical ciscoEnvMonTempStatusChangeNotif traps at the same time with these values:
 

ciscoEnvMonTemperatureStatusDescr.433 (OctetString): module 13 VDB inlet temperature

ciscoEnvMonTemperatureStatusValue.433 (Gauge): 19

ciscoEnvMonTemperatureState.433 (Integer): normal(1)
  - Between 20 through 60 seconds later, multiple identical traps with these values:
 

ciscoEnvMonTemperatureStatusDescr.433 (OctetString): module 13 VDB inlet temperature

ciscoEnvMonTemperatureStatusValue.433 (Gauge): 0

ciscoEnvMonTemperatureState.433 (Integer): notPresent(5)

This problem is resolved in Release 12.2(18)SXD5. (CSCsa87388)

- With Border Gateway Protocol (BGP) route redistribution configured to an Interior Gateway Protocol (for example, OSPF or EIGRP), routes might not be properly removed when a BGP-learned route is withdrawn. This situation might cause a control plane inconsistency and data plane forwarding loops. This problem is resolved in Release 12.2(18)SXD5. (CSCsa80861)
- If you modify an ACL configured for a microflow policer while the ACL is filtering traffic, memory corruption and a reload might occur. This problem is resolved in Release 12.2(18)SXD5. (CSCsa77211)
- Ports on a [WS-X6748-GE-TX](#) switching module, hardware revision 2.1, stop sending traffic when configured to operate only at 10 Mbps or only at 100 Mbps. This problem is resolved in Release 12.2(18)SXD5. (CSCsa76031)
- After switchover to a redundant supervisor engine with EIGRP stub routing configured, EIGRP neighbors do not see routes. This problem is resolved in Release 12.2(18)SXD5. (CSCin84644)
- A reload might fail because the software image does not decompress. This problem is resolved in Release 12.2(18)SXD5. (CSCin53807)
- IGMP snooping does not constrain multicast traffic for multicast group addresses in the range x.128-255.x.x until a receiver joins the multicast group. This problem is resolved in Release 12.2(18)SXD5. (CSCeh62522)
- With Cisco IOS SLB configured, hardware-accelerated egress IOS ACLs configured on a VLAN interface might be applied to ingress bridged traffic. This problem is resolved in Release 12.2(18)SXD5. (CSCeh54533)
- In egress multicast replication mode, after online insertion or removal (OIR) of a module, some fabric channel utilization might be higher than normal because some multicast traffic is sent across the switch fabric more than often than is necessary. This problem is resolved in Release 12.2(18)SXD5. (CSCeg28814)
- You might see input errors on 802.1Q trunks for packets larger than 1,496 bytes. This problem is resolved in Release 12.2(18)SXD5. (CSCef10010)
- The **dot1x host-mode multi-host** command might fail in these releases:
  - Release 12.2(18)SXD
  - Release 12.2(18)SXD1
  - Release 12.2(18)SXD2
  - Release 12.2(18)SXD3
  - Release 12.2(18)SXD4

This problem is resolved in Release 12.2(18)SXD5. (CSCee82867)

- In rare situations, a ROMMON upgrade for these modules might fail:
  - [WS-X6704-10GE](#)
  - [WS-X6748-SFP](#)
  - [WS-X6724-SFP](#)
  - [WS-X6748-GE-TX](#)

This problem is resolved in Release 12.2(18)SXD5. (CSCee37771)

- The **v2-single-tcp** keyword for the **dlsw remote-peer** command is not supported. See this publication for more information about the keyword:  
[http://www.cisco.com/en/US/tech/tk331/tk336/technologies\\_tech\\_note09186a0080093db6.shtml](http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a0080093db6.shtml)

This problem is resolved in Release 12.2(18)SXD5. (CSCeb47150)

- Following an NSF with SSO switchover with OSPF NSF configured, OSPF traffic loss occurs for a few seconds because neighboring OSPF routers withdraw the OSPF routes. This problem is resolved in Release 12.2(18)SXD5. (CSCsa74271)
- If you configure multiple IP service level agreement (SLA) jitter probes to send packets to the same destination IP address and port number, and you turn the responder router off and back on, the probes show traffic loss (displayed as the packetMIA value) that is equal to the probe's number of packets minus one. This problem is resolved in Release 12.2(18)SXD5. (CSCeg64124)
- A memory leak might occur on the redundant supervisor engine if there is a continuous stream of IGMP joins for unique multicast groups being sent to a port where IGMP snooping is enabled and where the total number of multicast groups is increasing. This problem is resolved in Release 12.2(18)SXD5. (CSCeg56052)
- Several MIB entity tables share one entCacheFlag and under rare circumstances, accessing the MIB entity tables might cause an entCacheFlag state that is not valid for all the MIB entity tables and a reload might occur. This problem is resolved in Release 12.2(18)SXD5. (CSCeg19038)
- If you repeatedly change the configuration of a Gigabit Ethernet interface between Layer 2 and Layer 3 when there is traffic flowing, the interface drops traffic. This problem is resolved in Release 12.2(18)SXD5. (CSCef82367)
- Modifying the configuration of statically configured bidirectional PIM rendezvous points (RPs) can cause very high CPU utilization. This problem is resolved in Release 12.2(18)SXD5. (CSCef36367)
- Policing might not be accurate for packets smaller than 82 bytes. This problem is resolved in Release 12.2(18)SXD5. (CSCee78451)
- Boot failure might occur when there are more than 256 different policy maps attached as service policies. This problem is resolved in Release 12.2(18)SXD5. (CSCee24349)
- On an EtherChannel IEEE 802.1q trunk that is configured with VLAN 1 as the native VLAN, connectivity is lost if you change the native VLAN. This problem is resolved in Release 12.2(18)SXD5. (CSCsa80358)

#### Resolved General Caveats in Release 12.2(18)SXD4

- Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

This problem is resolved in Release 12.2(18)SXD4. (CSCef68324)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

This problem is resolved in Release 12.2(18)SXD4. (CSCef60659, CSCef44225, CSCsa59600, CSCef44699, CSCef61610)

- When an OSPF external route has a forwarding address with a next hop address in the routing table, the next hop address does not get updated in the type 5 link-state advertisement (LSA) when the forwarding address gets a more specific entry in the routing table with a different next hop address. This problem is resolved in Release 12.2(18)SXD4. (CSCed59370)
- When the MPLS-LSR-MIB MIB is enabled and you query the object mplsXCIndexNext and there are more than 1,000 Multiprotocol Label Switching (MPLS) labels active, the Simple Network Management Protocol (SNMP) agent might use 99 percent of the CPU capacity of the MSFC for an arbitrarily long time and might generate CPUHOG errors and cause a reload. This problem is resolved in Release 12.2(18)SXD4. (CSCef37186)
- You cannot configure the MAC address aging time for traffic that has the routed MAC (RM) bit set. This problem is resolved in Release 12.2(18)SXD4 with the **mac-address-table aging-time number\_of\_seconds routed-mac** command. (CSCef72013)
- In rare situations, with a mix of Link State Advertisements (LSAs) that travel throughout the Autonomous System (Types 5 and 11) and LSAs that travel within a particular open shortest path first (OSPF) area (Types 1, 2, 3, 4, 6, 7, 9 and 10), a reload might occur. This problem is resolved in Release 12.2(18)SXD4. (CSCef93215)
- The BPDU guard feature does not work on an access port when you configure a voice VLAN unless either the voice VLAN or the access VLAN is VLAN 1. This problem is resolved in Release 12.2(18)SXD4. (CSCef93371)
- In a PE router configuration, the CoS value of BPDU packets are not copied to the MPLS EXP bits. This problem is resolved in Release 12.2(18)SXD4. (CSCsa59260)

- The output of the **show diskslot\_number** and **dir diskslot\_number** commands might be inconsistent or the commands might show a file more than once in any of these situations:
  - When you delete a file, and the deletion is successful, but you see a “No such file” message.
  - When you enter the **fsck** command and a file is truncated and an orphan file is created.
  - When you copy multiple images.
  - When you make two copies of a file to the disk using two VTYs and you enter the **show diskslot\_number** and **dir diskslot\_number** commands at the same time from the two VTYs.
  - When you rename a directory that has many subdirectories or files.
  - When an snmpGet operation on a ciscoFlashFileSize object enters a loop because of the problem underlying caveat CSCed63357.

This problem is resolved in Release 12.2(18)SXD4. (CSCed63357)

- A reload might occur if you enter the **show ip bgp** command. This problem is resolved in Release 12.2(18)SXD4. (CSCef50427)
- Ingress multicast traffic might stop after the receipt of a multicast join message on an RPF interface if a downstream router has already converged. This problem is resolved in Release 12.2(18)SXD4. (CSCef60452)
- OSPF might generate recurring SYS-3-CPUHOG messages and tracebacks. This problem is resolved in Release 12.2(18)SXD4. (CSCef65500)
- A connection between two [WS-X6704-10GE](#) switching module ports equipped with 10GBASE-LR XENPAKs occasionally stops transmitting and receiving, but the interface state always remains “up/up.” This problem is resolved in Release 12.2(18)SXD4. (CSCef96465)
- In a configuration with two PE routers that advertise routes via eBGP and a border router that is configured with a higher local preference than the PE routers, when the eBGP route of the primary path is withdrawn and the route of the secondary path is installed, an eBGP route might continue to be redistributed into EIGRP after the eBGP route is deleted or EIGRP might not redistribute an eBGP route after the eBGP route has been installed. This problem is resolved in Release 12.2(18)SXD4. (CSCeg07725)
- An SNMP walk on LAN switching module 802.1Q subinterfaces might return inaccurate 64-bit statistics for InOctets and OutOctets. This problem is resolved in Release 12.2(18)SXD4. (CSCeg26993)
- If you delete a Layer 3 LAN port subinterface, the port’s traffic counters stop working. This problem is resolved in Release 12.2(18)SXD4. (CSCeg48068)
- In NSF with SSO redundancy mode, a redundant Supervisor Engine 720 might reload when you configure Frame Relay. This problem is resolved in Release 12.2(18)SXD4. (CSCeg51616)
- Ingress VLAN SPAN (VSPAN) does not work for voice VLANs. This problem is resolved in Release 12.2(18)SXD4. (CSCeg70376)
- When eBGP multihop is configured between PE and CE routers and static VRF routes are configured in the PE router to reach the CE router's address, the routes learned through the eBGP session are not populated in the LFIB table. This situation drops packets coming from the PE routers. This problem is resolved in Release 12.2(18)SXD4. (CSCeg90033)
- When BGP next hop information for a prefix changes because of topology changes, BGP updates its path information and IP routing table entry properly, but CEF might not update the corresponding CEF entry, which leaves a stale CEF entry. This inconsistency between BGP and CEF might cause a connectivity problem. This problem is resolved in Release 12.2(18)SXD4. (CSCeh07809)



- In releases where caveat [CSCef30577](#) is resolved, adding or changing an IP address on a loopback interface might cause a reload. This problem is resolved in Release 12.2(18)SXD4. (CSCeh12233)
- Configuring WCCPv2 on a Supervisor Engine 720 causes high CPU utilization. This problem is resolved in Release 12.2(18)SXD4. (CSCeh13292)
- The commands to configure OSPF for redistribution into a specific VRF in another routing protocol are not saved in the configuration file and after a reload, OSPF uses the default routing table. This problem is resolved in Release 12.2(18)SXD4. (CSCeh15802)
- When a CE router stops advertising a BGP route to a PE router, the BGP routing table on the PE router reflects the route change, but still indicates that the route is valid. This problem is resolved in Release 12.2(18)SXD4. (CSCsa40588)
- Rarely, on a Supervisor Engine 720, a fabric synchronization error might cause a reload during bootup. This problem is resolved in Release 12.2(18)SXD4. (CSCsa49748)
- With a Supervisor Engine 720, configuring RSPAN causes high CPU utilization. This problem is resolved in Release 12.2(18)SXD4. (CSCsa51770)
- With a Supervisor Engine 720, dCEF hardware switching might freeze if you shut down an interface or change VRF routes and no other interfaces can be provisioned to handle the traffic. This problem is resolved in Release 12.2(18)SXD4. (CSCsa53117)
- The CEF table might be incorrect if you configure a static route in one VRF on two separate PE routers and the static route is exported into another VRF. This situation causes suboptimal routing. This problem is resolved in Release 12.2(18)SXD4. (CSCsa55048)

### Resolved General Caveats in Release 12.2(18)SXD3

- If the number of Layer 4 operations specified in the ACL exceeds 12, the destination ports for the additional operations will not expand. This problem is resolved in Release 12.2(18)SXD3. (CSCeg19269)
- After removing a VRF instance from the configuration, a CEF table error and a data structure error might occur. This problem is resolved in Release 12.2(18)SXD3. (CSCsa44122)
- Layer 3-interface statistics collection causes higher than normal CPU utilization. This occurs with a large number of EtherChannels configured. This problem is resolved in Release 12.2(18)SXD3. (CSCef01725)
- In a network with MPLS VPN configured, the system may lose IP connectivity. This occurs when a configured QoS policy causes aggregate MPLS labels to be recirculated through the PFC. After this recirculation, the entries for the VLANs that were mapped to the aggregate MPLS labels are removed from the route table. This problem is resolved in Release 12.2(18)SXD3. (CSCef14446)
- VRF is taking approximately 10 minutes to delete instances from the VRF table instead of approximately one minute. This problem is resolved in Release 12.2(18)SXD3. (CSCee85202)
- An ACL configured to filter with an IP address and a Layer 4 port number ignores the IP address and filters only on the Layer 4 port number. This problem is resolved in Release 12.2(18)SXD3. (CSCin84750)
- With redundant Supervisor Engines, following a NSF/SSO switchover, the forwarding tables for the port ASIC on the WS-X6816-GBIC fail to repopulate. This causes traffic to be dropped. This problem is resolved in Release 12.2(18)SXD3. (CSCef88685)
- Catalyst 67xx-series DFC-equipped modules may reset during process intensive tasks such as MAC limiting. This problem is resolved in Release 12.2(18)SXD3. (CSCef58323)
- In rare situations, a timing problem might cause a Supervisor Engine 720 to reload. This problem is resolved in Release 12.2(18)SXD3. (CSCee86168)

- With TCP header compression configured, TCP packet length is incorrect after decompression. This problem is resolved in Release 12.2(18)SXD3. (CSCeg08344)
- A reload might occur when Optimized Edge Routing (OER) and BGP dampening are both configured and OER injects a route that does not exist in the routing information base (RIB). This problem is resolved in Release 12.2(18)SXD3. (CSCed63876)
- VRF traffic might be routed in software on the MSFC because CEF entries are not updated. This problem is resolved in Release 12.2(18)SXD3. (CSCeg26378)
- MPLS-to-IP traffic might not recover after switchover to a redundant supervisor engine. This problem is resolved in Release 12.2(18)SXD3. (CSCee37430)
- With a Supervisor Engine 720 and a [WS-SVC-NAM-2](#), a reload occurs after an SSO switchover if you enter the **ip route-cache flow** command under an ATM physical interface and the **ip nbar protocol-discovery** command under an ATM subinterface. This problem is resolved in Release 12.2(18)SXD3. (CSCef06034)
- A reload might occur if you configure NetFlow version 9 on the MSFC. This problem is resolved in Release 12.2(18)SXD3. (CSCeg02873)
- With a Supervisor Engine 2, the software and hardware CEF tables might not be consistent with each other. This problem is resolved in Release 12.2(18)SXD3. (CSCef27359)
- With a configuration that connects an MPLS backbone to an IPv4 cloud, traffic might be dropped following a reload. This problem is resolved in Release 12.2(18)SXD3. (CSCeg40177)
- When an extremely low amount of free memory disables CEF, traffic is dropped in hardware. This problem is resolved in Release 12.2(18)SXD3: the traffic is sent to the MSFC to be routed in software. (CSCee76895)
- With parallel links between two provider edge (PE) routers, the Label Distribution Protocol (LDP) does not work after failure of one of the links. This problem is resolved in Release 12.2(18)SXD3. (CSCeg24287)
- IEEE 802.1X port-based authentication might not work if it is enabled on more than 50 ports. This problem is resolved in Release 12.2(18)SXD3. (CSCin83972)
- BGP might send incorrect updates to peers for which the “remove-private-as” BGP feature or the “as-override” BGP feature is configured. This problem is resolved in Release 12.2(18)SXD3. (CSCeg31951)
- With a Supervisor Engine 720 and a PFC3BXL, the Layer 2 CoS value of egress-routed multicast traffic might be changed inappropriately. This problem is resolved in Release 12.2(18)SXD3. (CSCeg06698)
- With exterior border gateway protocol (eBGP) neighbors from different autonomous systems (AS) in the same peer-group, the “remote-private-as” feature might fail to remove a private AS from BGP updates. This problem is resolved in Release 12.2(18)SXD3. (CSCeg05830)
- An implicit-null label might be allocated to an MPLS traffic engineering tunnel. This problem is resolved in Release 12.2(18)SXD3. (CSCeg03885)
- If BGP multipath is not configured for the IPv4 unicast address family, then multipath does not work correctly for other address families. This problem is resolved in Release 12.2(18)SXD3. (CSCef89294)
- An MPLS traffic engineering tunnel to a non-Cisco device that ignores PathErr and ResvTear messages might stop carrying traffic after failure and recovery of a Cisco interface in the tunnel. This problem is resolved in Release 12.2(18)SXD3. (CSCef80349)



- After tunnels have been configured and removed, traffic loss occurs over OSM POS links, OSM ATM links, and FlexWAN serial links. This problem is resolved in Release 12.2(18)SXD3. (CSCef76828)
- MAC addresses learned through a [WS-F6K-DFC3A](#) card on a [WS-X6516A-GBIC](#) switching module are not sent to the PFC3. This problem is resolved in Release 12.2(18)SXD3. (CSCef48810)
- The **snmp-server enable traps config** command is always rejected as ambiguous. This problem is resolved in Release 12.2(18)SXD3. (CSCef42312)
- The software does not respond to hardware-reported ECC errors in the Layer 2 MAC address table. This problem is resolved in Release 12.2(18)SXD3. (CSCef35707)
- Non-BGP static routes configured with BGP-specific match statements might not be redistributed. This problem is resolved in Release 12.2(18)SXD3. (CSCef08797)
- You might see “ALIGN-3-SPURIOUS: Spurious memory access” messages. This problem is resolved in Release 12.2(18)SXD3. (CSCee88898)
- With the **maximum-paths import** command configured, a BGP VPNv4 table might contain paths that were imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix. This problem is resolved in Release 12.2(18)SXD3. (CSCee59315)
- When you bring up a single bundle link associated with a multilink Frame Relay (MFR) interface, there might be no local management interface (LMI) exchanges over the MFR interface. This problem is resolved in Release 12.2(18)SXD3. (CSCee32365)
- If you remove a secondary IP address from a VRRP group, the MAC address associated with the group is also removed from the interface. This situation causes a loss of connectivity for the rest of IP addresses in the VRRP group. This problem is resolved in Release 12.2(18)SXD3. (CSCed82551)
- Unicast routing updates might not be sent to RIP static neighbors. This problem is resolved in Release 12.2(18)SXD3. (CSCed63342)
- An MPLS VPN PE router might use a source address from its global routing table for some packets that originate in one of its VRF interfaces when it replies to an ICMP echo request that was sent from a VRF interface of another router through the MPLS backbone to the network or to a broadcast address of the VRF interface on the MPLS VPN PE router. This problem is resolved in Release 12.2(18)SXD3. (CSCec10116)
- In rare situations, intensive SNMP polling might use all available I/O memory. This problem is resolved in Release 12.2(18)SXD3. (CSCeg11566)
- With IGMP snooping disabled and with a static multicast address configured in a VLAN, a reload might occur if you enter the **vlan *vlan\_id*** and **no vlan *vlan\_id*** global configuration commands for the VLAN. This problem is resolved in Release 12.2(18)SXD3. (CSCeg01510)
- In rare situations, a software-forced reload might occur. This problem is resolved in Release 12.2(18)SXD3. (CSCef91572)
- A VACL can match BPDUs. Spanning tree loops can occur if the VACL drops or redirects the BPDUs. This problem is resolved in Release 12.2(18)SXD3. (CSCef58932)
- With a large number of EtherChannels configured, CPU utilization might periodically rise to unacceptably high values. This problem is resolved in Release 12.2(18)SXD3. (CSCee55233)
- With VRF and more than 9,000 routes configured, the CEF reloader process might cause CPUHOG messages to be displayed. This problem is resolved in Release 12.2(18)SXD3. (CSCed57281)

- When more than 12 logical operator units (LOUs) are used in a policy attached to an interface, the entries are expanded. If the expanded entries are for a non-deny ACE, the entries are not accurate. The resulting ACEs for the policy are also inaccurate. This problem is resolved in Release 12.2(18)SXD3. (CSCed47753)

## Resolved General Caveats in Release 12.2(18)SXD2

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

This problem is resolved in Release 12.2(18)SXD2. (CSCee67450)

- Some traffic loss might occur when all of the following situations occur simultaneously:
  - You have a nontrunking Layer 2 EtherChannel with member ports on a fabric-enabled module and on a nonfabric-enabled module (for example, an EtherChannel with member ports on a Supervisor Engine 720 and on a [WS-X6408A-GBIC](#) switching module).
  - You have two or more [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching modules installed, or you have one of each.
  - You have a port in the same VLAN as the EtherChannel on each [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching module.
  - One of the [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching modules resets.

This problem is resolved in Release 12.2(18)SXD2. (CSCef82797)

- The PFC2 does not support source-only or destination-only microflow policing, but after an SSO switchover, the flow mask is set to destination only. This problem is resolved in Release 12.2(18)SXD2. (CSCin82979)
- DFC-equipped switching modules support only 1024 VLANs for egress multicast replication. This problem is resolved in Release 12.2(18)SXD2. (CSCef63549)
- After a reload, Control Plane Policing (CoPP) is not supported in hardware. This problem is resolved in Release 12.2(18)SXD2. (CSCeg05819)
- When one of two trunks configured as parallel links goes down, traffic might be directed to the inactive trunk instead of to the active trunk. This problem is resolved in Release 12.2(18)SXD2. (CSCef89139)
- With BGP multipath support enabled, eBGP learns two equivalent eBGP paths from the same neighboring AS, but it installs only one best path in the IP routing table. This problem is resolved in Release 12.2(18)SXD2. (CSCea19918)

- Some IP traffic might be sent with incorrect alignment, and you might see “ALIGN-SP-3-CORRECT: Alignment correction made” messages. This problem is resolved in Release 12.2(18)SXD2. (CSCef73076)

## Resolved General Caveats in Release 12.2(18)SXD1

- A system may lock for a long period of time while several instances of the following message are displayed:

```
%CWAN_RP-4-SEMAHOG: Process 74 (MIP Mailbox)hogging CCB BLK Sema 10! calling proc 221 (IFCOM Msg Hdlr)
```

This problem is resolved in Release 12.2(18)SXD1. (CSCin79495)

- When you enter the **shutdown** and **no shutdown** interface commands on an ATM subinterface, the state of an associated permanent virtual circuit (PVC) will be UP on an active supervisor engine and INAC on the standby supervisor engine. This problem exists with a large number of PVCs configured (for example, 500). This problem is resolved in Release 12.2(18)SXD1. (CSCin79468)
- Connectivity for destinations that are reachable by an MPLS TE tunnel may fail when the tunnel is fast-rerouted. The loss of connectivity may result in the loss of TCP sessions (Border Gateway Protocol (BGP), Label Distribution Protocol (LDP), and so forth.) for those destinations.

When the problem occurs, the output of the **show ip cef** network command shows “invalid cached adjacency” for the tunnel but does not show “fast tag rewrite”.

This problem occurs when all of the following conditions are present:

- The adjacency of the primary tunnel becomes incomplete when FRR is active, as can be observed in the output of the **show adjacency [type number]** command. Whether or not the adjacency becomes incomplete is media dependent. For example, with Point-to-Point Protocol (PPP) the adjacency becomes incomplete. With High-Level Data Link Control (HDLC), the adjacency does not become incomplete.
- The primary tunnel is the only path to reach the prefix in question.
- The **ip cef accounting non-recursive** command is not enabled.
- A routing change occurs for the prefix after the FRR switchover. (Dependency on this condition is topology dependent.)

The symptom affects the traffic that originates on the tunnel head end. The transit traffic going through the tunnel is not affected. The symptom does not occur if there are multiple paths to the destination, where one of the paths is the tunnel.

### Workaround:

- Use HDLC encapsulation instead of PPP to prevent the adjacency from becoming incomplete.
- Use forwarding adjacencies to prevent the routing change.

This problem is resolved in Release 12.2(18)SXD1. (CSCef25866)

- With Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) configured, a reload might occur when you connect or disconnect a Packet-over-SONET (POS) interface cable. This problem is resolved in Release 12.2(18)SXD1. (CSCed54416)
- MPLS traffic-engineered (TE) network tunneling port counters fail to increment if the tunnel’s head-end node also acts as a provider edge (PE) interface for a carrier supporting carrier (CSC) that provides MPLS virtual private network (VPN) services. This problem is resolved in Release 12.2(18)SXD1. (CSCee68057)

- Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

This problem is resolved in Release 12.2(18)SXD1. (CSCin82407)

- When a recursive route is deleted, the CEF hardware table entry is not updated immediately and traffic is sent to the MSFC to be routed in software for a longer period than is correct. This problem is resolved in Release 12.2(18)SXD1. (CSCef30577)




---

**Note** See resolved caveat [CSCeh12233](#) for information related to caveat CSCef30577.

---

- With multicast support configured on a Supervisor Engine 2, VACLs do not capture traffic for RSPAN. This problem is resolved in Release 12.2(18)SXD1. (CSCef07017)
- Non-Cisco P routers sometimes change the label on a TE tunnel without issuing a tear message. This situation causes a Cisco router to receive an “RESV” message with a label that is different from the previously programmed label and program an implicit null for the IP address associated with the tunnel. This problem is resolved in Release 12.2(18)SXD1. (CSCed21063)
- Using SNMP to change the name of VLAN 1002, 1003, 1004, or 1005 causes a traceback and corrupts the VLAN database. This problem is resolved in Release 12.2(18)SXD1. (CSCef43000)
- If MPLS changes state rapidly, MPLS interfaces might stop passing traffic. This problem is resolved in Release 12.2(18)SXD1. (CSCin78000)
- The **network** keyword for the **isis** interface command is not present on LAN interfaces. This problem is resolved in Release 12.2(18)SXD1. (CSCed77612)
- SNMP get-bulk requests for objects in the CISCO-STACK-MIB raises CPU utilization unacceptably. This problem is resolved in Release 12.2(18)SXD1. (CSCef67810)
- With redundant Supervisor Engine 720s, occasionally following an SSO switchover, a [WS-X6816-GBIC](#) switching module might reset. This problem is resolved in Release 12.2(18)SXD1. (CSCef41228)

- With the following configuration, some Layer 3 traffic that traverses a Layer 2 EtherChannel might be lost and some Layer 3 traffic that is processed by the central rewrite engine (for example, multicast, GRE, MPLS, IPV6, NAT, PBR) might be lost:

- **WS-SUP720**, hardware revision 3.2 or higher

Enter the **show module version | include WS-SUP720-** command to display the hardware revision. For example:

```
Router# show module version | include WS-SUP720-
7      2  WS-SUP720-BASE      SAD075301SZ Hw :3.2
```

- SPAN or RSPAN configured
- “Flow through” global fabric switching mode

Enter the **show fabric switching-mode | include Global** command to display the global switching mode. For example:

```
Router# show fabric switching-mode | include Global
Global switching mode is Flow through
```

An additional effect is that local SPAN and RSPAN source ports do not copy VACL-redirected traffic. This problem is resolved in Release 12.2(18)SXD1. (CSCef75924, CSCef78235)

- If you enter the **no mls mpls tunnel-recir** and **mls mpls tunnel-recir** commands, MPLS VRF PE-to-CE traffic over a GRE tunnel is switched in software on the MSFC. This problem is resolved in Release 12.2(18)SXD1. (CSCef07848)
- Under the following circumstances, some OSM configuration commands fail:
  - Redundant supervisor engine installed.
  - The configuration file is large.
  - The configured redundancy mode is SSO or RPR+.
  - The operational redundancy mode is RPR because the supervisor engines have different software versions.
  - You do an RPR fast software upgrade to synchronize the supervisor engine images.
  - You boot the redundant supervisor engine while the active supervisor engine is booting.

This problem is resolved in Release 12.2(18)SXD1. (CSCef10192)

- With a Supervisor Engine 720, NetFlow entries for Cisco IOS SLB firewall load balancing do not age out correctly. This situation causes some packets to be forwarded incorrectly and some connections cannot be made. This problem is resolved in Release 12.2(18)SXD1. (CSCee70293)
- The unknown unicast flood protection (UUFP) **mac-address-table unicast-flood** command does not always work after an SSO switchover. This problem is resolved in Release 12.2(18)SXD1. (CSCin78773)
- The **match ip address** VACL configuration command accepts only one ACL. This problem is resolved in Release 12.2(18)SXD1. (CSCin74811)
- With a Supervisor Engine 720, after an SSO switchover, Cisco IOS SLB might not work. This problem is resolved in Release 12.2(18)SXD1. (CSCee43191)
- If routes from one VRF table are distributed to another VRF table, occasionally the port-to-VRF mapping is incorrect. This problem is resolved in Release 12.2(18)SXD1. (CSCef44976)
- Occasionally, an all-zero address entry for a static route is made in the hardware routing table because the entry is made before the adjacency for the address is resolved. This problem is resolved in Release 12.2(18)SXD1. (CSCef30308)

- If BGP receives identical route information from two different BGP routers, the hardware routing table only has the routes from one of the BGP routers. If the link to that BGP router goes down, all BGP routing occurs in software on the MSFC until new routes are installed in the hardware routing table. This situation causes long BGP convergence times and high CPU utilization. This problem is resolved in Release 12.2(18)SXD1. (CSCef08097)
- In a PE configuration, you might see “TOOBIG” messages and a traceback. This problem is resolved in Release 12.2(18)SXD1. (CSCee95708)
- With a Supervisor Engine 720, a reload might occur when you configure context-based access control (CBAC). This problem is resolved in Release 12.2(18)SXD1. (CSCee75620)
- Some type-7 encrypted forms of passwords might not work. This problem is resolved in Release 12.2(18)SXD1. (CSCed88768)
- With the same IP address configured on two interfaces as part of the Packet-over-SONET (POS) Automatic Protection Switching (APS) configuration, when one interface goes down, traffic destined to the IP address might not be received by the interface that remains up. This problem is resolved in Release 12.2(18)SXD1. (CSCed36386)
- With incremental shortest path first (iSPF) configured under open shortest path first (OSPF), a reload might occur. This problem is resolved in Release 12.2(18)SXD1. (CSCec22723)
- Network Address Translation (NAT) does not work with WCCP configured. This problem is resolved in Release 12.2(18)SXD1. (CSCeb28941)
- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

This problem is resolved in Release 12.2(18)SXD1. (CSCef46191)

- Occasionally, these modules might lose the ability to communicate over the Ethernet Out of Band Channel (EOBC) and reset:
  - [WS-X6416-GBIC](#)
  - [WS-X6348-RJ-45](#)
  - [WS-X6148-RJ-45](#)
  - [WS-X6348-RJ-21V](#)
  - [WS-X6148-RJ-21](#)
  - [WS-X6316-GE-TX](#)
  - [WS-X6324-100FX](#)
  - [WS-X6416-GE-MT](#)
  - [WS-X6024-10FL-MT](#)

This problem is resolved in Release 12.2(18)SXD1. (CSCef23843)

- When an output ACL is applied on multiple interfaces and the first interface to which it is applied is not configured with an IP address, the ACL denies all traffic on all interfaces where it is applied. This problem is resolved in Release 12.2(18)SXD1. (CSCef21575)
- RFC 1889 Compressed Real-Time Protocol (cRTP) does not work with CEF enabled on FlexWAN modules. This problem is resolved in Release 12.2(18)SXD1. (CSCee85257)
- A reload might occur if you use SNMP to collect the statistics from a policy map that has a shared aggregate policer. This problem is resolved in Release 12.2(18)SXD1. (CSCee83655)
- With BGP and MPLS configured on OC-48, OC-12, or OC-3 OSM-POS interfaces, BGP neighbors go up and down every few hours. This problem is resolved in Release 12.2(18)SXD1. (CSCee72817)
- When a large number of VRFs (more than 200) and prefixes (more than 220,000) are configured, BGP inbound update processing slows down and prolonged high CPU utilization occurs. This problem is resolved in Release 12.2(18)SXD1. (CSCee43166)
- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

This problem is resolved in Release 12.2(18)SXD1. (CSCed78149)

- In VTP transparent mode, the VLAN database might be lost after a VTP configuration error occurs. This problem is resolved in Release 12.2(18)SXD1. (CSCef47414)

## Resolved General Caveats in Release 12.2(18)SXD

- After a Stateful Switchover (SSO) occurs, the redundant supervisor engine might stop responding. This situation might prevent the redundant supervisor engine from entering the STANDBY-HOT state and from being ready to perform a switchover. This problem is resolved in Release 12.2(18)SXD. (CSCed92837)
- Traffic that uses a Layer 2 port channel interface is software switched after that port channel is removed and recreated. This problem is resolved in Release 12.2(18)SXD. (CSCee56573)



- With a Supervisor Engine 720, you might see software-forced reloads. This problem is resolved in Release 12.2(18)SXD. (CSCed36177)
- Following an RPR+ switchover, the MLS long aging value is not synchronized to the redundant supervisor engine. This problem is resolved in Release 12.2(18)SXD. (CSCee32301, CSCsa68081)
- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>.

This problem is resolved in Release 12.2(18)SXD. (CSCed65285, CSCed65778)

- The inner time-to-live (TTL) field is not decremented properly in tunneled traffic. This problem is resolved in Release 12.2(18)SXD. (CSCee30816)
- A memory leak might occur when the MPLS Label Switching Router (LSR) MIB is queried. This problem is resolved in Release 12.2(18)SXD. (CSCee26700)
- A reload might occur if you perform Simple Network Management Protocol (SNMP) get operations on Open Shortest Path First (OSPF) MIBs. This problem is resolved in Release 12.2(18)SXD. (CSCeb40561)
- Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

More details can be found in the security advisory, which is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

This problem is resolved in Release 12.2(18)SXD. (CSCed40933)

- In rare situations, this message might be displayed:

```
ro=1: PBIF mem ECC1 P2N
```

The message indicates that an ECC error has been detected in a packet. The message is not sent to SYSLOG servers. This problem is resolved in Release 12.2(18)SXD. (CSCed79251)

- With a PFC2 or DFCs, you might see “L3-PS-DRVR” messages. This problem is resolved in Release 12.2(18)SXD. (CSCee24424)
- If IGMP snooping source specific multicast (SSM) safe reporting is enabled on a VLAN with both IGMPv2 and IGMPv3 hosts, then any IGMP leave sent by the IGMPv2 hosts is ignored. This problem is resolved in Release 12.2(18)SXD. (CSCee53706)
- A reload might occur if one process is writing to NVRAM and another process is reading from NVRAM and the read fails. This problem is resolved in Release 12.2(18)SXD. (CSCec63011)
- While the output of the **show ip vrf interface** command is being displayed in one administrative session, a reload might occur if you enter **no ip vrf** commands in another administrative session. This problem is resolved in Release 12.2(18)SXD. (CSCeb40653)



- In IP packets with the IP options field populated, the IP type of service (ToS) byte might be truncated to a 3-bit long field. This problem deletes 3 bits of the 6-bit DSCP value and causes incorrect QoS operation. This problem is resolved in Release 12.2(18)SXD. (CSCed93264)
- There is no response to SNMP requests and memory use increases until tracebacks occur. This problem is resolved in Release 12.2(18)SXD. (CSCed52841)
- With a default route configured, a reload might occur if you enter the **clear ip route \*** command. This problem is resolved in Release 12.2(18)SXD. (CSCee35125)
- This message might be displayed, followed by a reload:

```
EARL-SP-2-PATCH_INVOCATION_LIMIT: 10 Recovery patch invocations
in the last 30 secs have been attempted.
Max limit reached
```

This problem is resolved in Release 12.2(18)SXD. (CSCed66865)

- With ROMMON configured to ignore the startup-config file, if you enter the **mls cef maximum-routes** command and do a reload, continuous reloads occur. This problem is resolved in Release 12.2(18)SXD. (CSCee07395)
- With OSPF configured between a PE router and a CE router, when there is an import map configured on the PE router, there are no routes from the CE router in the BGP route table. This problem is resolved in Release 12.2(18)SXD. (CSCed81317)
- With IGMP snooping configured, the flow of multicast traffic to a multicast receiver might be stopped after failure to respond to one IGMP query, instead of two. This problem is resolved in Release 12.2(18)SXD. (CSCee68052)
- The DSCP value is incorrectly set to zero in NBAR traffic. This problem is resolved in Release 12.2(18)SXD. (CSCec49042)
- OIR of a fabric-enabled switching module might cause a reload. This problem is resolved in Release 12.2(18)SXD. (CSCec12236)
- When configured as a PE router, if you change the layer encapsulation of a PPP, Frame Relay, or HDLC PE subinterface, ping traffic to a CE router might fail. This problem is resolved in Release 12.2(18)SXD. (CSCed13350)
- In a VRF-lite configuration, if you import host routes from one VRF to a VRF configured on a LAN interface, traffic destined to those host routes that is received in the VRF into which the routes were imported is routed in software on the MSFC3. This problem is resolved in Release 12.2(18)SXD. (CSCea47545, CSCed13707)
- QoS access control lists with Layer 4 port operations are not supported. This problem is resolved in Release 12.2(18)SXD. (CSCdx91720)
- When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as “OID not increasing” might occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured but HSRP is not configured at all. This problem is resolved in Release 12.2(18)SXD. (CSCed52163)
- With an ATA flash device, you might see this message:

```
PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router or PC. A format
in this router is required before an image can be booted from this device
```

This problem is resolved in Release 12.2(18)SXD. (CSCec69091)

- When a Layer 3 VLAN interface is configured as an OSPF nonbroadcast network and a polling interval is configured for every OSPF neighbor, unnecessary ARPs are sent. This problem is resolved in Release 12.2(18)SXD. (CSCed26217)
- With a PFC2 and GRE tunnel traffic, the do not fragment (DF) bit not be copied correctly and the time-to-live (TTL) count might not be decremented correctly. This problem is resolved in Release 12.2(18)SXD. (CSCuk49481)
- SNMP returns a null value for the Cisco IOS SLB real server name. This problem is resolved in Release 12.2(18)SXD. (CSCee60121)
- After a reload, the **no diagnostic cns publish** and **logging event link-status** commands revert to their defaults in the running-config file and **switchport mode access** commands might be missing from the running-config file. This problem is resolved in Release 12.2(18)SXD. (CSCee53998)
- 802.1X port-based authentication does not support receipt of a VLAN ID in the tunnel attribute from a RADIUS server. The tunnel attribute from a RADIUS server is seen as a VLAN name. This problem is resolved in Release 12.2(18)SXD. (CSCee51684)
- In a release where caveat CSCeb06811 is resolved and with STP loop guard configured, two ports connected together might incorrectly stay in the STP loopguard loop-inconsistent state. This problem is resolved in Release 12.2(18)SXD. (CSCee45170)
- No Cisco Discovery Protocol (CDP) packets are received if you enter the **dlsw ethernet redundancy-enable** command on a VLAN interface. This problem is resolved in Release 12.2(18)SXD. (CSCee39240)
- With very large flows, NDE byte counts might be incorrect (NDE packet counts remain correct). This problem is resolved in Release 12.2(18)SXD. (CSCee23058, CSCee65953)
- PIM does not remove interfaces from the (S,G) output interface list when it receives a (\*,G) prune message if the interfaces were added to the (S,G) output interface list because of a (\*,G) join message. This problem is resolved in Release 12.2(18)SXD. (CSCee04368)
- When you configure NBAR on a LAN port, there is no message that the NBAR traffic is processed in software on the MSFC. This problem is resolved in Release 12.2(18)SXD. (CSCed90255)
- The VLAN translation feature does not work on **WS-X6816-GBIC** modules. This problem is resolved in Release 12.2(18)SXD. (CSCed73700)
- A VLAN interface configured on a VLAN that is carrying Layer 2 protocol tunneling traffic processes untagged CDP frames and displays the CDP-frame-source devices as CDP neighbors. This problem is resolved in Release 12.2(18)SXD. (CSCed55283)
- After a few days of running time, the **show environment temperature** command does not display current values. This problem is resolved in Release 12.2(18)SXD. (CSCed49423)
- A Secure Shell (SSH) connection that is using TACACS+ for authentication that fails due to an unknown username or incorrect password results in a memory leak and a TCP connection that hangs in the CLOSEWAIT or ESTAB state. An SSH2 connection (if supported) results in the leak even if the authentication succeeds. This problem is resolved in Release 12.2(18)SXD. (CSCed65285)
- With the **service compress-config** command or the **boot config** command in the configuration, a reload because of a bus error and stack overflow or stack corruption might occur if the configuration is larger than the NVRAM size and you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command. This problem is resolved in Release 12.2(18)SXD. (CSCed45942)
- After some VRF interfaces go up and down, several prefixes for nonredistributed and connected interfaces in the VRFs may be partially bound to the same MPLS VPN label, causing traffic that is bound for one or more of these VRFs to be disrupted. This problem is resolved in Release 12.2(18)SXD. (CSCed45746)

- Caveat CSCdz27200 is resolved in Release 12.2(14) and in Release 12.2(14)SX and later 12.2SX releases. In releases where caveat CSCdz27200 is resolved, files copied to an ATA disk might be corrupt. This problem is resolved in Release 12.2(18)SXD. (CSCed44319)
- When configured as an MPLS VPN PE router with recursive routes that go over the PE-CE link and with the link's CE-side IP address as the next hop, or if labels for IPv4 BGP routes are exchanged, and with a less specific route to get to the next hop, the DFC tag forwarding tables might not have complete entries even though the MSFC does. This situation drops ingress tagged traffic for the missing tag forwarding entries. This problem is resolved in Release 12.2(18)SXD. (CSCed39059)
- If you configure a Bridge-Group Virtual Interface (BVI), a reload might occur when IP packets are received through the BVI and then these IP packets are forwarded as Multiprotocol Label Switching (MPLS) packets through another interface. This problem is resolved in Release 12.2(18)SXD. (CSCed22837)
- You might see high CPU utilization if you enter the **logging synchronous** command. This problem is resolved in Release 12.2(18)SXD. (CSCed16920)
- Malfunctioning PIM, MLSM, or mwheel processes might cause “CPUHOG” and “WATCHDOG” messages and reloads. This problem is resolved in Release 12.2(18)SXD. (CSCed12393)
- Ping packets that are larger than 1498 bytes might not pass successfully through a multilink interface when a bridge group is configured on the multilink interface. This problem is resolved in Release 12.2(18)SXD. (CSCed09364)
- A 512 MB small outline DIMM (SODIMM) registers as only 256 MB when you enter the **show diagnostic** command. This problem is resolved in Release 12.2(18)SXD. (CSCed07253)
- If the ACL specified in the **ip multicast boundary *acl\_name* filter-autorp** command has non-wildcard entries, the filter-autorp functionality does not work. This problem is resolved in Release 12.2(18)SXD. (CSCed02952)
- Directly connected multicast enabled subnets might not be programmed correctly on the PFC. This problem is resolved in Release 12.2(18)SXD. (CSCed00394)
- When protocol independent multicast (PIM) dense mode is enabled, an interface in the outgoing interface list may indicate it is in forwarding mode, but the P flag may be set to the group (S,G) state, which prevents the interface from forwarding packets. This problem is resolved in Release 12.2(18)SXD. (CSCec70428)
- With bursty multicast sources on the network, a reload might occur because of a watchdog timeout if a nondefault holdtime value is received in a Protocol Independent Multicast (PIM) join message. The holdtime value might be nondefault because it is from a non-Cisco network device or because the Internet Group Management Protocol (IGMP) query interval has been modified on an interface. This problem is resolved in Release 12.2(18)SXD. (CSCec70366)
- When an interface that is configured with multiple IP multicast helper maps for the same group address and for different broadcast addresses is removed, it generates false memory-access errors. If the interface is reconfigured and removed again, the router will crash. This problem is resolved in Release 12.2(18)SXD. (CSCec63186)
- An IGMP packet flood might cause a reload. This problem is resolved in Release 12.2(18)SXD. (CSCec39132)
- A reload might occur if you enter the **interface loopback *interface\_number*** interface configuration command and the value of the *interface\_number* argument is a 9-digit number that starts with 10. This problem is resolved in Release 12.2(18)SXD. (CSCec03907)
- A reload might occur if you configure a Frame Relay SVC with a data-link connection identifier (DLCI) that is already in use. This problem is resolved in Release 12.2(18)SXD. (CSCea43177)

- In a topology where MAC addresses move frequently (for example, as the result of wireless access through various access points) and where there are STP topology change notices (TCNs), EtherChannels with interfaces on different DFC-equipped switching modules might drop traffic. This problem is resolved in Release 12.2(18)SXD. (CSCee83733)
- A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. See the Security Advisory for a complete list of affected release trains.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>.

This problem is resolved in Release 12.2(18)SXD. (CSCec16481)

- All ingress IPv6 traffic on an IPv4 VRF-enabled interface is routed in software on the MSFC3. This problem is resolved in Release 12.2(18)SXD. (CSCed02778, CSCec03707)
- Occasionally, CEF mistakes the state of an active interface and does not forward traffic to what it sees as an inactive interface. This problem is resolved in Release 12.2(18)SXD. (CSCdt38401)
- You cannot disable the power reserved for empty slots. This problem is resolved in Release 12.2(18)SXD: you can enter the **no power enable module** command for an empty slot. (CSCed56651)
- In releases where caveat CSCdy36604 is resolved, you cannot use SNMP to retrieve dot1dBase group data on VLANs where the spanning tree protocol is not enabled. This problem is resolved in Release 12.2(18)SXD. (CSCee39798)
- Ignore spurious memory access errors during an SSO switchover. This problem is resolved in Release 12.2(18)SXD. (CSCee30050, CSCed76955, CSCee10728, CSCee32558)
- If you configure an IPv6 address on an interface and exit the configuration mode, and then configure an IPv4 address on the interface, IP traffic is not Layer 3 switched in hardware. This problem is resolved in Release 12.2(18)SXD. (CSCed46165)
- You might see the following message on a redundant supervisor engine:

```
SM-SP-STDBY-4-BADEVENT:
Event 'bundle_sync' is invalid for the current state 'COLLECTING_DISTRIBUTING':
traceback= 40306D5C 404975E8 40499DBC 4048E65C 408EB04C 406CC9DC 406C7F1C
```

This problem is resolved in Release 12.2(18)SXD. (CSCed20448)

- The output of the **show mls qos ip port** command displays two policies attached to the port when only one is attached. This problem is resolved in Release 12.2(18)SXD. (CSCed16185)
- If you enter a **no mpls ip** or **no ip addr** interface command, and then enter an **interface range** command, ignore any “const\_mpls\_dec\_mpls\_use: error - zero mpls\_use\_count” messages. This problem is resolved in Release 12.2(18)SXD. (CSCeb64700)
- These objects in SWITCH-ENGINE-MIB return inaccurate values:
  - cseFlowMcastResultDstVlans
  - cseFlowMcastResultDstVlans2k

- cseFlowMcastResultDstVlans3k
- cseFlowMcastResultDstVlans4k

This problem is resolved in Release 12.2(18)SXD. (CSCed14797)

- With IGMP snooping enabled, and some IGMPv3 groups that have many sources, you might see messages about high CPU usage if you enter the **clear ip igmp snooping statistics** command. This problem is resolved in Release 12.2(18)SXD. (CSCed30453)
- Multicast subnet entries are not removed when you disable Protocol Independent Multicast (PIM) on an interface. The stale subnet entries remain programmed in hardware. The forwarding of multicast packets is not affected because the entries are used only for bridging. This problem is resolved in Release 12.2(18)SXD. (CSCed28813)

- When booting, you might see the following message:

```
%C6K_PROCMIB-SP-3-IPC_PORTOPEN_FAIL: Failed to open port while connecting to process
statistics: error code = no such port
-Traceback= 4071AD28 4071AE34
```

This problem is resolved in Release 12.2(18)SXD. (CSCed12970)

- In releases where CSCeb80453 is resolved, the order-dependent ACL merge (ODM) algorithm does not support the Cisco IOS Firewall Authentication Proxy feature. This problem is resolved in Release 12.2(18)SXD. (CSCin72202)
- The **logging snmp-authfail** command is enabled by default. This problem is resolved in Release 12.2(18)SXD. (CSCeb71693)
- The Egress Multicast Replication feature assumes that there is a supervisor engine in slot 1, which can be invalid for a Supervisor Engine 720. If a port on a module in slot 1 is a member of a multicast group, this problem sends multicast traffic to a Supervisor Engine 720 when the Supervisor Engine 720 uplink ports are not members of the multicast group. This problem is resolved in Release 12.2(18)SXD. (CSCee40846)

## FlexWAN Module Caveats in Release 12.2(18)SXD and Rebuilds

- [Open FlexWAN Module Caveats in Release 12.2\(18\)SXD7a, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD7a, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD7, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD6, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD5, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD5, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD4, page 358](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD3, page 359](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD2, page 359](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD1, page 359](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(18\)SXD, page 360](#)

## Open FlexWAN Module Caveats in Release 12.2(18)SXD7a

- Under a high traffic load, a [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) port adapter might display an increasing rx\_no\_buffer counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter might stop receiving traffic.

**Workaround:** Enter the **shutdown** and **no shutdown** interface configuration commands on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter or reset the FlexWAN module. This problem is resolved in Release 12.2(18)SXE. (CSCin77553)

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD7a

None.

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD7

None.

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD6

None.

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD5

None.

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD5

- A memory leak and reload might occur if you configure many subinterfaces on an Enhanced FlexWAN module. This problem is resolved in Release 12.2(18)SXD5. (CSCsa88102)

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD4

- When you send larger than fragment-sized packets from a multilink interface that has a traffic-shaping class configured and that is configured for fragmentation, traffic loss occurs when the queue size increases to the queue limit. This problem is resolved in Release 12.2(18)SXD4. (CSCef66517)
- With an Enhanced FlexWAN module, you might see “Hyperion Transmit packet header crc error” messages. This problem is resolved in Release 12.2(18)SXD4. (CSCin87976)
- After a reload, a FlexWAN module [PA-POS-2OC3](#) POS interface might be incorrectly reported as administratively up/up. This problem is resolved in Release 12.2(18)SXD4. (CSCeg67986)
- A hardware problem on an ATM [PA-A3](#) port adapter might cause the port adapter to reload or freeze. This problem is resolved in Release 12.2(18)SXD4. (CSCin84694)
- On an ATM [PA-A3](#) port adapter, when a virtual circuit (VC) class that is configured for create on-demand is attached to the physical ATM interface and then the create on-demand configuration is removed and reapplied to the VC class, auto provisioning might get disabled. This problem is resolved in Release 12.2(18)SXD4. (CSCin86455)

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD3

- When you modify the configuration of a serial interface, you might see messages similar to these:

```
%INTERFACE_API-3-NODESTROYSUBBLOCK: The HWIDB subblock named COPS_PR was not removed
-Traceback=
```

This problem is resolved in Release 12.2(18)SXD3. (CSCin65698)

- In releases where caveat CSCec15517 is resolved, permanent virtual circuits (PVCs) might be unstable. This problem is resolved in Release 12.2(18)SXD3. (CSCee22810)
- With a [PA-MC-8TE1+](#) or [PA-MC-8E1/120](#) port adapter, you might not be able to configure a Frame Relay class under “frame-relay interface-dlci.” This problem is resolved in Release 12.2(18)SXD3. (CSCef47829)
- The [PA-2T3+](#) port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.2(18)SXD3. (CSCee70591)
- The [PA-MC-2T3+](#) port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.2(18)SXD3. (CSCee49862)
- 1,500-byte pings fail on a [PA-A3](#) ATM subinterface configured for MPLS and configured with the **ip mtu 1500** command. This problem is resolved in Release 12.2(18)SXD3. (CSCef91994)

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD2

None.

## Resolved FlexWAN Module Caveats in Release 12.2(18)SXD1

- With an Enhanced FlexWAN module, “EOS-RESET” messages might be followed by “HYPERION-RESET” messages. This problem is resolved in Release 12.2(18)SXD1. (CSCef25710)
- On an Enhanced FlexWAN module, an IP packet with an invalid “total length” field value (less than 19) can disrupt traffic for a few milliseconds. This problem is resolved in Release 12.2(18)SXD1. (CSCef60434)
- Packet-over-SONET (POS) Automatic Protection Switching (APS) does not work on [PA-MC-STM-1](#) port adapters. This problem is resolved in Release 12.2(18)SXD1. (CSCef49330)
- With a Supervisor Engine 2, you might see a “hardware TCAM entry capacity exceeded message” if you configure a security ACL and a policy route map on a FlexWAN module POS interface. This problem is resolved in Release 12.2(18)SXD1. (CSCef13797)
- Following a reload, an Enhanced FlexWAN module might not boot. This problem is resolved in Release 12.2(18)SXD1. (CSCef02439)
- A response time reporter (RTR) probe does not report input or output packets for serial interfaces of [PA-MC-8T1](#), [PA-MC-8E1/120](#), and [PA-MC-8TE1+](#) port adapters. This problem is resolved in Release 12.2(18)SXD1. (CSCee82681)
- A FlexWAN module might reload if you reuse a channel group that was previously configured with a Frame Relay data-link connection identifier (DLCI) “set” service policy. This problem is resolved in Release 12.2(18)SXD1. (CSCee36050)



- With multiple link point-to-point protocol (MLPPP) configured on a [PA-A3](#) ATM port adapter that has a 128-Kbps permanent virtual circuit (PVC) and class-based weighted fair queueing (CBWFQ) configured on the virtual template interface and the distributed link fragmentation and interleaving (dLFI) fragment delay configured to 13 microseconds or less, you might see ATM BADVCD messages and some MLPPP fragment loss. This problem is resolved in Release 12.2(18)SXD1. (CSCef44786)
- When other modules have large configurations, an E1 controller on a [PA-MC-8TE1+](#) port adapter might not be active following a reload. This problem is resolved in Release 12.2(18)SXD1. (CSCin78110)
- With a WS-X6582-2PA Enhanced FlexWAN module and PA-MC-4T1 or [PA-POS-OC3](#) port adapters, ignore any “MajFail Error” startup diagnostic messages. This problem is resolved in Release 12.2(18)SXD1. (CSCin76828, CSCef04875)
- With a PFC3, the **set mpls exp** command does not work in a service policy applied to ingress FlexWAN or Enhanced FlexWAN module interfaces. This problem is resolved in Release 12.2(18)SXD1. (CSCee44637)

### Resolved FlexWAN Module Caveats in Release 12.2(18)SXD

- On FlexWAN module ATM interfaces and subinterfaces, service policies applied to a virtual template do not take effect. This problem is resolved in Release 12.2(18)SXD. (CSCed58116, CSCee94391)
- On FlexWAN module ATM interfaces and subinterfaces, service policies applied to a virtual template do not take effect. This problem is resolved in Release 12.2(18)SXD. (CSCed58116, CSCee94391)
- An administratively shut-down subinterface that is configured for Frame-Relay encapsulation might forward packets. This problem is resolved in Release 12.2(18)SXD. (CSCed78803)
- With multilink PPP configured, fragmentation might cause spurious accesses and tracebacks. This problem is resolved in Release 12.2(18)SXD. (CSCed65436)
- You might see CWAN\_RP-3-SEMAHOG messages and tracebacks or CMDTIMEOUT messages and tracebacks. This problem is resolved in Release 12.2(18)SXD. (CSCin54713)
- VACL capture does not support PPP multilinks on the FlexWAN module. This problem is resolved in Release 12.2(18)SXD. (CSCee07996)
- With QoS configured on FlexWAN ports, spurious memory accesses and alignment errors might occur. This problem is resolved in Release 12.2(18)SXD. (CSCed69233)
- With a FlexWAN module, following a reload, you might see erroneous OIR-6-REMCARD messages and the FlexWAN module might reset. This problem is resolved for Frame-Relay interfaces in Release 12.2(18)SXD. (CSCed53595)
- The FlexWAN module may reload when it is booting up. This problem is resolved in Release 12.2(18)SXD. (CSCec55445)
- A 1-port E3 serial port adapter ([PA-E3](#)) might fail to recover to the up/up state even when the original cause of the failure is corrected. This problem is resolved in Release 12.2(18)SXD. (CSCec33028)
- [OSM-2+4GE-WAN+](#) ports do not automatically adjust the MTU size to accommodate tagged traffic. Ingress tagged packets destined for the MSFC are dropped if the packet size is larger than the ingress interface MTU size. This problem is resolved in Release 12.2(18)SXD. (CSCee59667)
- Following a reload, modular QoS CLI (MQC) MPLS CoS classification does not work. This problem is resolved in Release 12.2(18)SXD. (CSCed35900)



## Service Module Caveats in Release 12.2(18)SXD and Rebuilds

- [Open Service Module Caveats in Release 12.2\(18\)SXD7a, page 361](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD7a, page 361](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD7, page 361](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD6, page 362](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD5, page 362](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD4, page 362](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD3, page 363](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD2, page 364](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD1, page 364](#)
- [Resolved Service Module Caveats in Release 12.2\(18\)SXD, page 365](#)

### Open Service Module Caveats in Release 12.2(18)SXD7a

- With an IPsec VPN Acceleration Services Module, if you change the ACL name in a **match address** *acl\_name* crypto-map command, the crypto-map is removed from the VPN module and is not sent to the VPN module with the new name.

**Workaround:** Reset the VPN module. This problem is resolved in Release 12.2(18)SXE. (CSCef77822)

- With an IPsec VPN Acceleration Services Module, following a switchover to a redundant supervisor engine under heavy traffic conditions, traffic might stop flowing through IPsec and GRE IPsec tunnels that are configured for tunnel protection.

**Workaround:** Reset the VPN module. This problem is resolved in Release 12.2(18)SXE. (CSCef75411)

- With an IPsec VPN Acceleration Services Module, a memory leak might occur when thousands of VPN clients are connecting and disconnecting at the same time. (CSCee25454)

### Resolved Service Module Caveats in Release 12.2(18)SXD7a

- You might be unable to access an Multi-Processor WAN Application Module (MWAM) through a console or Telnet session for 10 minutes after the module has been reloaded.

**Workaround:** Configure the **ip rcmd rcp-enabled** command.

This problem is resolved in Release 12.2(18)SXD7a. (CSCsa50215)

### Resolved Service Module Caveats in Release 12.2(18)SXD7

- If a service module goes down, the module sends a message to the supervisor engine requesting an image download so that it can reinitialize. The supervisor engine ignores the message, does not notice that the service module is down for 180 seconds, and then downloads the image. This problem is resolved in Release 12.2(18)SXD7. (CSCei37672)
- With a VPN Service Module (VPN-SM/WS-SVC-IPSEC-1) installed, large packet drops might occur when you configure the **ip mtu** command on a GRE IPsec tunnel interface. This problem is resolved in Release 12.2(18)SXD7. (CSCsb12076)

- With a Supervisor Engine 720, a Cisco Multiprocessor WAN Application Module (MWAM) might experience connectivity problems if there are any Layer 2 [distributed EtherChannels \(DECs\)](#) configured. This problem is resolved in Release 12.2(18)SXD7 (CSCsb50559)

### Resolved Service Module Caveats in Release 12.2(18)SXD6

None.

### Resolved Service Module Caveats in Release 12.2(18)SXD5

- When configured with a standby Content Switching Module ([CSM](#)), a bus error exception and a reload might occur if there is an SNMP request for the Cisco IOS SLB MIB for the standby CSM and the **hw-module csm slot\_num standby config-sync** command is entered on the active CSM. This problem is resolved in Release 12.2(18)SXD5. (CSCsa74464)
- When the [CSM](#) Cisco IOS SLB mode is “RP”, a reload might occur if you enter the **ip slb mode csm** command and then enter the **show running-config** command. This problem is resolved in Release 12.2(18)SXD5. (CSCef93632)
- The traffic counters displayed by the show interfaces tunnel command are incorrect for GRE IPsec tunnels on the IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)). This problem is resolved in Release 12.2(18)SXD5. (CSCef56578)
- With public key infrastructure (PKI) and Internet Key Management Protocol (IKMP) configured, a memory leak might occur. This problem is resolved in Release 12.2(18)SXD5. (CSCec22308)
- With a Rivest, Shamir, and Adelman signature (RSA-SIG) and Internet Key Management Protocol (IKMP) configured, a memory leak might occur. This problem is resolved in Release 12.2(18)SXD5. (CSCec32184)
- With a Supervisor Engine 720, service modules might experience connectivity problems if there are any Layer 2 EtherChannels configured with member ports on different DFC-equipped switching modules. With a Supervisor Engine 720 in bus fabric switching mode, service modules might experience connectivity problems if there are any Layer 2 EtherChannels. This problem is resolved in Release 12.2(18)SXD5. (CSCee10005)



#### Note

With Release 12.2(18)SXD5 and rebuilds, you can use the **fabric switching-mode force bus-mode** command to avoid the bus fabric switching mode. See the Release 12.2SX command reference for more information.

### Resolved Service Module Caveats in Release 12.2(18)SXD4

- SNMP traps are sent for every Internet Key Exchange (IKE) timeout and rekey but not for every IPsec timeout and rekey. This situation might generate many false alerts that an IKE tunnel is down when the IKE tunnel is torn down but immediately rebuilt. Releases where CSCee91044 is resolved do not send SNMP traps for normal IKE operation. This problem is resolved in Release 12.2(18)SXD4. (CSCee91044)
- The trunk connection to a [WS-X6066-SLB-APC](#) Content Switching Module (CSM) carries VLANs that are not used by the CSM. This problem is resolved in Release 12.2(18)SXD4. (CSCeg41623)
- With at least one security association (SA) established, if you retrieve the IPsec IKE SNMP variables once every 10 minutes, a reload occurs after a few hours. This problem is resolved in Release 12.2(18)SXD4. (CSCdz54403)

- With a large number of IPsec tunnels terminated, a reload might occur if you poll the IKE MIB variables. This problem is resolved in Release 12.2(18)SXD4. (CSCed11835)
- With auto-reconnect configured on an EzVPN server, authentication, authorization, and accounting (AAA) failures might occur when an EzVPN client attempts to connect. This problem is resolved in Release 12.2(18)SXD4. (CSCee59999)
- When two sites initiate security associations (SAs) at the same time, a memory leak might occur in the Crypto IKMP process. This problem is resolved in Release 12.2(18)SXD4. (CSCee67261)
- When you delete a Content Services Gateway (CSG) module billing plan, you might see a “Failed to Delete Billing Plan” message when the deletion is successful. This problem is resolved in Release 12.2(18)SXD4. (CSCef82884)
- You can configure CSG policies with names that are 15 characters long, but you cannot assign the policies successfully to the CSG. This problem is resolved in Release 12.2(18)SXD4. (CSCef92360)
- When a VPN client session is terminated abnormally, the username might not be properly removed from the AAA user database and subsequent user logins might be rejected. This problem is resolved in Release 12.2(18)SXD4. (CSCeg77040)

### Resolved Service Module Caveats in Release 12.2(18)SXD3

- A Supervisor Engine 2 resets with a Traffic Anomaly Detector module or an Anomaly Guard module installed in the chassis. This problem is resolved in Release 12.2(18)SXD3. (CSCeg31792)
- With the Easy VPN server feature configured on an IPsec VPN Acceleration Services Module that terminates VPN client sessions, a memory leak might occur in the processor memory pool. This can be identified by an increasing amount of memory held by the Crypto IKMP process in the show process memory output. This problem is resolved in Release 12.2(18)SXD3. (CSCsa40962)
- If you configure more than one pair of accounting services and user-groups in a system with a Content Services Gateway module installed and then take one of the accounting services out of service using the **no inservice** command, the quota servers and BMAs for all the accounting services configured go out of service. This problem is resolved in Release 12.2(18)SXD3. (CSCeg43854)
- In a system with a Wireless LAN Service module, wireless client applications may lose connectivity due to MTU and fragmentation issues. This problem is resolved in Release 12.2(18)SXD3. (CSCeg26382)
- When an IPsec VPN Acceleration Services Module (VPN module) is configured to authenticate users with RADIUS, and the module cannot connect to the RADIUS server, a reload might occur with an “Unexpected Exception” error when trying to authenticate a user. This problem is resolved in Release 12.2(18)SXD3. (CSCed45971)
- With a VPN module, you might see “SYS-2-FREEBAD” or “ALIGN-1-FATAL” messages followed by a reload. This problem is resolved in Release 12.2(18)SXD3. (CSCeg41762)
- Setting the do not fragment (DF) bit disables VPN module-to-VPN module switchover. After the DF bit is set, these features might not work on the active VPN module:
  - IPsec security association (SA) expiry
  - Dead peer detection (DPD)
  - Idle timeout
 (CSCeg22198)
- The Cisco Discovery Protocol (CDP) does not recognize [WS-SVC-MWAM-1](#) service modules. This problem is resolved in Release 12.2(18)SXD3. (CSCin83554)

- With a dynamic crypto map configured, a reload might occur when you enter the **clear crypto sa peer** command while traffic is flowing through the tunnel. This problem is resolved in Release 12.2(18)SXD3. (CSCec00930)
- A reload might occur if you enter the **mls ip ids acl\_name** command. This problem is resolved in Release 12.2(18)SXD3. (CSCef53290)
- If you reset a [WS-X6066-SLB-APC](#) Content Switching Module (CSM), other modules might also reset. This problem is resolved in Release 12.2(18)SXD3. (CSCed25505)

## Resolved Service Module Caveats in Release 12.2(18)SXD2

- On a Content Services Gateway (CSG) module, when there are no client or server VLANs configured in the “ContentServicesGateway” configuration mode, if the addition of a ruleset fails, the configuration mode might change to a Content Switching Module (CSM) configuration mode. This problem is resolved in Release 12.2(18)SXD2. (CSCef70677)

## Resolved Service Module Caveats in Release 12.2(18)SXD1

- An IPsec VPN Acceleration Services Module configured for GRE over IPsec might stop passing traffic through the GRE tunnels. This problem is resolved in Release 12.2(18)SXD1. (CSCef65827)
- With Release 12.2(18)SXD, the **no nat server** command is not supported with CSM software version 3.3. This problem is resolved in Release 12.2(18)SXD1. (CSCef72233)
- On a POS OSM, if you remove and reconfigure a Frame Relay subinterface, you might see “CWTLC-3-FR\_CHANGEDLCI” messages and the subinterface might drop traffic. This problem is resolved in Release 12.2(18)SXD1. (CSCee54446)
- An IPsec VPN Acceleration Services Module might reload if you use an ACL that has only “any any” statements in all ACEs in a class map that provides filtering for IPsec traffic. This problem is resolved in Release 12.2(18)SXD1. (CSCef65249)
- With an IPsec VPN Acceleration Services Module and a Supervisor Engine 2, when you configure a GRE-over-IPsec tunnel, any already configured GRE-over-IPsec tunnels stop receiving traffic. This problem is resolved in Release 12.2(18)SXD1. (CSCef52858)
- With an IPsec VPN Acceleration Services Module and a Supervisor Engine 720, occasionally a reload might occur. This problem is resolved in Release 12.2(18)SXD1. (CSCef49811)
- With an IPsec VPN Acceleration Services Module and IPsec configured, any of these conditions might cause a reload:
  - A large number of IPsec tunnels (for example, more than 1,000)
  - A high volume of IPsec traffic with a short IPsec security association (SA) lifetime
  - High CPU load caused by SA creation, SA deletion, or IPsec MIB statistics collection
 This problem is resolved in Release 12.2(18)SXD1. (CSCef26926)
- With an IPsec VPN Acceleration Services Module, a reload might occur if you configure an IPsec tunnel when there is already a large number of IPsec tunnels (for example, 4,000) in use. This problem is resolved in Release 12.2(18)SXD1. (CSCee93511)
- Following an SSO switchover, a [WS-SVC-IDSM2-K9](#) Intrusion Detection System Module 2 might not detect attacks. This problem is resolved in Release 12.2(18)SXD1. (CSCef14106)
- Two systems equipped with IPsec VPN Acceleration services modules running as active and standby both advertise static routes if running routing protocols. If the standby module is picked as the best path, the traffic routed to it is not deliverable because there are no IPsec tunnels established on it.

This problem exists in VRF mode only and on systems with VPN Service Modules in a Hot Standby Router Protocol (HSRP) Stateless High Availability (HA) topology with static crypto maps. This problem is resolved in Release 12.2(18)SXD1. (CSCef79411)

### Resolved Service Module Caveats in Release 12.2(18)SXD

- Some loss might occur in traffic from a service module that crosses the switch fabric. This problem is resolved in Release 12.2(18)SXD. (CSCee68381)
- If a CSM serverfarm is configured with a real server name instead of a real server IP address, SNMP does not retrieve and display the IP address of the real server in the CISCO-SLB-MIB server table. This problem is resolved in Release 12.2(18)SXD. (CSCed84042)
- If you add VLANs 1002-1005 to the allowed VLAN list for an SSL module, the SSL module might have a connectivity problem. This problem is resolved in Release 12.2(18)SXD. (CSCec60933)

### OSM Caveats in Release 12.2(18)SXD and Rebuilds

- [Open OSM Caveats in Release 12.2\(18\)SXD7a, page 365](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD7a, page 365](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD7, page 365](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD6, page 366](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD5, page 366](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD4, page 366](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD3, page 366](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD2, page 367](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD1, page 367](#)
- [Resolved OSM Caveats in Release 12.2\(18\)SXD, page 368](#)

### Open OSM Caveats in Release 12.2(18)SXD7a

- If you enter the **encapsulation dot1q** *vlan\_id* command on an OSM Gigabit Ethernet WAN port with the VLAN ID of an internal VLAN, the port does not forward traffic.  
**Workaround:** Enter the ID of an unused VLAN. This problem is resolved in Release 12.2(18)SXE. (CSCef08790)
- Changing the MTU size on a port might not change the MPLS MTU size.  
**Workaround:** Enter the **shutdown** and **no shutdown** commands after configuring an MTU size on a port. This problem is resolved in Release 12.2(18)SXE. (CSCed17226, CSCed33822)

### Resolved OSM Caveats in Release 12.2(18)SXD7a

None.

### Resolved OSM Caveats in Release 12.2(18)SXD7

None.

## Resolved OSM Caveats in Release 12.2(18)SXD6

None.

## Resolved OSM Caveats in Release 12.2(18)SXD5

- The Virtual Container 12 (VC-12) RFI bit is undefined in the International Telecommunication Union (ITU) G.707/Y.1322 standard. Instead of ignoring the VC-12 RFI bit, an [OSM-1CHOC12/T1-SI](#) reports a Remote Fault Indication (RFI) for VC-12 and shuts down its E1 interfaces if it is connected to a synchronous digital hierarchy (SDH) switch that has the VC-12 RFI bit set. This problem is resolved in Release 12.2(18)SXD5. (CSCsa85123)
- Disposition packets that are index-directed from a core-facing OSM are not passed to a CE-facing channelized OSM. This problem is resolved in Release 12.2(18)SXD5. (CSCeh29617)
- Egress OSM port policing might drop ISIS routing control packets. This problem is resolved in Release 12.2(18)SXD5. (CSCeg49010)

## Resolved OSM Caveats in Release 12.2(18)SXD4

- With OSM serial interfaces configured, you might see these messages:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 65535
-Process= "<interrupt level>", ipl= 1
-Traceback= 4021F160 402E3BCC 40E9CA28 40E90E68 402D545C 40294A0C
```

This problem is resolved in Release 12.2(18)SXD4. (CSCed82736)

- Some VPLS VCs fail to pass traffic after a link failure in the core network. This problem is resolved in Release 12.2(18)SXD4. (CSCeg16684)
- When the VLAN interfaces are unstable at both ends of a Virtual Private LAN Service (VPLS) virtual circuit (VC), both ends try to reinitialize the VPLS VC. The initialization attempts conflict and prevent reestablishment of the VPLS VC. This problem is resolved in Release 12.2(18)SXD4. (CSCeg30437)
- Some OSM virtual circuits (VCs) might not pass any traffic following switchover to a redundant Supervisor Engine 2. This problem is resolved in Release 12.2(18)SXD4. (CSCeg40543)
- Traffic loss might occur if you configure more than one RFC1483 bridging-enabled permanent virtual circuit (PVC) on an [OSM-2OC12-ATM](#). This problem is resolved in Release 12.2(18)SXD4. (CSCeg47780)
- Port 1/7 ingress traffic is dropped if the egress port is on an OSM. This problem is resolved in Release 12.2(18)SXD4. (CSCeh05310)

## Resolved OSM Caveats in Release 12.2(18)SXD3

- Following a supervisor engine reset, a Gigabit Ethernet WAN module resets and the 802.1q interfaces reregister. In this situation, all configured subinterfaces fail to reregister with the Interface MIB. This problem is resolved in Release 12.2(18)SXD3. (CSCef82720)
- An OSM might not report the default QoS class statistics if the default class is not explicitly configured. This problem is resolved in Release 12.2(18)SXD3. (CSCef79592)
- When configured as an 802.1q trunk port, the Layer 2 LAN ports on OSMs do not allow for the 802.1q tag when counting packets as giants. This problem is resolved in Release 12.2(18)SXD3. (CSCef74227)



- For a GE-WAN interface priority queue, you cannot add additional match criteria to a class map that is configured with the **match mpls** command. This problem is resolved in Release 12.2(18)SXD3. (CSCeg24675)
- For an OSM WAN interface priority queue, you cannot add additional match criteria to a class map that is configured with the **match mpls** command. This problem is resolved in Release 12.2(18)SXD3. (CSCeg24675)
- When deleting and recreating channels on an [OSM-12CT3/T1](#) T1 interface, the SNMP ifindex disappears. This problem is resolved in Release 12.2(18)SXD3. (CSCef70298)
- With an OSM, you might see these messages:

```
%EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR: EARL L2 ASIC #0: L2L3 Mismatch seq #0x1306
%EARL_L2_ASIC-SP-3-INTR_WARN: EARL L2 ASIC 0: Non-fatal interrupt l2l3_seq_mismatch
%CWTLC-3-MEDUSA_FATAL: OSM Medusa ASIC Fatal Error. ERROR CODE: 3, 62,
```

This problem is resolved in Release 12.2(18)SXD3. (CSCeg03144)

- When any interface on an [OSM-12CT3/T1](#) goes down, traffic to a directly connected router might experience high latency. This problem is resolved in Release 12.2(18)SXD3. (CSCef47466)
- If you configure 802.1Q tunneling on a LAN port and 802.1Q-tunnel bridging on an [OSM-2OC12-ATM-SI+](#) subinterface, the OSM might reload. This problem is resolved in Release 12.2(18)SXD3. (CSCef35398)
- The serial interface input and output counters for an OSM always show 0 when you enter the **show interfaces serial** command. This problem is resolved in Release 12.2(18)SXD3. (CSCed07367)

#### Resolved OSM Caveats in Release 12.2(18)SXD2

- A GE-WAN subinterface configured for MPLS might stop forwarding traffic. This problem is resolved in Release 12.2(18)SXD2. (CSCef72205)

#### Resolved OSM Caveats in Release 12.2(18)SXD1

- A Content Switching Module ([CSM](#)) reloads when you enter a **redirect-vserver REDIR1** command to remove a server farm that has a redirect-vserver entry that has a web host backup configured. The CSM first executes a **no redirect-vserver REDIR1** command and then resets. This problem is resolved in Release 12.2(18)SXD1. (CSCef47639)

- After frequent optical service module (OSM) online OIRs, you might see the following error message and a reload of the OSM.

```
%FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error for channel 10
(Module 4, fabric connection 0)
```

This problem is resolved in Release 12.2(18)SXD1. (CSCef12193)

- For 64-byte Frame Relay over MPLS (FRoMPLS) payloads, OSMs do not include the length of the control word (4 bytes) in the payload length calculation. If the disposition interface is not on an OSM, the packets are truncated by 4 bytes. This problem is resolved in Release 12.2(18)SXD1. (CSCef83690)
- On OSMs, padded Frame Relay over MPLS (FRoMPLS) packets are truncated because the pad length is calculated incorrectly. This problem is resolved in Release 12.2(18)SXD1. (CSCef63516)
- With an ATM OSM providing the core-facing interfaces for both ATM Adaptation Layer 5 over MPLS (AAL5oMPLS) and Cell Relay over MPLS (CRoMPLS) tunnels, if you enter the loopback line interface configuration command, the tunnels are disabled. This problem is resolved in Release 12.2(12)SXD1. (CSCed19898)

- Reloads might not be successful with a large number (for example, 500) of subinterfaces configured on a GE-WAN port. This problem is resolved in Release 12.2(12(18)SXD1. (CSCee42657)

## Resolved OSM Caveats in Release 12.2(18)SXD

- There is no customer-edge (CE) router to provider-edge (PE) router connectivity if you configure a multiple link point-to-point protocol (MLPPP) interface on an [OSM-12CT3/T1](#) or [OSM-1CHOC12/T1-SI](#) in the CE-PE link. This problem is resolved in Release 12.2(18)SXD. (CSCef19811)
- Hierarchical service policies do not work correctly on physical interfaces configured for Frame Relay encapsulation when sub-interfaces are also configured. This problem is resolved in Release 12.2(18)SXD. (CSCee38898)
- [OSM-1CHOC12/T1-SI](#) T1 interfaces that have path coding violations (PCVs) might cause erroneous Layer 1 errors to be displayed for other T1 interfaces. This problem is resolved in Release 12.2(18)SXD. (CSCed86486)
- VRF ping packets are counted by the input counters for OSM physical interfaces, but not by the sub-interface input counters. This problem is resolved in Release 12.2(18)SXD. (CSCea74537)
- A reload might occur if you enter a **show controllers sonet** command with an invalid number for a T1 interface on a [OSM-1CHOC12/T1-SI](#) or [OSM-12CT3/T1](#) module. This problem is resolved in Release 12.2(18)SXD. (CSCee50911)
- [OSM-1CHOC12](#) modules become unresponsive and are power cycled. This problem is resolved in Release 12.2(18)SXD. (CSCee45508)
- An [OSM-12CT3/T1](#) module configured with an E1 channel group is powered down. This problem is resolved in Release 12.2(18)SXD. (CSCee42278)
- An E3 serial interface on an [OSM-1CHOC12/T3-SI](#) module might be inactive after you enter **shutdown** and **no shutdown** commands. This problem is resolved in Release 12.2(18)SXD. (CSCed92724)
- An OC-12 POS OSM might reset as a result of memory corruption. This problem is resolved in Release 12.2(18)SXD. (CSCec59550)
- The 64-bit counter on the [OSM-2+4GE-WAN+](#) main interface shows an incorrect value of zero. This problem is resolved in Release 12.2(18)SXD. (CSCec34010)
- Traffic loss might occur on OSMs when there are frequent online insertion and removals (OIRs). This problem is resolved in Release 12.2(18)SXD. (CSCee54642)
- OSM interface byte counts might be incorrect after a few hours of traffic handling. High traffic levels on OC-48 interfaces might produce incorrect byte counts. This problem is resolved in Release 12.2(18)SXD. (CSCee55056)

## Caveats in Release 12.2(17d)SXB and Rebuilds

- [General Caveats in Release 12.2\(17d\)SXB and Rebuilds, page 369](#)
- [FlexWAN Module Caveats in Release 12.2\(17d\)SXB and Rebuilds, page 397](#)
- [Service Module Caveats in Release 12.2\(17d\)SXB and Rebuilds, page 402](#)
- [OSM Caveats in Release 12.2\(17d\)SXB and Rebuilds, page 405](#)



**Note**

Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with Part No. 800-24557-01, as described in this external field notice (CSCee47030):

<http://www.cisco.com/warp/public/770/fn29736.shtml>

## General Caveats in Release 12.2(17d)SXB and Rebuilds

- [Open General Caveats in Release 12.2\(17d\)SXB11a, page 369](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB11a, page 370](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB11, page 370](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB10, page 371](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB9, page 371](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB8, page 376](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB7, page 377](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB6, page 379](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB5, page 381](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB4, page 384](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB3, page 385](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB2, page 386](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB1, page 389](#)
- [Resolved General Caveats in Release 12.2\(17d\)SXB, page 392](#)

### Open General Caveats in Release 12.2(17d)SXB11a

- Ignore spurious memory access errors during an SSO switchover. This problem is resolved in Release 12.2(18)SXD. (CSCee30050, CSCed76955, CSCee10728, CSCee32558)
- These objects in SWITCH-ENGINE-MIB return inaccurate values:
  - cseFlowMcastResultDstVlans
  - cseFlowMcastResultDstVlans2k
  - cseFlowMcastResultDstVlans3k
  - cseFlowMcastResultDstVlans4k

This problem is resolved in Release 12.2(18)SXD. (CSCed14797)
- EtherChannels might stop transmitting traffic after an OIR of a [WS-X6148-GE-TX](#) switching module. (CSCee81056)

**Note**

CSCee81056 is not seen in later releases.

- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

### Resolved General Caveats in Release 12.2(17d)SXB11a

- Occasionally in an IGMP multicast configuration, the PFC or DFC FIFO stops processing, and this message is displayed:

```
EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
```

This problem is resolved in Release 12.2(17d)SXB11a. (CSCej21698)

- A reload might occur with a breakpoint exception (signal=5). This problem can occur in any release that contains the fix for CSCee28288 when a 32-bit counter continues to increment until it wraps around to 0. In most cases approximately 40 to 50 weeks of continuous uptime elapses before this problem is observed. This problem is resolved in Release 12.2(17d)SXB11a. (CSCsb98702)
- This DDTs documents changes in how Cisco IOS software handles packets destined to the router. This problem is resolved in Release 12.2(17d)SXB11a. (CSCek26492)

### Resolved General Caveats in Release 12.2(17d)SXB11

- A system that is configured with a large number of VPLS VCs that are going up and down might cause the egress interface to stop passing traffic. This situation might make OSPF and other protocols go down. This problem is resolved in Release 12.2(17d)SXB11. (CSCsb90602)
- Under rare conditions, a data structure in the ENTITY-MIB might get corrupted. Because the **show inventory** command uses this data structure to gather the information for display, the software can get stuck in an infinite loop when the data structure is corrupt, eventually followed by a stack overflow and reload. To avoid this problem, the output of the **show inventory** command has been removed from the output of the **show tech-support** command in Release 12.2(17d)SXB11. (CSCsc31677)

- WS-X67xx switching modules might reload with the following error messages:

```
PM_SCP-SP-1-LCP_FW_ERR: System resetting module <mod-no> to recover from error: [Log]
Rohini 3: packet buffer P2N EEC1
OIR-SP-3-PWRCYCLE: Card in module <mod-no>, is being power-cycled off (Module
experiencing Port asic error
C6KPWR-SP-4-DISABLED: power to module in slot <mod-no> set off (Module experiencing
Port asic error)
```

This problem is resolved in Release 12.2(17d)SXB11. (CSCej52641)

- Passwords and other sensitive information should not be sent to Access Control Server (ACS) logs. When command accounting is enabled, the full text of each command is sent to an ACS server. This information is sent to the server encrypted, but the server decrypts the packets and logs these commands in plain text. This problem is resolved in Release 12.2(17d)SXB11. (CSCed09685)
- The giants counter on WS-X67xx switching modules might increment for ports that are trunking. This situation does not affect performance. This problem is resolved in Release 12.2(17d)SXB11. (CSCef87392)

## Resolved General Caveats in Release 12.2(17d)SXB10

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

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

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

This problem is resolved in Release 12.2(17d)SXB10. (CSCei61732)

- Traffic that uses a Layer 2 port channel interface is software switched after that port channel is removed and recreated. This problem is resolved in Release 12.2(17d)SXB10. (CSCee56573)
- If you enter a **write memory** command, the module in the redundant supervisor engine slot reloads, and you might see one of the following messages:

```
CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 6 for software recovery, Reason: Failed
TestMacNotification
CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 6 for software recovery, Reason: Failed
TestFabricCh0Health
```

This problem occurs where there is either a redundant supervisor engine or a DFC-equipped module in the redundant supervisor engine slot. This problem is resolved in Release 12.2(17d)SXB10. (CSCeg29451)

## Resolved General Caveats in Release 12.2(17d)SXB9

- Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

This problem is resolved in Release 12.2(17d)SXB9. (CSCeh73049)

- Receipt of a Border Gateway Protocol (BGP) autonomous system (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh13489)
- Following an RPR+ switchover, the MLS long aging value is not synchronized to the redundant supervisor engine. This problem is resolved in Release 12.2(17d)SXB9. (CSCee32301, CSCsa68081)
- Subinterfaces on these ports do not provide hardware switching for IPv4 multicast traffic:
  - Ethernet1/1
  - FastEthernet1/1

- GigabitEthernet1/1
- TenGigabitEthernet1/1

This problem is resolved in Release 12.2(17d)SXB9. (CSCec77178, CSCed26629, CSCef91498)

- With a Supervisor Engine 720, if you enter the **mls ip cef load-sharing simple** command, traffic might be lost that uses MPLS adjacencies for routes that have a next hop that is reachable through an MPLS cloud. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa50071, CSCeg71317)
- While the output of the **show ip mroute vrf vrf\_name** command is being displayed in one administrative session, a reload might occur if you enter the **no ip vrf vrf\_name** command for the same VRF in another administrative session. This problem is resolved in Release 12.2(17d)SXB9. (CSCeg52076, CSCeg55595)
- With RPR+ redundancy mode configured, the supervisor engine might fail bootup diagnostics with an “AclPermit” test failure and a reload. This problem is resolved in Release 12.2(17d)SXB9. (CSCef20654)
- When the FIB TCAM is full, CPU utilization might be unacceptably high. This problem is resolved in Release 12.2(17d)SXB9. (CSCeb85827, CSCeb29888, CSCec14802, CSCec42634, CSCed58661, CSCee00311, CSCee22821, CSCin77977, CSCin78030, CSCin80590)
- After a reload of a Supervisor Engine 2 with DFC-equipped switching modules, Gateway Load Balancing Protocol (GLBP) traffic might be routed in software on the MSFC2, because the GLBP virtual MAC address might not be enabled. This problem is resolved in Release 12.2(17d)SXB9. (CSCee70075)
- RFC 1889 Compressed Real-Time Protocol (cRTP) does not work with CEF enabled on FlexWAN modules. This problem is resolved in Release 12.2(17d)SXB9. (CSCee85257)
- Ignore spurious memory access errors during an SSO switchover. This problem is resolved in Release 12.2(17d)SXB9. (CSCed64648, CSCeb55269, CSCed44945, CSCed47559, CSCed50801, CSCed51914, CSCed64843, CSCed80188, CSCed88244, CSCee10565, CSCee19150, CSCee32558, CSCee42141, CSCee56069, CSCee59872, CSCin70853, CSCin72244)
- With a PFC3, on Layer 3 interfaces that are configured to support IPX routing, but which are not configured with an IP address, the **mls rate-limit** commands incorrectly limit IPX traffic.

**Workaround:** Configure an IP address on Layer 3 interfaces that are configured to support IPX routing. Use an IP address to which IP routing does not send any traffic. Configure an IP access list to drop IP ingress traffic. This problem is resolved in Release 12.2(17d)SXB9. (CSCee09692)

- If you configure an IPv6 address on an interface and exit configuration mode, and then configure an IPv4 address on the interface, IP traffic is not Layer 3 switched in hardware.

**Workaround:** Configure both IPv6 and IPv4 addresses in the same configuration session. This problem is resolved in Release 12.2(17d)SXB9. (CSCed46165)

- You might see the following message on a redundant supervisor engine:

```
SM-SP-STDBY-4-BADEVENT:
Event 'bundle_sync' is invalid for the current state 'COLLECTING_DISTRIBUTING':
traceback= 40306D5C 404975E8 40499DBC 4048E65C 408EB04C 406CC9DC 406C7F1C
```

This problem is resolved in Release 12.2(17d)SXB9. (CSCed20448)

- The output of the **show mls qos ip port** command displays two policies attached to the port when only one is attached. This problem is resolved in Release 12.2(17d)SXB9. (CSCed16185)
- If you enter a **no mpls ip** or **no ip addr** interface command, and then enter an **interface range** command, ignore any “const\_mpls\_dec\_mpls\_use: error - zero mpls\_use\_count” messages. This problem is resolved in Release 12.2(17d)SXB9. (CSCeb64700)

- With IGMP snooping enabled, and some IGMPv3 groups that have many sources, you might see messages about high CPU usage if you enter the **clear ip igmp snooping statistics** command. This problem is resolved in Release 12.2(17d)SXB9. (CSCed30453)
- Multicast subnet entries are not removed when you disable PIM on an interface. The stale subnet entries remain programmed in hardware. The forwarding of multicast packets is not affected because the entries are used only for bridging.

**Workaround:** Enter a **shutdown** command on the interface before removing Protocol Independent Multicast (PIM). This problem is resolved in Release 12.2(17d)SXB9. (CSCed28813)

- When booting, you might see the following message:

```
%C6K_PROCMIB-SP-3-IPC_PORTOPEN_FAIL: Failed to open port while connecting to process
statistics: error code = no such port
-Traceback= 4071AD28 4071AE34
```

This problem is resolved in Release 12.2(17d)SXB9. (CSCed12970)

- All ingress IPv6 traffic on an IPv4 VRF-enabled interface is routed in software on the MSFC3. This problem is resolved in Release 12.2(17d)SXB9. (CSCed02778, CSCec03707)
- In IP packets with the IP options field populated, the IP type of service (ToS) byte might be truncated to a 3-bit long field. This problem deletes 3 bits of the 6-bit DSCP value and causes incorrect QoS operation. This problem is resolved in Release 12.2(17d)SXB9. (CSCed93264)
- In rare situations, a ROMMON upgrade for these modules might fail:
  - [WS-X6704-10GE](#)
  - [WS-X6748-SFP](#)
  - [WS-X6724-SFP](#)
  - [WS-X6748-GE-TX](#)

This problem is resolved in Release 12.2(17d)SXB9. (CSCee37771)

- If you configure a SPAN destination port on any of these modules, and the SPAN destination port goes down and comes back up, ingress traffic through other ports on the same port ASIC as the SPAN destination port might experience high latency:
  - Supervisor Engine 2
  - [WS-X6408-GBIC](#)
  - [WS-X6408A-GBIC](#)
  - [WS-X6416-GE-MT](#)
  - [WS-X6416-GBIC](#)
  - [WS-X6516-GBIC](#)
  - [WS-X6516A-GBIC](#)
  - [WS-X6816-GBIC](#)
  - [WS-X6316-GE-TX](#)
  - [WS-X6516-GE-TX](#)

This problem is resolved in Release 12.2(17d)SXB9. (CSCef32513)

- With redundant Supervisor Engines, following a NSF/SSO switchover, the forwarding tables for the port ASIC on the WS-X6816-GBIC fail to repopulate. This causes traffic to be dropped. This problem is resolved in Release 12.2(17d)SXB9. (CSCef88685)

- In egress multicast replication mode, after online insertion or removal (OIR) of a module, some fabric channel utilization might be higher than normal because some multicast traffic is sent across the switch fabric more than often than is necessary. This problem is resolved in Release 12.2(17d)SXB9. (CSCeg28814)
- Layer 2 EtherChannels configured with ports on different DFC-equipped switching modules periodically purge and refresh their Layer 2 address tables. Typically, the refresh takes a few seconds as the EtherChannel learns the destination MAC addresses, during which time the EtherChannel floods all egress traffic to other ports in the VLAN as unknown unicast traffic. With a Layer 2 EtherChannel configured with ports on different DFC-equipped switching modules, the EtherChannel might flood traffic for several minutes. This problem is resolved in Release 12.2(17d)SXB9. (CSCeg39091)
- When a PIM neighbor expires that is the designated forwarder (DF) for multiple rendezvous points (RPs), the DF election is triggered only for the first RP on the list and does not occur for all the other RPs. This problem is resolved in Release 12.2(17d)SXB9. (CSCeg83460)
- The source MAC addresses of traffic received on a Layer 2 [distributed EtherChannel \(DEC\)](#) might be learned in multiple VLANs. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh40945)
- With IOS SLB configured, hardware-accelerated egress IOS ACLs configured on a VLAN interface might be applied to ingress bridged traffic. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh54533)
- At boot time, online diagnostics assume that the ASICs on switching modules are synchronized when they are not. This situation can cause the TestL3VlanMet, TestIngressSpan, and TestEgressSpan tests to fail on WS-6548-GE-TX and WS-6516A-GBIC switching modules. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh56398)
- IGMP snooping does not constrain multicast traffic for multicast group addresses in the range x.128-255.x.x until a receiver joins the multicast group. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh62522)
- A crashinfo file generated as the result of communication failure between the MSFC and the supervisor engine does not contain sufficient diagnostic information. This problem is resolved in Release 12.2(17d)SXB9. (CSCei18018)
- Rarely, on a Supervisor Engine 720, a fabric synchronization error might cause a reload during bootup. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa49748)
- With the default flow control configuration, the ports in an unstable link between a Supervisor Engine 720 equipped with a copper SFP and a port in a chassis with a Supervisor Engine 2 remain in the “up/down” state. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa61788)
- A reload might occur if you enter the **tfoot-server** command with a file name that is longer than 67 characters. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa82886)
- Occasionally, the BGP-allocated per-VRF aggregate tag is not present in the label forwarding information base (LFIB). This situation causes destinations to be unreachable. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa85588)
- Unicast traffic floods continuously to all ports in the VLAN instead of being forwarded only to the EtherChannel member ports. This situation occurs if you shut down member ports in a [distributed EtherChannel \(DEC\)](#) and leave active only the member ports served by a single fabric connection. This problem is resolved in Release 12.2(17d)SXB9. (CSCsb16396)
- On a Supervisor Engine 720, unicast traffic on a Layer 2 [distributed EtherChannel \(DEC\)](#) floods unnecessarily. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh59654)
- Under rare conditions, when you enter a **show mls netflow creation** command, a bus error exception and a system reset may occur. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa96704)

- On an EtherChannel IEEE 802.1q trunk that is configured with VLAN 1 as the native VLAN, connectivity is lost if you change the native VLAN. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa80358)
- Inter-Card Communication (ICC) gets blocked during bootup if the routed MAC aging time is set to 0 (no aging) or the aging time is set to 0. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa76812)
- The system resets because of a TestSPRPInbandPing failure after QoS is enabled and is incorrectly applied to the traffic. This problem is resolved in Release 12.2(17d)SXB9. (CSCsa63184)
- **PA-MC-8TE1+** port adapters fail to check and drop invalid packets with a datagram size of one byte. This problem is resolved in Release 12.2(17d)SXB9. (CSCin78324)
- In releases where CSCeb80453 is resolved, the order-dependent ACL merge (ODM) algorithm does not support the Cisco IOS Firewall Authentication Proxy feature. This problem is resolved in Release 12.2(17d)SXB9. (CSCin72202)
- An update in a bidirectional rendezvous point (Bidir RP) cache during a designated forwarder (DF) election might result in an erroneous path cost. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh95160)
- Unicast traffic carried by a **distributed EtherChannel (DEC)** can be transmitted from different member ports. When the DEC selects a member port supported by one DFC to transmit a packet, and reverse traffic of the same flow is being received by another member port supported by another DFC, the unicast traffic is flooded if the Layer 2 MAC address has aged out on the DFC that is transmitting the packet. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh73110)
- The PFC3 cannot update the DFCs with information about some MAC addresses learned on the PFC under these circumstances:
  - A Supervisor Engine 720 operating in bus mode
  - An egress SPAN source port configured on a DFC-equipped module or an egress SPAN source VLAN that includes ports on a DFC-equipped module
  - Other fabric-enabled modules installed

Traffic to the affected MAC addresses that is received by DFC-equipped modules floods in the VLAN. This problem is resolved in Release 12.2(17d)SXB9. (CSCeh54386)
- IEEE 802.1X port-based authentication fails if the radius authentication server is configured to use MD5 encryption with a per-server radius secret key. This problem is resolved in Release 12.2(17d)SXB9. (CSCeg09691)
- On a Supervisor Engine 2, MAC addresses unnecessarily age out every 4 seconds. This problem is resolved in Release 12.2(17d)SXB9. (CSCef66632)
- When you enter the **interface loopback** command to create a new virtual interface or when you enter the **tag-switching** command, the Network Time Protocol (NTP) configuration might be altered to use an invalid source interface. This problem is resolved in Release 12.2(17d)SXB9. (CSCdx86562)
- The **logging snmp-authfail** command is enabled by default. This problem is resolved in Release 12.2(17d)SXB9. (CSCeb71693)
- The Egress Multicast Replication feature assumes that there is a supervisor engine in slot 1, which can be invalid for a Supervisor Engine 720. If a port on a module in slot 1 is a member of a multicast group, this problem sends multicast traffic to a Supervisor Engine 720 when the Supervisor Engine 720 uplink ports are not members of the multicast group. This problem is resolved in Release 12.2(17d)SXB9. (CSCee40846)

- When an EtherChannel trunk is configured to carry many VLANs, traffic pauses for as much as several seconds when you add or remove member ports from the EtherChannel. This problem is resolved in Release 12.2(17d)SXB9. (CSCef33051)
- In VTP transparent mode, the VLAN database might be lost after a VTP configuration error occurs. This problem is resolved in Release 12.2(17d)SXB9. (CSCef47414)
- Closing an existing Telnet session may cause the system to reset. This problem is resolved in Release 12.2(17d)SXB9. (CSCds33629)
- With a Supervisor Engine 720 and DFC-equipped switching modules, you might see messages similar to these followed by tracebacks and a reload:

```
EARL_L2_ASIC-DFC6-4-SRCH_ENG_FAIL: EARL L2 ASIC Search Engine has failed
SCHED-DFC6-3-STILLWATCHING: Process still watching boolean EARL SE watched boolean
```

This problem is resolved in Release 12.2(17d)SXB9. (CSCsb32028)

### Resolved General Caveats in Release 12.2(17d)SXB8

- The SNMP ifInDiscards value incorrectly resets to zero. This problem is resolved in Release 12.2(17d)SXB8. (CSCef76161)
- With a Supervisor Engine 720, you might see software-forced reloads. This problem is resolved in Release 12.2(17d)SXB8. (CSCed36177)
- If you configure multiple IP service level agreement (SLA) jitter probes to send packets to the same destination IP address and port number, and you turn the responder router off and back on, the probes show traffic loss (displayed as the packetMIA value) that is equal to the probe's number of packets minus one. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg64124)
- Several MIB entity tables share one entCacheFlag and under rare circumstances, accessing the MIB entity tables might cause an entCacheFlag state that is not valid for all the MIB entity tables and a reload might occur. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg19038)
- In a configuration with many routes and many routing changes, you might see IPC-3-NOBUFF messages indicating that the IPC message header cache is exhausted and a reload might occur. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg08562)
- Modifying the configuration of statically configured bidirectional PIM rendezvous points (RPs) can cause very high CPU utilization. This problem is resolved in Release 12.2(17d)SXB8. (CSCef36367)
- Ingress multicast traffic might stop after the receipt of a multicast join message on an RPF interface if a downstream router has already converged. This problem is resolved in Release 12.2(17d)SXB8. (CSCef60452)
- On a Supervisor Engine 720, the **show version** command might display an incorrect cause for a reload. This problem is resolved in Release 12.2(17d)SXB8. (CSCef80423)
- Ingress VLAN SPAN (VSPAN) does not work for voice VLANs. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg70376)
- With OSPF routing configured, and with default routes learned from multiple autonomous system boundary routers (ASBRs) as equal cost paths, reconfiguring the cost of one of the interfaces for the default routes does not correctly update the routing table. This problem is resolved in Release 12.2(17d)SXB8. (CSCee16068)



## Resolved General Caveats in Release 12.2(17d)SXB7

- Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

This problem is resolved in Release 12.2(17d)SXB7. (CSCef68324)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

This problem is resolved in Release 12.2(17d)SXB7. (CSCef60659, CSCef44225, CSCsa59600, CSCef44699, CSCef61610)

- Malfunctioning PIM, MLSM, or mwheel processes might cause “CPUHOG” and “WATCHDOG” messages and reloads. This problem is resolved in Release 12.2(17d)SXB7. (CSCed12393)
- If you enter the **no ip vrf vrf\_name** command in one administrative session, a reload might occur if you enter the **ip vrf vrf\_name** command for the same VRF in another administrative session before the deletion process completes. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg51793)
- While the output of the **show mls ip multicast vrf vrf\_name** command is being displayed in one administrative session, a reload might occur if you enter the **no ip vrf vrf\_name** command for the same VRF in another administrative session. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg55565)
- Bridged UDP broadcasts are not forwarded correctly if you enter the **ip forward-protocol turbo-flood** command. This problem is resolved in Release 12.2(17d)SXB7 and rebuilds with the **udp-checksum** keywords (see the Command Reference). (CSCef46561)

- When there is a unicast routing loop and when a static multicast route has been configured, a Reverse Path Forwarding (RPF) lookup might cause a reload because of a stack overflow. This problem is resolved in Release 12.2(17d)SXB7. (CSCeb51147)
- Performance might be lower than expected and CPU utilization might be high during packet forwarding under the following circumstances:
  - There is a service policy attached to one or more interfaces.
  - The policy map of the service policy contains one or more class maps that are configured with one or more **match access-group name** *access\_group\_name* class-map configuration commands.
  - There is a large number of named extended IP access control lists (ACLs) configured, and traffic matches these ACLs.

This problem is resolved in Release 12.2(17d)SXB7. (CSCdv68743)

- A reload might occur if you perform Simple Network Management Protocol (SNMP) get operations on Open Shortest Path First (OSPF) MIBs. This problem is resolved in Release 12.2(17d)SXB7. (CSCeb40561)
- A reload might occur when Optimized Edge Routing (OER) and BGP dampening are both configured and OER injects a route that does not exist in the routing information base (RIB). This problem is resolved in Release 12.2(17d)SXB7. (CSCed63876)
- A memory leak might occur when the MPLS Label Switching Router (LSR) MIB is queried. This problem is resolved in Release 12.2(17d)SXB7. (CSCee26700)
- The inner time-to-live (TTL) field is not decremented properly in tunneled traffic. This problem is resolved in Release 12.2(17d)SXB7. (CSCee30816)
- In rare situations, a timing problem might cause a Supervisor Engine 720 to reload. This problem is resolved in Release 12.2(17d)SXB7. (CSCee86168)
- When the MPLS-LSR-MIB MIB is enabled and you query the object `mplsXCIndexNext` and there are more than 1,000 Multiprotocol Label Switching (MPLS) labels active, the Simple Network Management Protocol (SNMP) agent might use 99 percent of the CPU capacity of the MSFC for an arbitrarily long time and might generate CPUHOG errors and cause a reload. This problem is resolved in Release 12.2(17d)SXB7. (CSCef37186)
- The voltage termination (VTT) minor and major temperature alarm thresholds are 85°C and 100°C instead of 100°C and 115°C. This problem is resolved in Release 12.2(17d)SXB7. (CSCef58590)
- If you repeatedly change the configuration of a Gigabit Ethernet interface between Layer 2 and Layer 3 when there is traffic flowing, the interface drops traffic. This problem is resolved in Release 12.2(17d)SXB7. (CSCef82367)
- In rare situations, with a mix of Link State Advertisements (LSAs) that travel throughout the Autonomous System (Types 5 and 11) and LSAs that travel within a particular open shortest path first (OSPF) area (Types 1, 2, 3, 4, 6, 7, 9 and 10), a reload might occur. This problem is resolved in Release 12.2(17d)SXB7. (CSCef93215)
- With TCP header compression configured, the TCP packet length is incorrect after decompression. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg08344)
- With OSPF configured, a reload might occur if you simultaneously deconfigure OSPF in one administrative session and configure it in another administrative session. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg19442)

- A memory leak might occur on the redundant supervisor engine if there is a continuous stream of IGMP joins for unique multicast groups being sent to a port where IGMP snooping is enabled and where the total number of multicast groups is increasing. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg56052)
- If you enter the **ip forward-protocol turbo-flood** command, UDP broadcasts are not forwarded correctly on interfaces where bridge groups are configured. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg65640)
- If EoMPLS or VPLS VCs were previously configured and the disposition labels for these VCs are allocated to a different path, ingress MPLS traffic might be dropped. This problem is resolved in Release 12.2(17d)SXB7. (CSCeh11095)
- In a PE router configuration, per-VLAN spanning tree (PVST) bridge protocol data units (BPDUs) are incorrectly untagged. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa57079)
- In a PE router configuration, the CoS value of BPDUs are not copied to the MPLS EXP bits. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa59260)
- With a very long IP access list containing primarily /32 entries configured to provide PFC QoS filtering, any ACL change (for example, adding or deleting an access-list entry) causes high CPU usage for several minutes. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg10174)
- With a Supervisor Engine 720, configuring RSPAN causes high CPU utilization. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa51770)

### Resolved General Caveats in Release 12.2(17d)SXB6

- You cannot configure the MAC address aging time for traffic that has the routed MAC (RM) bit set. This problem is resolved in Release 12.2(17d)SXB6 with the **mac-address-table aging-time number\_of\_seconds routed-mac** command. (CSCef72013)
- A reload might occur if one process is writing to NVRAM and another process is reading from NVRAM and the read fails. This problem is resolved in Release 12.2(17d)SXB6. (CSCec63011)
- Traffic loss might occur if you configure a loopback interface with an IP address that is already in use elsewhere in the network and there are multiple paths to the prefix. This problem is resolved in Release 12.2(17d)SXB6. (CSCee85152)
- A reload might follow OIR of a switching module configured with EtherChannels that are carrying multicast traffic. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg15012)
- With PIM Snooping enabled, if a downstream router sends a (S,G,R) prune, it is not seen by other routers that are receiving traffic for G on the shared tree (these routers have a (\*,G) join state). This situation drops the traffic for G that is going to the other routers. This problem is resolved in Release 12.2(17d)SXB6. (CSCef45495)
- Boot failure might occur when there are more than 256 different policy maps attached as service policies. This problem is resolved in Release 12.2(17d)SXB6. (CSCee24349)
- While the output of the **show ip vrf interface** command is being displayed in one administrative session, a reload might occur if you enter **no ip vrf** commands in another administrative session. This problem is resolved in Release 12.2(17d)SXB6. (CSCeb40653)
- Over an SSHv2 connection, the output from a command that displays many lines of text pauses until you press a key. This problem is resolved in Release 12.2(17d)SXB6. (CSCef61978)
- The CEF entries for traffic from a directly connected Layer 3 address are removed and recreated randomly, which causes Unicast traffic loss for the affected entries. This problem is resolved in Release 12.2(17d)SXB6. (CSCeb53542)

- IEEE 802.1X port-based authentication might not work if it is enabled on more than 50 ports. This problem is resolved in Release 12.2(17d)SXB6. (CSCin83972)
- With a configuration that connects an MPLS backbone to an IPv4 cloud, traffic might be dropped following a reload. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg40177)
- VRF traffic might be routed in software on the MSFC because CEF entries are not updated. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg26378)
- With parallel links between two provider edge (PE) routers, the Label Distribution Protocol (LDP) does not work after failure of one of the links. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg24287)
- With a Supervisor Engine 720 and a PFC3BXL, the Layer 2 CoS value of egress-routed multicast traffic might be changed inappropriately. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg06698)
- After tunnels have been configured and removed, traffic loss occurs over OSM POS links, OSM ATM links, and FlexWAN serial links. This problem is resolved in Release 12.2(17d)SXB6. (CSCef76828)
- The software does not respond to hardware-reported ECC errors in the Layer 2 MAC address table. This problem is resolved in Release 12.2(17d)SXB6. (CSCef35707)
- With a Supervisor Engine 2, the software and hardware CEF tables might not be consistent with each other. This problem is resolved in Release 12.2(18)SXD3. (CSCef27359)
- With the **maximum-paths import** command configured, a BGP VPNv4 table might contain paths that were imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix. This problem is resolved in Release 12.2(17d)SXB6. (CSCee59315)
- MPLS-to-IP traffic might not recover after switchover to a redundant supervisor engine. This problem is resolved in Release 12.2(17d)SXB6. (CSCee37430)
- Unicast routing updates might not be sent to RIP static neighbors. This problem is resolved in Release 12.2(17d)SXB6. (CSCed63342)
- In a PE configuration, you might see “TOOBIG” messages and a traceback. This problem is resolved in Release 12.2(17d)SXB6. (CSCee95708)
- The VLAN translation feature does not work on [WS-X6816-GBIC](#) modules. This problem is resolved in Release 12.2(17d)SXB6. (CSCed73700)
- When a Layer 3 VLAN interface is configured as an OSPF nonbroadcast network and a polling interval is configured for every OSPF neighbor, unnecessary ARPs are sent. This problem is resolved in Release 12.2(17d)SXB6. (CSCed26217)
- With a Supervisor Engine 720 and a [WS-SVC-NAM-2](#), a reload occurs after an SSO switchover if you enter the **ip route-cache flow** command under an ATM physical interface and the **ip nbar protocol-discovery** command under an ATM subinterface. This problem is resolved in Release 12.2(17d)SXB6. (CSCef06034)

## Resolved General Caveats in Release 12.2(17d)SXB5

- Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

This problem is resolved in Release 12.2(17d)SXB5. (CSCin82407)

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

This problem is resolved in Release 12.2(17d)SXB5. (CSCee67450)

- IEEE 802.1X port-based authentication might not work if it is enabled on more than 50 ports. This problem is resolved in Release 12.2(17d)SXB5. (CSCef75501)
- DFC-equipped switching modules support only 1024 VLANs for egress multicast replication. This problem is resolved in Release 12.2(17d)SXB5. (CSCef63549)
- With redundant Supervisor Engine 720s, occasionally following an SSO switchover, a [WS-X6816-GBIC](#) switching module might reset. This problem is resolved in Release 12.2(17d)SXB5. (CSCef41228)
- In rare situations, a software-forced reload might occur. This problem is resolved in Release 12.2(17d)SXB5. (CSCef91572)
- This message might be displayed, followed by a reload:

```
EARL-SP-2-PATCH_INVOCATION_LIMIT: 10 Recovery patch invocations
in the last 30 secs have been attempted.
Max limit reached
```

This problem is resolved in Release 12.2(17d)SXB5. (CSCed66865)

- With Open Shortest Path First (OSPF) configured, but with the **limit retransmissions non-dc disable** configuration command not configured, retransmission counters might not be reset when a neighbor is terminated. This problem is resolved in Release 12.2(17d)SXB5. (CSCec29953)
- With BGP and MPLS configured on OC-48, OC-12, or OC-3 OSM-POS interfaces, BGP neighbors go up and down every few hours. This problem is resolved in Release 12.2(17d)SXB5. (CSCee72817)

- Policy-based routing (PBR) does not work if both PBR and Cisco IOS server load balancing (SLB) are configured on same interface. This problem is resolved in Release 12.2(17d)SXB5. (CSCin82741)
- The unknown unicast flood protection (UUFPP) automated error-recovery process does not work. This problem is resolved in Release 12.2(17d)SXB5. (CSCin79961)
- In rare situations, intensive SNMP polling might use all available I/O memory. This problem is resolved in Release 12.2(17d)SXB5. (CSCeg11566)
- With IGMP snooping disabled and with a static multicast address configured in a VLAN, a reload might occur if you enter the **vlan** *vlan\_id* and **no vlan** *vlan\_id* global configuration commands for the VLAN. This problem is resolved in Release 12.2(17d)SXB5. (CSCeg01510)
- A VACL can match BPDUs. Spanning tree loops can occur if the VACL drops or redirects the BPDUs. This problem is resolved in Release 12.2(17d)SXB5. (CSCef58932)
- After you remove the IP address from an interface, the interface continues to forward IP traffic. This problem is resolved in Release 12.2(17d)SXB5. (CSCef05282)
- In switch-fabric “bus” mode with either [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching modules installed, some ingress SPAN traffic is duplicated. This problem is resolved in Release 12.2(17d)SXB5. (CSCee78323)
- The **show interface status** command displays “notconnected” for SPAN destination ports. This problem is resolved in Release 12.2(17d)SXB5. (CSCee77136)
- With a default route configured, a reload might occur if you enter the **clear ip route \*** command. This problem is resolved in Release 12.2(17d)SXB5. (CSCee35125)
- With ROMMON configured to ignore the startup-config file, if you enter the **mls cef maximum-routes** command and do a reload, continuous reloads occur. This problem is resolved in Release 12.2(17d)SXB5. (CSCee07395)
- With OSPF configured between a PE router and a CE router, when there is an import map configured on the PE router, there are no routes from the CE router in the BGP route table. This problem is resolved in Release 12.2(17d)SXB5. (CSCed81317)
- With VRF and more than 9,000 routes configured, the CEF reloader process might cause CPUHOG messages to be displayed. This problem is resolved in Release 12.2(17d)SXB5. (CSCed57281)
- There is no response to SNMP requests and memory use increases until tracebacks occur. This problem is resolved in Release 12.2(17d)SXB5. (CSCed52841)
- If a BGP peer group member establishes itself more slowly than other peer group members and becomes active while other members of the peer group are already converging, the recently established peer group member might not advertise routes that were sent to the other members. This problem is resolved in Release 12.2(17d)SXB5. (CSCea64725)
- With a PFC2 and GRE tunnel traffic, the do not fragment (DF) bit not be copied correctly and the time-to-live (TTL) count might not be decremented correctly. This problem is resolved in Release 12.2(17d)SXB5. (CSCuk49481)
- When one of two trunks configured as parallel links goes down, traffic might be directed to the inactive trunk instead of to the active trunk. This problem is resolved in Release 12.2(17d)SXB5. (CSCef89139)

- Some traffic loss might occur when all of the following situations occur simultaneously:
  - You have a nontrunking Layer 2 EtherChannel with member ports on a fabric-enabled module and on a nonfabric-enabled module (for example, an EtherChannel with member ports on a Supervisor Engine 720 and on a [WS-X6408A-GBIC](#) switching module).
  - You have two or more [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching modules installed, or you have one of each.
  - You have a port in the same VLAN as the EtherChannel on each [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching module.
  - One of the [WS-X6516A-GBIC](#) or [WS-X6548-GE-TX](#) switching modules resets.

This problem is resolved in Release 12.2(17d)SXB5. (CSCef82797)

- With the following configuration, some Layer 3 traffic that traverses a Layer 2 EtherChannel might be lost and some Layer 3 traffic that is processed by the central rewrite engine (for example, multicast, GRE, MPLS, IPV6, NAT, PBR) might be lost:

- [WS-SUP720](#), hardware revision 3.2 or higher

Enter the **show module version | include WS-SUP720-** command to display the hardware revision. For example:

```
Router# show module version | include WS-SUP720-
7      2  WS-SUP720-BASE      SAD075301SZ Hw :3.2
```

- SPAN or RSPAN configured
- “Flow through” global fabric switching mode

Enter the **show fabric switching-mode | include Global** command to display the global switching mode. For example:

```
Router# show fabric switching-mode | include Global
Global switching mode is Flow through
```

An additional effect is that local SPAN and RSPAN source ports do not copy VACL-redirected traffic. This problem is resolved in Release 12.2(17d)SXB5. (CSCef75924, CSCef78235)

- Some IP traffic might be sent with incorrect alignment, and you might see “ALIGN-SP-3-CORRECT: Alignment correction made” messages. This problem is resolved in Release 12.2(17d)SXB5. (CSCef73076)
- SNMP get-bulk requests for objects in the CISCO-STACK-MIB raises CPU utilization unacceptably. This problem is resolved in Release 12.2(17d)SXB5. (CSCef67810)
- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

This problem is resolved in Release 12.2(17d)SXB5. (CSCef46191)



- Occasionally, an all-zero address entry for a static route is made in the hardware routing table because the entry is made before the adjacency for the address is resolved. This problem is resolved in Release 12.2(17d)SXB5. (CSCef30308)
- With a Supervisor Engine 720, a reload might occur when you configure context-based access control (CBAC). This problem is resolved in Release 12.2(17d)SXB5. (CSCee75620)
- When more than 12 logical operator units (LOUs) are used in a policy attached to an interface, the entries are expanded. If the expanded entries are for a non-deny ACE, the entries are not accurate. The resulting ACEs for the policy are also inaccurate. This problem is resolved in Release 12.2(17d)SXB5. (CSCed47753)
- If you enter the **show tech-support** command, you might see “%SCHED-2-NOTWATCHTIMER” and “%SCHED-3-STILLWATCHINGT” messages. This problem is resolved in Release 12.2(17d)SXB5. (CSCec67602)
- A reload might occur if you delete a VPN routing and forwarding (VRF) instance while the **show ip vrf vrf\_name EXEC** command executes. This problem is resolved in Release 12.2(17d)SXB5. (CSCea83675)
- With very large flows, NDE byte counts might be incorrect (NDE packet counts remain correct). This problem is resolved in Release 12.2(17d)SXB5. (CSCee23058, CSCee65953)
- Directly connected multicast enabled subnets might not be programmed correctly on the PFC. This problem is resolved in Release 12.2(17d)SXB5. (CSCed00394)
- QoS access control lists with Layer 4 port operations are not supported. This problem is resolved in Release 12.2(17d)SXB5. (CSCdx91720)

#### Resolved General Caveats in Release 12.2(17d)SXB4

- With optical transceivers installed, a SFF8472-3-INTERNAL\_ERROR assert might occur. This problem is resolved in Release 12.2(17d)SXB4. (CSCef27457)
- The **logging event link-status** interface command does not work properly after you enter the **load-interval** interface command. This problem is resolved in Release 12.2(17d)SXB4. (CSCef14934)
- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.



The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

This problem is resolved in Release 12.2(17d)SXB4. (CSCed78149)

- When a large number of VRFs (more than 200) and prefixes (more than 220,000) are configured, BGP inbound update processing slows down and prolonged high CPU utilization occurs. This problem is resolved in Release 12.2(17d)SXB4. (CSCee43166)
- Following a reload with Distributed Link Fragmentation and Interleaving (dLFI) and hierarchical QoS configured on WAN ports, packet output and drop counters are not updated. (CSCin79768)

### Resolved General Caveats in Release 12.2(17d)SXB3

- On a Supervisor Engine 720, if you enter a **clear scp status** command, you see repeated SCP-SP-5-ASYNC\_WATERMARK messages. This problem is resolved in Release 12.2(17d)SXB3. (CSCef15223)
- With multicast support configured on a Supervisor Engine 2, VACLs do not capture traffic for RSPAN. This problem is resolved in Release 12.2(17d)SXB3. (CSCef07017)
- With IGMP snooping configured, the flow of multicast traffic to a multicast receiver might be stopped after failure to respond to one IGMP query, instead of two. This problem is resolved in Release 12.2(17d)SXB3. (CSCee68052)
- The DSCP value is incorrectly set to zero in NBAR traffic. This problem is resolved in Release 12.2(17d)SXB3. (CSCec49042)
- With a large number of EtherChannels configured, CPU utilization might periodically rise to unacceptably high values. This problem is resolved in Release 12.2(17d)SXB3. (CSCee55233)
- PIM does not remove interfaces from the (S,G) output interface list when it receives a (\*,G) prune message if the interfaces were added to the (S,G) output interface list because of a (\*,G) join message. This problem is resolved in Release 12.2(17d)SXB3. (CSCee04368)
- Occasionally, these modules might lose the ability to communicate over the Ethernet Out of Band Channel (EOBC) and reset:
  - [WS-X6416-GBIC](#)
  - [WS-X6348-RJ-45](#)
  - [WS-X6148-RJ-45](#)
  - [WS-X6348-RJ-21V](#)
  - [WS-X6148-RJ-21](#)
  - [WS-X6316-GE-TX](#)
  - [WS-X6324-100FX](#)
  - [WS-X6416-GE-MT](#)
  - [WS-X6024-10FL-MT](#)

This problem is resolved in Release 12.2(17d)SXB3. (CSCef23843)

- When an output ACL is applied on multiple interfaces and the first interface to which it is applied is not configured with an IP address, the ACL denies all traffic on all interfaces where it is applied. This problem is resolved in Release 12.2(17d)SXB3. (CSCef21575)

- A reload might occur if you use SNMP to collect the statistics from a policy map that has a shared aggregate policer. This problem is resolved in Release 12.2(17d)SXB3. (CSCee83655)
- Occasionally, CEF mistakes the state of an active interface and does not forward traffic to what it sees as an inactive interface. This problem is resolved in Release 12.2(17d)SXB3. (CSCdt38401)

### Resolved General Caveats in Release 12.2(17d)SXB2

- If there are more than 50 files on the flash card, access from CiscoView Device Manager (CVDm) might cause a reload. This problem is resolved in Release 12.2(17d)SXB2. (CSCef07965)
- With an SFM, some modules might stop egressing traffic. This problem is resolved in Release 12.2(17d)SXB2. (CSCee08015)
- A sparse mode multicast router in static rendezvous point (RP) mode configured without the override keyword changes from static RP mode to bidirectional mode if it receives an “AutoRP” message advertising multicast groups in bidirectional mode. This problem is resolved in Release 12.2(17d)SXB2. (CSCea86164)
- Tracebacks might occur when you modify a policer or an ACL. This problem is resolved in Release 12.2(17d)SXB2. (CSCee43009)
- Following an SSO switchover, all EtherChannel member ports shut down and then come back up. This problem is resolved in Release 12.2(17d)SXB2. (CSCed77602)
- After an OIR of a CEF720 switching module, traffic loss might occur on the module because the Multicast Expansion Table might not be downloaded correctly. This problem is resolved in Release 12.2(17d)SXB2. (CSCee67561)
- With BGP multipath configured, when the underlying path changes for an existing BGP prefix, the hardware entry for it is deleted and reinstalled. This situation causes long route convergence times. This problem is resolved in Release 12.2(17d)SXB2. (CSCec50884)
- An OSPF designated router (DR) does not generate a network link-state advertisement (LSA) for a broadcast network when another interface on the designated router has an administratively shutdown interface with a duplicate address configured with the OSPF passive-interface command. This problem is resolved in Release 12.2(17d)SXB2. (CSCea35186)
- If you delete or add a redirect interface in a VACL access map, and then an RPR+ switchover occurs, the newly active MSFC might reload. This problem is resolved in Release 12.2(17d)SXB2. (CSCin76766)
- Occasionally, with IEEE 802.1s multiple spanning tree (MST) configured with redundant supervisor engines, the root bridge priority and MAC address are set to zero following a switchover to the redundant supervisor engine. This problem is resolved in Release 12.2(17d)SXB2. (CSCin74123)
- If you power-cycle redundant SFMs, DFC-equipped switching modules might not come back online. This problem is resolved in Release 12.2(17d)SXB2. (CSCin70599)
- On a Layer 2 port, microflow policing might not work because the automatically configured flowmask is incorrect. This problem is resolved in Release 12.2(17d)SXB2. (CSCin68355)
- A reload might occur if you enter the **mac-address-table limit** command for VLAN 1. This problem is resolved in Release 12.2(17d)SXB2. (CSCef14436)
- The approximate Layer 2 switching rate displayed by the **show mls statistics** command is double the actual rate. This problem is resolved in Release 12.2(17d)SXB2. (CSCee92338)
- If you enter the **mls ip multicast stub** command on a VLAN interface that is configured with a secondary IP address, the RACL that is automatically loaded into the TCAM on the PFC does not contain a permit statement for the secondary IP address. This problem is resolved in Release 12.2(17d)SXB2. (CSCee88700)

- A reload might occur if the output of a **show** command is left at the “More” prompt for an extended period and you attempt to resume display of the command output. This problem is resolved in Release 12.2(17d)SXB2. (CSCee89232)
- OIR of any module makes the egress QoS counters for other modules inaccurate. This problem is resolved in Release 12.2(17d)SXB2. (CSCee82440)
- Under certain circumstances, a first hop router randomly fails to add the outgoing interfaces of some (S,G) flows to its forwarding information base (FIB) hardware table. This problem is resolved in Release 12.2(17d)SXB2. (CSCee80365)
- UPD packets are fragmented if an ingress interface has a larger MTU size than the egress interface. On a Supervisor Engine 720, a VACL configured to provide VLAN filtering drops the UPD fragments. This problem is resolved in Release 12.2(17d)SXB2. (CSCee69687)
- When multihop exterior Border Gateway Protocol (eBGP) with multiple links is configured between PE and CE routers, the console is flooded with “taginfo do not own rew, but ctgrew notcreated yet” debug messages. This problem is resolved in Release 12.2(17d)SXB2. (CSCee54526)
- 48-port switching modules that support power-over-Ethernet (PoE) daughtercards, but that do not have a PoE daughter card installed, might stop forwarding traffic for approximately 5 minutes after a reload or module reset. This problem is resolved in Release 12.2(17d)SXB2. (CSCee51501)
- Traffic loss might occur on fabric-enabled modules when there are frequent OIRs. This problem is resolved in Release 12.2(17d)SXB2. (CSCee44496, CSCee48403, CSCee78766)
- SPAN sessions might not work correctly after an SSO switchover. This problem is resolved in Release 12.2(17d)SXB2. (CSCee25844)
- After an OIR of a fan, the fan type and information from the fan IDPROM is not available. This problem is resolved in Release 12.2(17d)SXB2. (CSCee24634)
- EtherChannels might not work on OSM LAN ports. This problem is resolved in Release 12.2(17d)SXB2. (CSCee23164)
- At chassis power up, if the active supervisor engine has a fault that causes it to reload before the redundant supervisor engine is ready to become active, the redundant supervisor engine might also be reset and never become active. This problem is resolved in Release 12.2(17d)SXB2. (CSCee05653)
- Under heavy traffic conditions, online insertion or removal (OIR) of a switch fabric module or OIR of a nonfabric-enabled module might cause OSMs to stop forwarding traffic. This problem is resolved in Release 12.2(17d)SXB2. (CSCec49269)
- With other CEF256 or CEF720 modules installed, a [WS-X6816-GBIC](#) module does not come on line after a hot insert or software reset. This problem is resolved in Release 12.2(17d)SXB2. (CSCec27072)
- The time-to-live (TTL) value might not be decremented correctly in tunnel traffic. This problem is resolved in Release 12.2(17d)SXB2. (CSCea77189)
- With bidirectional PIM configured, when the designated forwarder (DF) fails and the nondesignated forwarder takes over, “pim cpuhog” messages are seen on the nondesignated forwarder. This problem is resolved in Release 12.2(17d)SXB2. (CSCea49566)
- The **no ip vrf vrf\_name** command does not delete the virtual routing and forwarding (VRF) configuration. This problem is resolved in Release 12.2(17d)SXB2. (CSCeb78347)
- An **snmpwalk** command on a loopback interface does not yield any results. This problem is resolved in Release 12.2(17d)SXB2. (CSCdz27562)

- With Gigabit Ethernet line-rate traffic directed to a Virtual Router Redundancy Protocol (VRRP) virtual address, there might be more than one master VRRP router. This problem is resolved in Release 12.2(17d)SXB2. (CSCdz21402)
- When a Multicast Source Discovery Protocol (MSDP)-enabled rendezvous point (RP) for a multicast group fails and an incoming (\*,G) join message is received, the RP does not build an (S,G) state from its Source-Active (SA) cache when it should do so. Depending on the topology and if a Shortest Path Tree (SPT) threshold is configured as infinite, this situation might result in a multicast forwarding interruption of up to 2 minutes. This problem is resolved in Release 12.2(17d)SXB2. (CSCee89438)
- With distributed Cisco IOS IPv6 Provider Edge (6PE) configured on a module, if you OIR the module or reload the module, the 6PE routes are reloaded on the module but they do not have tag rewrites present and so appear as recursive unresolved routes. This problem is resolved in Release 12.2(17d)SXB2. (CSCee79408)
- The **distribute-list** command does not work correctly on Multiprotocol BGP (MBGP) virtual routing and forwarding (VRF) interfaces. This problem is resolved in Release 12.2(17d)SXB2. (CSCee46753)
- WCCP-redirected packets that have no next hop ARP cache entry are process switched to generate an ARP request, but because of the WCCP redirection, no ARP request is sent and the ARP cache is never populated for the next hop and subsequent WCCP-redirected packets continue to be process switched. This problem is resolved in Release 12.2(17d)SXB2. (CSCed92290)
- When the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured, the withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table. This problem is resolved in Release 12.2(17d)SXB2. (CSCed60800)
- Following a reload, an OSPF designated router (DR) might fail to regenerate the network link-state advertisement (LSA) when there is a shutdown interface with the same interface address in the OSPF area. This problem is resolved in Release 12.2(17d)SXB2. (CSCee36721)
- If you enter a **shutdown** command on a VLAN interface where you have disabled the spanning tree protocol with the **bridge-group group\_id spanning-disabled** interface command, the spanning tree protocol is enabled after you enter a **no shutdown** command. This problem is resolved in Release 12.2(17d)SXB2. (CSCec84887)
- With Internet Group Management Protocol (IGMP) and IP Protocol Independent Multicast (PIM) enabled, continual tracebacks might occur when you perform an online insertion and removal (OIR) of a module. This problem is resolved in Release 12.2(17d)SXB2. (CSCec13278)
- If you change the STP root bridge, a Layer 2 loop might exist very briefly. This problem is resolved in Release 12.2(17d)SXB2. (CSCed85411)
- TCP FIN and RST packets might be dropped, which causes a 3- to 4-second delay in retrieving web content, if a hardware-switched TCP connection carrying more than 1,000 packets per second is load balanced through Cisco IOS Firewall Load Balancing or Cisco IOS server load balancing. This problem is resolved in Release 12.2(17d)SXB2. (CSCed38956)
- A reload might follow receipt of a corrupt CPD packet. This problem is resolved in Release 12.2(17d)SXB2. (CSCec25430)
- A reload might occur when you enter a **show** command that is related to IP multicast if the “more” prompt has been displayed for a long period of time. This problem is resolved in Release 12.2(17d)SXB2. (CSCea81029)
- Protocol Independent Multicast (PIM) join messages might not be sent when buffer allocation failures occur and when the I/O memory is low. This problem is resolved in Release 12.2(17d)SXB2. (CSCec40377)

- Configured static multicast routes may be ignored in the Reverse Path Forwarding (RPF) calculation. This problem is resolved in Release 12.2(17d)SXB2. (CSCeb57662)
- In a multicast virtual private network (MVPN) environment with a provider edge (PE) router configuration and with the **ip pim register-rate-limit** global configuration command enabled, PIM register messages might not be sent for the default multicast distribution tree (MDT) to its rendezvous point (RP). This situation prevents PE routers from establishing PIM adjacencies with other PE routers in the MVPN. This problem is resolved in Release 12.2(17d)SXB2. (CSCea59359)
- A reload might occur when you enter the **no mpls l2transport route** interface configuration command to remove a Label Distribution Protocol (LDP) configuration before you remove an Ethernet over Multiprotocol Label Switching (EoMPLS) configuration. This problem is resolved in Release 12.2(17d)SXB2. (CSCdx80484)

### Resolved General Caveats in Release 12.2(17d)SXB1

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>.

This problem is resolved in Release 12.2(17d)SXB1. (CSCed65285)

- Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

More details can be found in the security advisory, which is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

This problem is resolved in Release 12.2(17d)SXB1. (CSCed40933)

- The values displayed by the **show mls statistics** command are incorrect. This problem is resolved in Release 12.2(17d)SXB1. (CSCee53572)
- With very short MLS aging times configured, the CPU usage of NetFlow feature be displayed as greater than 100 percent. This problem is resolved in Release 12.2(17d)SXB1. (CSCee18480)
- With certain configurations, a reload might occur when you enter the **show cdp entry \* protocol** command. This problem is resolved in Release 12.2(17d)SXB1. (CSCed40563)
- A Secure Shell (SSH) connection that is using TACACS+ for authentication that fails due to an unknown username or incorrect password results in a memory leak and a TCP connection that hangs in the CLOSEWAIT or ESTAB state. An SSH2 connection (if supported) results in the leak even if the authentication succeeds. This problem is resolved in Release 12.2(17d)SXB1. (CSCed65285)
- The process of collecting statistics and counter values might cause high CPU utilization. This problem is resolved in Release 12.2(17d)SXB1. (CSCee54862)

- When you enter the **access interface\_type route framed-ip** command on an Cisco IOS Radius Load Balancing (RLB) virtual server that is load balancing gateways, packets might incorrectly be Layer 3 switched in hardware, which causes a packet to loop until the IP Time-To-Live expires, because interface-full-flow mode is not being automatically configured. This problem is resolved in Release 12.2(17d)SXB1. (CSCee43090)
- For ACEs that match on DSCP, 7 bits, instead of 6 bits, are programmed into the ACL TCAM. This problem is resolved in Release 12.2(17d)SXB1. (CSCee39170)
- A reload might follow the display of these messages:

```
%RPC-SP-2-FAILED: Failed to send RPC request online_diag_sp_request:get_rp_cpu_info
-Traceback= 40929C90 4067A8F0 40683EB8 406609D4 406612C0 40661DAC 40660040 4065FEB8
%Software-forced reload
Unexpected exception, CPU signal 23, PC = 0x4013E95C
-Traceback= 4013E95C 4013C824 40929C98 4067A8F0 40683EB8 406609D4 406612C0 40661DAC
40660040 4065FEB8
```

This problem is resolved in Release 12.2(17d)SXB1. (CSCee36959)

- When you enter the **no mpls ip propagate-ttl** global configuration mode command, IPv6 packets are incorrectly processed: the TTL count is decremented. This problem is resolved in Release 12.2(17d)SXB1. (CSCee19156)
- The FibTcamSSRAM on-demand online diagnostic test fails for IPv6 packets. This problem is resolved in Release 12.2(17d)SXB1. (CSCee10614)
- To avoid a reload, do not enter the **test memory EXEC** command. This problem is resolved in Release 12.2(17d)SXB1. (CSCee13713)
- If you enter the **mdix auto** global configuration command, [WS-X6548-RJ-45](#) and [WS-X6548-RJ-21](#) Ethernet ports that are not configured to negotiate the Ethernet speed might not pass traffic. (CSCee07738)
- Releases earlier than Release 12.2(17d)SXB1 that have support for the [WS-SVC-MWAM-1](#) Multi-Processor WAN Application Module always actively listen on TCP port 514, instead of only when an WS-SVC-MWAM-1 is installed. This problem is resolved in Release 12.2(17d)SXB1. (CSCee06948)
- When the last client for a multicast group in one VLAN leaves the group, clients joining the same multicast group in other VLANs on the same switch may experience some minor packet loss (up to 20 packets). This problem is resolved in Release 12.2(17d)SXB1. (CSCed95515)
- With correctly configured redundant Supervisor Engine 720s, this erroneous message might be displayed after a reload:
 

```
%PFREDUN-SP-4-BOOTSTRING_INVALID: The bootfile slavebootflash:image_name is not
present in standby
```

 (CSCed93359)
- A [WS-F6700-DFC3A](#) might run out of memory and reload. This problem is resolved in Release 12.2(17d)SXB1. (CSCed89537)
- With IP phones connected to a [WS-X6148-GE-TX](#) switching module that is equipped with a [WS-F6K-GE48-AF](#) power over Ethernet daughtercard, the module might display “Inline Power Module timeout” messages and reset. This problem is resolved in Release 12.2(17d)SXB1. (CSCed87264)
- A group of 8 ports on a [WS-X6548-GE-TX](#) switching module might stop forwarding traffic. This problem is resolved in Release 12.2(17d)SXB1. (CSCed68821)

- Some packet loss might occur when a host sends and receives both bridged traffic and routed traffic through a Layer 3 switch that connects through a nontrunking cross-DFC EtherChannel to a Supervisor Engine 2. This problem is resolved in Release 12.2(17d)SXB1. (CSCed06744)
- When a packet is destined to a next hop that does not have an ARP entry, the packet needs to be sent to the MSFC. When the glean adjacency rate-limiter is enabled, any egress security ACL or egress QoS on the ingress interface is applied to the packets being sent to the MSFC. This problem is resolved in Release 12.2(17d)SXB1. (CSCed75920)
- With a “-p” image, you can configure only 5 VTY lines. This problem is resolved in Release 12.2(17d)SXB1: you can configure 16 VTY lines with a “-p” image. (CSCee37163)
- There is a 2-second delay between the time that a join is sent towards the multicast source and the time that the first packet of the multicast stream is forwarded towards the multicast receiver. This problem is resolved in Release 12.2(17d)SXB1. (CSCee28288)
- A memory leak occurs when you remove ATM virtual circuits (VCs). This problem is resolved in Release 12.2(17d)SXB1. (CSCee04747)
- A reload might occur if management software uses SNMP to copy the running-config file to the startup-config file and then very quickly polls the ccCopyState Object Identifier (OID) repeatedly and without waiting for ccCopyState to return a value, immediately sets the ccCopyEntryRowStatus OID to “destroy” (integer 6). This problem is resolved in Release 12.2(17d)SXB1. (CSCed81154)
- When a Gateway General Packet Radio System (GPRS) Support Node (GGSN) rejects a packet data protocol (PDP) create request due to a Universal Mobile Telecommunication System (UMTS) call admission control failure on an Access Point Name (APN) Manager, the call is torn down instead of attempting to reassign it to another GGSN. This problem is resolved in Release 12.2(17d)SXB1. (CSCed63590)
- Abnormally terminated FTP transfers might cause a small memory leak. This problem is resolved in Release 12.2(17d)SXB1. (CSCec55147)
- With OSPF configured, a memory leak might occur. This problem is resolved in Release 12.2(17d)SXB1. (CSCea80169)
- The Cisco IOS firewall authentication proxy feature might reject a connection. This problem is resolved in Release 12.2(17d)SXB1. (CSCea33481)
- Following switchover to a redundant supervisor engine, any EtherChannels on the newly active supervisor engine are not active and the newly redundant supervisor engine does not enter the standby state. This problem is resolved in Release 12.2(17d)SXB1. (CSCee44248)
- OSPF area border routers (ABRs) might continue to generate summary link-state advertisements (LSAs) for obsolete nonbackbone intra-area routes. This problem is resolved in Release 12.2(17d)SXB1. (CSCee36622)
- Traffic through a port-channel interface that has a Cisco IOS ACL configured might be dropped or switched in software after a reload or after switchover to a redundant supervisor engine or after you enter **shutdown** and **no shutdown** interface commands on a member port. This problem is resolved in Release 12.2(17d)SXB1. (CSCee21772, CSCee32057)
- A small (approximately 180 bytes) memory leak occurs when you delete a logical interface. This problem is resolved in Release 12.2(17d)SXB1. (CSCee05413)
- Receiving Cisco Discovery Protocol (CDP) packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.2(17d)SXB1. (CSCin67568)
- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an intrusion detection system (IDS) signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.2(17d)SXB1. (CSCed35253)

- With an IP multicast router directly connected to both a source and a receiver and when the shortest path tree (SPT) threshold is configured as infinite, (S,G) entries are deleted every minute, which may cause packet loss about once per minute. This problem is resolved in Release 12.2(17d)SXB1. (CSCeb30338)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

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

This advisory is available at

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

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

This problem is resolved in Release 12.2(17d)SXB1. (CSCed93836, CSCdz84583)

- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
Processor, alignment 0
-Process= "CDP Protocol", ipl= 0, pid= 42
-Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
```

This problem is resolved in Release 12.2(17d)SXB1. (CSCdz32659)

## Resolved General Caveats in Release 12.2(17d)SXB

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>.

This problem is resolved in Release 12.2(17d)SXB. (CSCed65778)



- A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

This vulnerability is documented as Cisco bug ID CSCed30113. There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsml.shtml>

This problem is resolved in Release 12.2(17d)SXB. (CSCed30113)

- Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

More details can be found in the security advisory which is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

This problem is resolved in Release 12.2(17d)SXB. (CSCeb56909)

- When you enter the **undebg all** privileged EXEC command, all traffic might stop that passes through an encrypted generic routing encapsulation (GRE) tunnel that is secured via IP Security (IPsec) and that is using Cisco Express Forwarding (CEF) switching. This problem is resolved in Release 12.2(17d)SXB. (CSCec86420)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

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

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>

This problem is resolved in Release 12.2(17d)SXB. (CSCed27956, CSCed38527)

- With Multiprotocol Label Switching (MPLS) configured, after accessing a freed Label Information Base (LIB) entry, this message might be displayed:

```
%TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
```

After the message is displayed, a reload might occur. This problem is resolved in Release 12.2(17d)SXB. (CSCed47409)

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

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

This problem is resolved in Release 12.2(17d)SXB. (CSCdu53656, CSCea28131)

- With Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) or IEEE 802.1s multiple spanning tree (MST), configured, when the root bridge in a spanning tree domain ages out, the remaining bridges reconverge after timing out the root bridge. During this reconvergence, a spanning tree loop might occur. This problem is resolved in Release 12.2(17d)SXB. (CSCed00441)
- In releases where caveat CSCed00441 is resolved and with Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) or IEEE 802.1s, multiple spanning tree (MST) configured, when an edge port goes down, a topology change is generated. This problem is resolved in Release 12.2(17d)SXB. (CSCed63897)
- When the MPLS-LSR-MIB MIB is enabled, and you query the mplsXCTable or a MIB walk occurs, and there are more than 10,000 Multiprotocol Label Switching (MPLS) labels active, the Simple Network Management Protocol (SNMP) agent may use 99 percent of the MSFC CPU bandwidth for an arbitrarily long time (hours or days), without necessarily generating CPUHOG errors. This situation causes other processes on the router to fail because these processes do not receive the CPU bandwidth that they require:
  - Routes may time out.
  - Tunnels may go down.
  - Accessing the router via a Telnet connection to a network port may become impossible.
  - The command-line interface (CLI) through the console line may become quite slow to respond.

The output of the **show snmp summary** EXEC command may indicate that the number of requests is “N” while the number of replies that were sent is “N-1.” The output of the **show processes cpu | include SN** EXEC command may indicate that the SNMP process uses 99 percent of the CPU bandwidth of the RP. (CSCea60559)

- With a PFC2 and with EtherChannels configured to include interfaces on different DFC-equipped switching modules, ARP traffic from a [WS-X6066-SLB-APC](#) Content Switching Module (CSM) that is running software version 3.2(2) and earlier might not be forwarded correctly. This problem is resolved in Release 12.2(17d)SXB. (CSCed35745)
- The **show power** command might incorrectly display a redundant Supervisor Engine 2 as a Supervisor Engine 1. This problem is resolved in Release 12.2(17d)SXB. (CSCdy56620)
- RSPAN fails to filter a destination VLAN from a source trunk port. This problem is resolved in Release 12.2(17d)SXB. (CSCec70454)
- WS-6516-GBIC with a DFC3A and WS-6816-GBIC do not support jumbo frame traffic on EtherChannels that have member ports on different DFC-equipped modules. This problem is resolved in Release 12.2(17d)SXB. (CSCed55342)
- When Border Gateway Protocol (BGP) uses multihome interfaces to peer with the neighbors that are part of the same peer group or the same update group, and you enter the neighbor next-hop-self router configuration command on routers of a peer group, the next-hop calculation is performed only on the first member of the peer group, and the same next-hop value is replicated to the rest of the peers instead of calculating the next hop based on the next-hop-self configuration. This problem is resolved in Release 12.2(17d)SXB. (CSCec14415)

- With a PFC3A, OSPF adjacencies fail to form following a reload with MPLS configured on more than one interface, and a static route for a connected subnet pointing to the null0 interface with an administrative distance of 254. This problem is resolved in Release 12.2(17d)SXB. (CSCed62337)
- With fall-back bridging configured, ARP fails after a switchover to the redundant supervisor engine. This problem is resolved in Release 12.2(17d)SXB. (CSCed61632)
- After a few days of running time, the **show environment temperature** command does not display current values. This problem is resolved in Release 12.2(17d)SXB. (CSCed49423)
- A VLAN with no active ports might not be shut down correctly. This problem is resolved in Release 12.2(17d)SXB. (CSCed47381)
- DLSw might not work. This problem is resolved in Release 12.2(17d)SXB. (CSCed40129)
- A small buffers pool memory leak might cause a reload. This problem is resolved in Release 12.2(17d)SXB. (CSCed34788)
- A memory leak causes an “IPC Failure” message and NDE stops exporting. This problem is resolved in Release 12.2(17d)SXB. (CSCed33380)
- The entPhysicalSerialNum MIB object in the Entity MIB is not providing the serial number for XENPAK modules. This problem is resolved in Release 12.2(17d)SXB. (CSCed30061)
- Fall-back bridging might not work. This problem is resolved in Release 12.2(17d)SXB. (CSCed29594)
- The [WS-X6816-GBIC](#) switching module might report a minor error after a reload and require OIR before it can be used. This problem is resolved in Release 12.2(17d)SXB. (CSCed05332)
- Occasionally following a reload, the IDPROM is not read correctly on a [WS-X6548-RJ-45](#) switching module that is equipped with a DFC, which holds the module in the “other” state. This problem is resolved in Release 12.2(17d)SXB. (CSCed04988)
- A Supervisor Engine 2 configured with the Cisco IOS SLB RADIUS Load Balancing (RLB) feature might reload unexpectedly because of a bus error at an illegal address when you make changes to the Cisco IOS Server Load Balancing (SLB) configuration. This problem is resolved in Release 12.2(17d)SXB. (CSCec55377)
- VACLs do not work on routed RSPAN traffic. This problem is resolved in Release 12.2(17d)SXB. (CSCeb61695)
- In the presence of faulty hardware, continuous reloads might follow display of an “SLCP Not Responding” message. This problem is resolved in Release 12.2(17d)SXB. (CSCea57452)
- A bus error might cause an indefinite pause on a Multiprotocol Label Switching (MPLS) provider edge (PE) router. This problem is resolved in Release 12.2(17d)SXB. (CSCeb77038)
- With a route in a different VPN routing and forwarding instance (VRF) attached to an interface, the interface might not be able to receive traffic being sent to an address that is configured on the MSFC. This problem is resolved in Release 12.2(17d)SXB. (CSCeb52270)
- A reload might occur when Border Gateway Protocol (BGP) is configured to carry Virtual Private Network version 4 (VPNv4) routes and VPNv4 import processing occurs when a BGP neighbor resets. This problem is resolved in Release 12.2(17d)SXB. (CSCeb17467)
- With multiple Frame Relay DLCIs attached to the same virtual-template interface and with distributed Link Fragmentation and Interleaving over Frame Relay (dLFIoFR) enabled, a reload might occur if you enter the **no encapsulation frame-relay** command on the physical interface. With multiple ATM PVCs attached to the same multilink virtual-access interface, a reload might occur if you remove the ATM PVC when the dLFI Virtual-Access interface is still up. This problem is resolved in Release 12.2(17d)SXB. (CSCin66010)

- To avoid a reload, do not enter the **no crypto map gre** command on a physical interface. This problem is resolved in Release 12.2(17d)SXB. (CSCed51674)
- With IPv6 CEF enabled, a reload might occur if IPv6 encounters a routing loop. This problem is resolved in Release 12.2(17d)SXB. (CSCed20042)
- If the **passive-interface default** router configuration command is enabled and you enter the **no passive-interface** *interface\_type interface\_number* router configuration command, the Routing Information Protocol (RIP) might not send updates through an interface that are configured for Virtual Private Networking (VPN). This problem is resolved in Release 12.2(17d)SXB. (CSCec44556)
- If you configure aggressive OSPF hello timers and dead timers, then during periods of high CPU utilization, OSPF packets are not processed, resulting in OSPF declaring OSPF neighbors to be inoperative (“down”). This problem is resolved in Release 12.2(17d)SXB. (CSCec42160)
- A **PA-A3-8T1IMA** port adapter might drop packets with a certain unknown pattern. This problem is resolved in Release 12.2(17d)SXB. (CSCeb56457)
- A reload might occur when generic routing encapsulation (GRE) packets are received through a GRE tunnel and forwarded as Multiprotocol Label Switching (MPLS) packets. This problem is resolved in Release 12.2(17d)SXB. (CSCeb36929)
- Occasionally a bus error and reload might occur if an MPLS packet triggers the sending of an Internet Control Message Protocol (ICMP) packet. This problem is resolved in Release 12.2(17d)SXB. (CSCeb27452)
- The core router Multiprotocol Label Switching (MPLS) forwarding entry has the correct outgoing interface but has an incorrect label to use for sending traffic to the edge router. The incorrect label is identical to the label that is sent by another core router for the same prefix through another interface. This problem is observed in a service provider network when the route to the prefix that has the incorrect MPLS forwarding entry is configured using a static recursive route and the specific IP address that is specified in the **ip route** *prefix mask ip\_address* global configuration command is changed by topology changes to go through a different adjacent router. The incorrect outgoing Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP) label corresponds to the router that was adjacent prior to the routing change. This problem is resolved in Release 12.2(17d)SXB. (CSCeb05519)
- With a Supervisor Engine 2, when a fabric-capable line card comes online and an RSPAN source session is configured, the RSPAN source session might stop working. When this happens, the traffic being monitored will not be replicated on the RSPAN VLAN. This problem is resolved in Release 12.2(17d)SXB. (CSCin61989)
- Traffic might flow in only one direction after assigning a LAN port to a different VLAN. This problem is resolved in Release 12.2(17d)SXB. (CSCed20566)
- Gigabit Ethernet negotiation does not work. This problem is resolved in Release 12.2(17d)SXB. (CSCed19431)
- Occasionally, the nvram:/startup-config file cannot be read. This problem is resolved in Release 12.2(17d)SXB. (CSCed06462)
- With VLAN aging configured, the routed MAC (RM) bit might be set on the Layer 2 entries for routed traffic, which causes the entries to be purged every 5 minutes. One packet might be flooded and relearned for each purged entry. This problem is resolved in Release 12.2(17d)SXB. (CSCec43605)

- Do not configure a VLAN used with one subinterface on another subinterface. This problem is resolved in Release 12.2(17d)SXB. (CSCed19336)
- An SNMP query to retrieve the policy maps attached to an interface that has multiple policy maps attached aggregates the policy maps into a display showing only one policy map. This problem is resolved in Release 12.2(17d)SXB. (CSCec72502)
- Ingress policing does not work on an interface configured to support MPLS. This problem is resolved in Release 12.2(17d)SXB. (CSCed36000, CSCin61428)
- You might see a traceback message if an MST instance loses its root port. If you have configured single router mode with stateful switchover (SRM with SSO) redundancy mode, an unnecessary synchronization of the root port information might occur. This problem is resolved in Release 12.2(17d)SXB. (CSCed30292)
- With UplinkFast configured, if the root port goes down and the alternate root port becomes the root port and the original root port comes back up, and then an SSO with SRM switchover occurs before the delay timer expires, the original root port remains in the blocking state until you enter **shutdown** and **no shutdown** commands. This problem is resolved in Release 12.2(17d)SXB. (CSCed10816)
- The **show tech support command** does not execute correctly. This problem is resolved in Release 12.2(17d)SXB. (CSCed31353)
- MST supports a total of 30,000 logical interfaces. This problem is resolved in Release 12.2(17d)SXB. (CSCed33864)
- Trunk configuration using the following MIB objects on access ports does not work. When each MIB object is set, the previously configured MIB objects are cleared:
  - vlanTrunkPortVlansEnabled
  - vlanTrunkPortVlansEnabled2k
  - vlanTrunkPortVlansEnabled3k
  - vlanTrunkPortVlansEnabled4k

This problem is resolved in Release 12.2(17d)SXB. (CSCed30335)

- If a single router mode with stateful switchover (SRM with SSO) switchover occurs when an interface is shut down that had ACLs or ACL features configured on it when it was in an admin up state, the newly active TCAM will have entries for the shutdown interface, which might result in TCAM exceptions if you apply features to active interfaces. This problem is resolved in Release 12.2(17d)SXB. (CSCed19296, CSCed15472)
- To avoid a reload, do not remove any interfaces that have IPv6 features configured (for example, an IPv6 ACL) or revert any interfaces that have IPv6 features configured to the default configuration. This problem is resolved in Release 12.2(17d)SXB. (CSCec74016)
- High-volume SNMP traffic might cause a reload. This problem is resolved in Release 12.2(17d)SXB. (CSCed79519)
- A [WS-X6748-GE-TX](#) module in slot 1 does not support speeds of 10 Mbps or 100 Mbps. This problem is resolved in Release 12.2(17d)SXB. (CSCed38862)

## FlexWAN Module Caveats in Release 12.2(17d)SXB and Rebuilds

- [Open FlexWAN Module Caveats in Release 12.2\(17d\)SXB11a, page 398](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB11a, page 398](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB11, page 398](#)

- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB10](#), page 398
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB9](#), page 398
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB8](#), page 399
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB7](#), page 399
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB6](#), page 399
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB5](#), page 400
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB4](#), page 400
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB3](#), page 400
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB2](#), page 400
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB1](#), page 401
- [Resolved FlexWAN Module Caveats in Release 12.2\(17d\)SXB](#), page 401

### Open FlexWAN Module Caveats in Release 12.2(17d)SXB11a

- With high-volume traffic flowing between the interfaces in the two bays of a WS-X6582-2PA Enhanced FlexWAN module, you might see “%CWAN\_RP-4-SEMAHOG” messages. (CSCed08264)




---

**Note** CSCed08264 is not seen in later releases.

---

- A FlexWAN module might reload if you configure distributed multilink Frame Relay (FRF.16). (CSCin68433, CSCef19220)




---

**Note** CSCin68433 and CSCef19220 are not seen in later releases.

---

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB11a

None.

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB11

None.

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB10

None.

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB9

None.



## Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB8

- Under a high traffic load, a [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) port adapter might display an increasing rx\_no\_buffer counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter might stop receiving traffic.

**Workaround:** Enter the **shutdown** and **no shutdown** interface configuration commands on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter or reset the FlexWAN module. This problem is resolved in Release 12.2(18)SXE. (CSCin77553)

- With a WS-X6582-2PA Enhanced FlexWAN module and PA-MC-4T1 or [PA-POS-OC3](#) port adapters, ignore any “MajFail Error” startup diagnostic messages. This problem is resolved in Release 12.2(18)SXD1. (CSCin76828, CSCef04875)
- On FlexWAN module ATM interfaces and subinterfaces, service policies applied to a virtual template do not take effect.

**Workaround:** Enter **shutdown** and **no shutdown** commands for the ATM interface. This problem is resolved in Release 12.2(18)SXD. (CSCed58116, CSCee94391)

## Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB7

- The distributed Weighted Fair Queuing (dWFQ) **fair-queue** interface command is not saved in the running-config file. This problem is resolved in Release 12.2(17d)SXB7. (CSCed51640)
- If you configure distributed link fragmentation and interleaving (dLFI) over a leased line, Multilink PPP (MLP), and QoS, a FlexWAN module might reload if you remove a service policy from a multilink interface or when a member link is removed from the multilink interface while heavy traffic is being processed. This problem is resolved in Release 12.2(17d)SXB7. (CSCee72906)
- With a multilink interface configured for fragmentation and interleaving, traffic loss might occur following an RPR+ switchover. With a multilink interface that has members from non-channelized port adapters, traffic loss might occur if any of the member links goes up and down. This problem is resolved in Release 12.2(17d)SXB7. (CSCeg57219)
- Routing protocol hello and update packets and ATM operation and maintenance (OAM) packets might be dropped if a FlexWAN egress interface is congested. This problem is resolved in Release 12.2(17d)SXB7. (CSCin76078)
- With Multilink Frame Relay (FRF.16) configured on bundled FlexWAN serial links, traffic loss occurs for packets smaller than 512 bytes. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa47020)
- With an Enhanced FlexWAN module, you might see “Hyperion Transmit packet header crc error” messages. This problem is resolved in Release 12.2(17d)SXB7. (CSCin87976)

## Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB6

- When you modify the configuration of a serial interface, you might see messages similar to these:

```
%INTERFACE_API-3-NODESTROYSUBBLOCK: The HWIDB subblock named COPS_PR was not removed
-Traceback=
```

This problem is resolved in Release 12.2(17d)SXB6. (CSCin65698)

- When you send larger than fragment-sized packets from a multilink interface that has a traffic-shaping class configured and that is configured for fragmentation, traffic loss occurs when the queue size increases to the queue limit. This problem is resolved in Release 12.2(17d)SXB6. (CSCef66517)

- The **PA-2T3+** port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.2(17d)SXB6. (CSCee70591)
- The **PA-MC-2T3+** port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.2(17d)SXB6. (CSCee49862)
- In releases where caveat CSCec15517 is resolved, permanent virtual circuits (PVCs) might be unstable. This problem is resolved in Release 12.2(17d)SXB6. (CSCee22810)
- Packet-over-SONET (POS) Automatic Protection Switching (APS) does not work on **PA-MC-STM-1** port adapters. This problem is resolved in Release 12.2(17d)SXB6. (CSCef49330)

#### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB5

- Following a reload, modular QoS CLI (MQC) MPLS CoS classification does not work. This problem is resolved in Release 12.2(17d)SXB5. (CSCed35900)
- 1,500-byte pings fail on a **PA-A3** ATM subinterface configured for MPLS and configured with the **ip mtu 1500** command. This problem is resolved in Release 12.2(17d)SXB5. (CSCef91994)
- With a Supervisor Engine 2, you might see a “hardware TCAM entry capacity exceeded message” if you configure a security ACL and a policy route map on a FlexWAN module POS interface. This problem is resolved in Release 12.2(17d)SXB5. (CSCef13797)
- Following a reload, modular QoS CLI (MQC) MPLS CoS classification does not work. This problem is resolved in Release 12.2(17d)SXB5. (CSCed35900)

#### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB4

- When other modules have large configurations, an E1 controller on a **PA-MC-8TE1+** port adapter might not be active following a reload. This problem is resolved in Release 12.2(17d)SXB4. (CSCin78110)
- With a PFC3, the **set mpls exp** command does not work in a service policy applied to ingress FlexWAN or Enhanced FlexWAN module interfaces. This problem is resolved in Release 12.2(17d)SXB4. (CSCee44637)

#### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB3

- With an Enhanced FlexWAN module, “EOS-RESET” messages might be followed by “HYPERION-RESET” messages. This problem is resolved in Release 12.2(17d)SXB3. (CSCef25710)
- On FlexWAN interfaces, you cannot configure policers with rates less than 32,000 bps. This problem is resolved in Release 12.2(17d)SXB3. (CSCef05966)
- With QoS configured on FlexWAN ports, spurious memory accesses and alignment errors might occur. This problem is resolved in Release 12.2(17d)SXB3. (CSCed69233)

#### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB2

- Packets sent internally on a WS-X6582-2PA Enhanced FlexWAN Module might have invalid CRC checksums. This problem is resolved in Release 12.2(17d)SXB2. (CSCee86930, CSCee42391)
- You can attach a service policy that contains invalid configuration to an interface. If you apply a Frame Relay map class with both input policing and output queuing to a DLCI twice, the FlexWAN module might reload. This problem is resolved in Release 12.2(17d)SXB2. (CSCin52060)



- Multilink Frame Relay (MFR) interface member links that were added after first link do not work. This problem is resolved in Release 12.2(17d)SXB2. (CSCin72180)
- The line protocol of a multilink Frame Relay (MFR) interface on a [PA-MC-2T3+](#) port adapter might go down if you enter **shutdown** and **no shutdown** commands on the MFR interface. This problem is resolved in Release 12.2(17d)SXB2. (CSCin75779)
- With distributed MultiLink PPP (MLP) configured on a FlexWAN module, the module might reload if the peer interface is reloaded while traffic is flowing. This problem is resolved in Release 12.2(17d)SXB2. (CSCin75771)
- With sustained WS-X6582-2PA enhanced FlexWAN module maximum CPU utilization, egress traffic might be dropped, including control traffic, which might cause interfaces to go down and back up. This problem is resolved in Release 12.2(17d)SXB2. (CSCee53705)
- On a WS-X6582-2PA enhanced FlexWAN module, traffic in a priority class might experience high latency or packet loss. This problem is resolved in Release 12.2(17d)SXB2. (CSCeb58952)
- When a [PA-MC-2T3+](#) port adapter with an unchannelized configuration and with a service policy attached is carrying a high volume of 64-byte packets, buffer leakage might occur. This situation might cause ping failures or very long packet delays. This problem is resolved in Release 12.2(17d)SXB2. (CSCee31618)
- With a Frame Relay permanent virtual circuit (PVC) policy configured, a reload might occur when you enter the **show policy-map interface EXEC** command. This problem is resolved in Release 12.2(17d)SXB2. (CSCec15517)

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB1

- The WS-X6582-2PA Enhanced FlexWAN module might be reset periodically. This problem is resolved in Release 12.2(17d)SXB1. (CSCee33103)
- If you repeatedly add and remove an ingress service policy from a FlexWAN interface, a policer in an egress service policy on the same interface might stop counting packets. This problem is resolved in Release 12.2(17d)SXB1. (CSCee23845)

### Resolved FlexWAN Module Caveats in Release 12.2(17d)SXB

- Operation, Administration, and Maintenance (OAM) permanent virtual circuits (PVC) on [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) interfaces are not active after an OIR. This problem is resolved in Release 12.2(17d)SXB. (CSCin65182)
- In releases where CSCdz32751 is resolved, ignore error messages about Cisco IOS fair queuing being disabled on low-speed serial interfaces. This problem is resolved in Release 12.2(17d)SXB. (CSCec28505)
- On a [PA-A3](#) port adapter with dCBWFQ configured, when one bandwidth class is congested, there might be extra latency in another bandwidth class that is not congested. This problem is resolved in Release 12.2(17d)SXB. (CSCeb61825)
- When a Tributary Unit Alarm Indication Signal (TU-AIS) is inserted for an E1 tributary on a [PA-MC-STM-1](#) port adapter in a Synchronous Payload Envelope (SPE), packet corruption might occur on the adjacent E1. This problem is resolved in Release 12.2(17d)SXB. (CSCea66218)
- MPLS on the FlexWAN module does not support Virtual Private LAN Service (VPLS). To avoid a reload, do not use a network topology where MPLS on the FlexWAN module receives VPLS traffic. This problem is resolved in Release 12.2(17d)SXB. (CSCed35405)

## Service Module Caveats in Release 12.2(17d)SXB and Rebuilds

- [Open Service Module Caveats in Release 12.2\(17d\)SXB11a](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB11a](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB11](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB10](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB9](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB8](#), page 402
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB7](#), page 403
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB6](#), page 403
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB5](#), page 403
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB4](#), page 403
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB3](#), page 404
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB2](#), page 404
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB1](#), page 404
- [Resolved Service Module Caveats in Release 12.2\(17d\)SXB](#), page 404

### Open Service Module Caveats in Release 12.2(17d)SXB11a

None.

### Resolved Service Module Caveats in Release 12.2(17d)SXB11a

- You might be unable to access an Multi-Processor WAN Application Module (MWAM) through a console or Telnet session for 10 minutes after the module has been reloaded.

**Workaround:** Configure the **ip rcmd rcp-enabled** command.

This problem is resolved in Release 12.2(17d)SXB11a. (CSCsa50215)

### Resolved Service Module Caveats in Release 12.2(17d)SXB11

None.

### Resolved Service Module Caveats in Release 12.2(17d)SXB10

None.

### Resolved Service Module Caveats in Release 12.2(17d)SXB9

None.

### Resolved Service Module Caveats in Release 12.2(17d)SXB8

- Rivest, Shamir, and Adelman (RSA) signature authentication on the IPsec VPN Acceleration services module (**WS-SVC-IPSEC-1**) does not support upper-case (A through Z) peer certificate URLs. This problem is resolved in Release 12.2(17d)SXB8. (CSCsa81928)

- When you enroll a Supervisor Engine 2 with a certification authority (CA) server and you request that the serial number be included with the subject name of the certificate, the serial number is incorrect in the certificate-signing request (CSR) and in the certificate. This problem is resolved in Release 12.2(17d)SXB8. (CSCsa67272)
- After an SRM with SSO redundancy mode switchover, SPAN does not forward packets to service modules. This problem is resolved in Release 12.2(17d)SXB8. (CSCeh21723)
- There is local cache support for only one certificate revocation list (CRL). This problem is resolved in Release 12.2(17d)SXB8. (CSCeh18999)
- With an IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) configured for Rivest, Shamir, and Adelman (RSA) signature authentication, if the certificate distribution point (CDP) in the peer certificate does not have the hostname or IP address of the lightweight directory access protocol (LDAP) CRL server, all Internet Key Exchange (IKE) negotiation fails and the Internet Key Management Protocol (IKMP) process might be blocked indefinitely because the CRL cannot be fetched. This problem is resolved in Release 12.2(17d)SXB8. (CSCsa78580)
- The trunk connection to a [WS-X6066-SLB-APC](#) Content Switching Module (CSM) carries VLANs that are not used by the CSM. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg41623)

### Resolved Service Module Caveats in Release 12.2(17d)SXB7

- With a Supervisor Engine 720, service modules might experience connectivity problems if there are any Layer 2 EtherChannels configured with member ports on different DFC-equipped switching modules. With a Supervisor Engine 720 in bus fabric switching mode, service modules might experience connectivity problems if there are any Layer 2 EtherChannels. This problem is resolved in Release 12.2(17d)SXB7. (CSCee10005)



**Note** With Release 12.2(17d)SXB7 and rebuilds, you can use the **fabric switching-mode force bus-mode** command to avoid the bus fabric switching mode. See the Release 12.2SX command reference for more information.

- Some loss might occur in traffic from a service module that crosses the switch fabric. This problem is resolved in Release 12.2(17d)SXB7. (CSCee68381)

### Resolved Service Module Caveats in Release 12.2(17d)SXB6

- With a VPN module, a reload might occur if you nest more than one GRE tunnel through an IPsec tunnel. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg09655)
- If you reset a [WS-X6066-SLB-APC](#) Content Switching Module (CSM), other modules might also reset. This problem is resolved in Release 12.2(17d)SXB6. (CSCed25505)

### Resolved Service Module Caveats in Release 12.2(17d)SXB5

- A reload might occur if you enter the **mls ip ids acl\_name** command. This problem is resolved in Release 12.2(17d)SXB5. (CSCef53290)
- An IPsec VPN Acceleration Services Module configured for GRE over IPsec might stop passing traffic through the GRE tunnels. This problem is resolved in Release 12.2(17d)SXB5. (CSCef65827)

### Resolved Service Module Caveats in Release 12.2(17d)SXB4

None.

### Resolved Service Module Caveats in Release 12.2(17d)SXB3

- Following an SSO switchover, a [WS-SVC-IDS-M2-K9](#) Intrusion Detection System Module 2 might not detect attacks. This problem is resolved in Release 12.2(17d)SXB3. (CSCef14106)

### Resolved Service Module Caveats in Release 12.2(17d)SXB2

- SPAN configured to send traffic to a service module fails after a switchover to the redundant supervisor engine if the service module changes to the “bus” switching mode. This problem is resolved in Release 12.2(17d)SXB2. (CSCee62630)

### Resolved Service Module Caveats in Release 12.2(17d)SXB1

- With a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) installed, nested IPsec traffic is decapsulated incorrectly. This problem is resolved in Release 12.2(17d)SXB1. (CSCed85276)
- With the Rapid Spanning Tree protocol (RSTP) enabled, resetting a [WS-SVC-MWAM-1](#) or a [WS-SVC-CSG-1](#) results in loss of connectivity between the supervisor engine and other WS-SVC-MWAM-1 modules and subsequent Cisco IOS SLB probe failure between supervisor engines running Cisco IOS SLB and WS-SVC-MWAM-1 modules running GPRS gateway support node (GGSN) or Service Selection Gateway (SSG) software in a load-balanced environment. This problem is resolved in Release 12.2(17d)SXB1. (CSCin74475)

### Resolved Service Module Caveats in Release 12.2(17d)SXB

- A traceback occurs if you enter the keepalive interface command on a tunnel with IPsec on both sides. This problem is resolved in Release 12.2(17d)SXB. (CSCec90162)
- With a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)), a reload might occur when there is a large number of GRE tunnels that are accelerated by the VPN module and that egress through the same VLAN interface and when, in a short period of time, changes are made to the crypto map that is attached to the VLAN interface or when a crypto map is attached or detached from the VLAN interface repeatedly in a short period of time. This problem is resolved in Release 12.2(17d)SXB. (CSCed62866)
- A memory leak might occur with a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) serving a large number of EZVPN clients when the clients frequently disconnect and reconnect. This problem is resolved in Release 12.2(17d)SXB. (CSCed58110)
- If you add a dynamic crypto map to an existing crypto map that has static entries without removing the crypto map from the interface, the reverse route injection route for the VPN clients gets deleted immediately after it is installed. This problem is resolved in Release 12.2(17d)SXB. (CSCed22494)
- With dynamic crypto maps configured and with reverse route injection enabled, reverse route injection routes incorrectly are not deleted. This problem is resolved in Release 12.2(17d)SXB. (CSCea80003)
- To avoid reloads, do not configure the single router mode with stateful switchover (SRM with SSO) redundancy mode with a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) installed. This problem is resolved in Release 12.2(17d)SXB. (CSCed17605)
- A grouping of two active IPsec VPN Acceleration services modules ([WS-SVC-IPSEC-1](#)) that are failover partners is called a blade failover group (BFG). If you OIR or administratively disable a VPN module that does not have a failover partner, the BFG configuration may be inconsistent. The workaround for this problem is to remove the module from the BFG and add it back to the BFG. A similar problem may occur when a VPN module is removed physically from the chassis and the

chassis is reloaded but the BFG configuration is not removed. The workaround for this problem is to remove the BFG from the configuration, save the configuration change to the startup configuration, and reload the chassis. This problem is resolved in Release 12.2(17d)SXB. (CSCed19505)

- In a blade failover group (BFG) with 2 IPsec VPN Acceleration services modules ([WS-SVC-IPSEC-1](#)) where the active VPN module has all the crypto connections configured, if you power down the active VPN module, save the configuration, and do a reload, the traffic may not go through the standby VPN module. This problem is resolved in Release 12.2(17d)SXB. (CSCed22645)

## OSM Caveats in Release 12.2(17d)SXB and Rebuilds

- [Open OSM Caveats in Release 12.2\(17d\)SXB11a, page 405](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB11a, page 405](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB11, page 405](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB10, page 405](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB9, page 405](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB8, page 406](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB7, page 406](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB6, page 406](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB5, page 407](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB4, page 407](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB3, page 407](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB2, page 407](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB1, page 408](#)
- [Resolved OSM Caveats in Release 12.2\(17d\)SXB, page 408](#)

### Open OSM Caveats in Release 12.2(17d)SXB11a

None.

### Resolved OSM Caveats in Release 12.2(17d)SXB11a

None.

### Resolved OSM Caveats in Release 12.2(17d)SXB11

None.

### Resolved OSM Caveats in Release 12.2(17d)SXB10

None.

### Resolved OSM Caveats in Release 12.2(17d)SXB9

- Changing the MTU size on a port might not change the MPLS MTU size.

**Workaround:** Enter **shutdown** and **no shutdown** commands after configuring an MTU size on a port. This problem is resolved in Release 12.2(17d)SXB9. (CSCed17226, CSCed33822)

- Rate counters for the Gigabit Ethernet WAN module always read a value of zero even though traffic is flowing. This problem is resolved in Release 12.2(18)SXB9. (CSCsb18038)

### Resolved OSM Caveats in Release 12.2(17d)SXB8

- MPLS traffic from the MSFC, for example, ping or Service Assurance Agent (SAA) traffic, is not enqueued correctly on [OSM-2+4GE-WAN+](#) egress ports. Because the traffic is not in the correct egress queue, incorrect QoS policies are applied to the traffic. This problem is resolved in Release 12.2(17d)SXB8. (CSCeg77503)
- There is no customer-edge (CE) router to provider-edge (PE) router connectivity if you configure a multiple link point-to-point protocol (MLPPP) interface on an [OSM-12CT3/T1](#) or [OSM-1CHOC12/T1-SI](#) in the CE-PE link. This problem is resolved in Release 12.2(17d)SXB8. (CSCef19811)
- Disposition packets that are index-directed from a core-facing OSM are not passed to a CE-facing channelized OSM. This problem is resolved in Release 12.2(17d)SXB8. (CSCeh29617)
- [OSM-1CHOC12](#) modules become unresponsive and are power cycled. This problem is resolved in Release 12.2(17d)SXB8. (CSCee45508)
- Port 1/7 ingress traffic is dropped if the egress port is on an OSM. This problem is resolved in Release 12.2(17d)SXB8. (CSCeh05310)

### Resolved OSM Caveats in Release 12.2(17d)SXB7

- With an OSM, you might see these messages:

```
%EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR: EARL L2 ASIC #0: L2L3 Mismatch seq #0x1306
%EARL_L2_ASIC-SP-3-INTR_WARN: EARL L2 ASIC 0: Non-fatal interrupt l2l3_seq_mismatch
%CWTLIC-3-MEDUSA_FATAL: OSM Medusa ASIC Fatal Error. ERROR CODE: 3, 62,
```

This problem is resolved in Release 12.2(17d)SXB7. (CSCeg03144)

- The [OSM-2OC12-ATM](#) module drops IPX traffic. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa47099)
- An OSM might reload when traffic levels are high and the traffic includes many large packets. This problem is resolved in Release 12.2(17d)SXB7. (CSCsa53708)

### Resolved OSM Caveats in Release 12.2(17d)SXB6

- Egress OSM port policing might drop ISIS routing control packets. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg49010)
- Some OSM virtual circuits (VCs) might not pass any traffic following switchover to a redundant Supervisor Engine 2. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg40543)
- When the VLAN interfaces are unstable at both ends of a Virtual Private LAN Service (VPLS) virtual circuit (VC), both ends try to reinitialize the VPLS VC. The initialization attempts conflict and prevent reestablishment of the VPLS VC. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg30437)
- Some VPLS VCs fail to pass traffic after a link failure in the core network. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg16684)
- With an OSM configuration that includes a large number of subinterfaces and with aggregate policing configured on all OSM ports, following a reload, queuing on the OSMs might not initialize correctly. This situation causes traffic loss. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg11415)

- For a GE-WAN interface priority queue, you cannot add additional match criteria to a class map that is configured with the **match mpls** command. This problem is resolved in Release 12.2(17d)SXB6. (CSCeg24675)

- With OSM serial interfaces configured, you might see these messages:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 65535
-Process= "<interrupt level>", ipl= 1
-Traceback= 4021F160 402E3BCC 40E9CA28 40E90E68 402D545C 40294A0C
```

This problem is resolved in Release 12.2(17d)SXB6. (CSCed82736)

- An OSM might not report the default QoS class statistics if the default class is not explicitly configured. This problem is resolved in Release 12.2(17d)SXB6. (CSCef79592)
- When configured as an 802.1q trunk port, the Layer 2 LAN ports on OSMs do not allow for the 802.1q tag when counting packets as giants. This problem is resolved in Release 12.2(17d)SXB6. (CSCef74227)

### Resolved OSM Caveats in Release 12.2(17d)SXB5

- If you configure 802.1Q tunneling on a LAN port and 802.1Q-tunnel bridging on an [OSM-2OC12-ATM-SI+](#) subinterface, the OSM might reload. This problem is resolved in Release 12.2(17d)SXB5. (CSCef35398)
- When deleting and re-adding channels on an [OSM-12CT3/T1](#) T1 interface, the SNMP ifindex disappears. This problem is resolved in Release 12.2(17d)SXB5. (CSCef70298)
- When any interface on an [OSM-12CT3/T1](#) goes down, ping traffic to a directly connected router might experience high latency. This problem is resolved in Release 12.2(17d)SXB5. (CSCef47466)
- A GE-WAN subinterface configured for MPLS might stop forwarding traffic. This problem is resolved in Release 12.2(17d)SXB5. (CSCef72205)

### Resolved OSM Caveats in Release 12.2(17d)SXB4

None.

### Resolved OSM Caveats in Release 12.2(17d)SXB3

- Reloads might not be successful with a large number (for example, 500) of subinterfaces configured on a GE-WAN port. This problem is resolved in Release 12.2(17d)SXB3. (CSCee42657)

### Resolved OSM Caveats in Release 12.2(17d)SXB2

- OSMs might reset following OIR of another module or switchover to the redundant supervisor engine. This problem is resolved in Release 12.2(17d)SXB2. (CSCed93022)
- With high CPU utilization and line-rate traffic, byte counters on OC-48 interfaces might be wrong. This problem is resolved in Release 12.2(17d)SXB2. (CSCee84887)
- Ingress traffic in tunnels with a destination address on an [OSM-4GE-WAN-GBIC](#) interface is dropped after approximately 75 packets have been received. This problem is resolved in Release 12.2(17d)SXB2. (CSCee79403)
- With a Supervisor Engine 720, LDP, EIGRP, and OSPF control protocols on non-Ethernet OSM interfaces are unstable without any traffic. This problem is resolved in Release 12.2(17d)SXB2. (CSCee69426)



- The **bandwidth** command does not work correctly on OSM ATM subinterfaces. This problem is resolved in Release 12.2(17d)SXB2. (CSCee65478)
- [OSM-2+4GE-WAN+](#) ports do not automatically adjust the MTU size to accommodate tagged traffic. Ingress tagged packets destined for the MSFC are dropped if the packet size is larger than the ingress interface MTU size. This problem is resolved in Release 12.2(17d)SXB2. (CSCee59667)
- Traffic loss might occur on OSMs when there are frequent OIRs. This problem is resolved in Release 12.2(17d)SXB2. (CSCee54642)
- With a redundant supervisor engine, entering a **no bridge-enable** interface command on an OSM POS interface causes tracebacks. This problem is resolved in Release 12.2(17d)SXB2. (CSCee52639)
- With the **mac-address-limit** command configured on both LAN and WAN ports (for example, with VPLS), traffic that has been limited and flooding disabled still floods out WAN ports that belong to the same bridge. This problem is resolved in Release 12.2(17d)SXB2. (CSCee04176)
- The interfaces on an [OSM-2+4GE-WAN+](#) module might be reported as administratively up/up when there is no GBIC installed. This problem is resolved in Release 12.2(17d)SXB2. (CSCee35867)
- The Gigabit Ethernet LAN ports on a [OSM-2+4GE-WAN+](#) module might be reported as administratively up/up when there is a GBIC installed but no cable attached. This problem is resolved in Release 12.2(17d)SXB2. (CSCee01868)
- Occasionally, [OSM-2+4GE-WAN+](#) module interfaces do not pass traffic after a reload or OIR. This problem is resolved in Release 12.2(17d)SXB2. (CSCed83227)
- With CRC32 configured on OSM interfaces, priority queues have high latency with line-rate traffic. This problem is resolved in Release 12.2(17d)SXB2. (CSCec62800)

#### Resolved OSM Caveats in Release 12.2(17d)SXB1

- OSM interface byte counts might be incorrect after a few hours of traffic handling. High traffic levels on OC-48 interfaces might produce incorrect byte counts. This problem is resolved in Release 12.2(17d)SXB1. (CSCee55056)
- With EoMPLS or Virtual Private LAN Service (VPLS) configured and with the **xconnect** interface configuration command on a VLAN interface and a GE-WAN interface as the MPLS uplink, the GE-WAN interface input counters are inaccurate. This problem is resolved in Release 12.2(17d)SXB1. (CSCed48085)

#### Resolved OSM Caveats in Release 12.2(17d)SXB

- On [OSM-2+4GE-WAN+](#) modules, the **ip mtu** interface command fails to increase the MTU from the size set with the **mtu** interface command. This problem is resolved in Release 12.2(17d)SXB. (CSCec03984)

## Caveats in Release 12.2(17b)SXA and Rebuilds

- [General Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 409](#)
- [FlexWAN Module Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 416](#)
- [Service Module Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 417](#)
- [OSM Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 418](#)



## General Caveats in Release 12.2(17b)SXA and Rebuilds

- [Open General Caveats in Release 12.2\(17b\)SXA2, page 409](#)
- [Resolved General Caveats in Release 12.2\(17b\)SXA2, page 411](#)
- [Resolved General Caveats in Release 12.2\(17b\)SXA, page 411](#)

### Open General Caveats in Release 12.2(17b)SXA2

- Ignore spurious memory access errors during an SSO switchover. (CSCed64648, CSCeb55269, CSCed44945, CSCed47559, CSCed50801, CSCed51914, CSCed64843, CSCed76955, CSCed80188, CSCed88244, CSCee10565, CSCee10728, CSCee19150, CSCee32558, CSCee42141, CSCee56069, CSCee59872, CSCin70853, CSCin72244)
- With a PFC3, on Layer 3 interfaces that are configured to support IPX routing, but which are not configured with an IP address, the **mls rate-limit** commands incorrectly limit IPX traffic.  
**Workaround:** Configure an IP address on Layer 3 interfaces that are configured to support IPX routing. Use an IP address to which IP routing does not send any traffic. Configure an IP access list to drop IP ingress traffic. This problem is resolved in Release 12.2(18)SXE. (CSCee09692)
- You might see the following message on a redundant supervisor engine:  

```
SM-SP-STDBY-4-BADEVENT:
Event 'bundle_sync' is invalid for the current state 'COLLECTING_DISTRIBUTING':
traceback= 40306D5C 404975E8 40499DBC 4048E65C 408EB04C 406CC9DC 406C7F1C
```

  
This problem is resolved in Release 12.2(18)SXD. (CSCed20448)
- An SNMP query to retrieve the policy maps attached to an interface that has multiple policy maps attached aggregates the policy maps into a display showing only one policy map. This problem is resolved in Release 12.2(17d)SXB. (CSCec72502)
- With the single router mode with stateful switchover (SRM with SSO) redundancy mode configured, the **show mls qos ip interface** command displays different egress QoS statistics and EtherChannel ingress QoS statistics for the active and redundant supervisor engines. (CSCec66293)



**Note** CSCec66293 is not seen in later releases.

- Ingress policing does not work on an interface configured to support MPLS. This problem is resolved in Release 12.2(17d)SXB. (CSCed36000, CSCin61428)
- The **show mls qos ip port** command output displays two policies attached to the port when only one is attached. This problem is resolved in Release 12.2(18)SXD. (CSCed16185)
- If you enter a **no mpls ip** or **no ip addr** interface command, and then enter an **interface range** command, ignore any “const\_mpls\_dec\_mpls\_use: error - zero mpls\_use\_count” messages. This problem is resolved in Release 12.2(18)SXD. (CSCeb64700)
- These objects in SWITCH-ENGINE-MIB return inaccurate values:
  - cseFlowMcastResultDstVlans
  - cseFlowMcastResultDstVlans2k
  - cseFlowMcastResultDstVlans3k
  - cseFlowMcastResultDstVlans4k

This problem is resolved in Release 12.2(18)SXD. (CSCed14797)

- If you enter the **clear ip igmp snooping statistics** command With IGMP snooping enabled, and some IGMPv3 groups that have many sources, you might see messages about high CPU usage. This problem is resolved in Release 12.2(18)SXD. (CSCed30453)
- Multicast subnet entries are not removed when you disable PIM on an interface. The stale subnet entries remain programmed in hardware. There is no effect on multicast forwarding of packet because the entries are used only for bridging.

**Workaround:** Enter a **shutdown** command on the interface before removing Protocol Independent Multicast (PIM). This problem is resolved in Release 12.2(18)SXD. (CSCed28813)

- You might see a traceback message if an MST instance loses its root port. If you have configured single router mode with stateful switchover (SRM with SSO) redundancy mode, an unnecessary synchronization of the root port information might occur. This problem is resolved in Release 12.2(17d)SXB. (CSCed30292)
- When booting, you might see the following message:

```
%C6K_PROCMIB-SP-3-IPC_PORTOPEN_FAIL: Failed to open port while connecting to process
statistics: error code = no such port
-Traceback= 4071AD28 4071AE34
```

This problem is resolved in Release 12.2(18)SXD. (CSCed12970)

- With UplinkFast configured, if the root port goes down and the alternate root port becomes the root port and the original root port comes back up, and then an SSO with SRM switchover occurs before the delay timer expires, the original root port remains in the blocking state until you enter **shutdown** and **no shutdown** commands. This problem is resolved in Release 12.2(17d)SXB. (CSCed10816)
- The **show tech support command** does not execute correctly. This problem is resolved in Release 12.2(17d)SXB. (CSCed31353)
- MST supports a total of 30,000 logical interfaces. This problem is resolved in Release 12.2(17d)SXB. (CSCed33864)
- Trunk configuration using the following MIB objects on access ports does not work. When each MIB object is set, the previously configured MIB objects are cleared:
  - vlanTrunkPortVlansEnabled
  - vlanTrunkPortVlansEnabled2k
  - vlanTrunkPortVlansEnabled3k
  - vlanTrunkPortVlansEnabled4k

**Workaround:** Configure the access ports for trunking using other MIBs. Once trunking is operational, configure the above four MIBs, one MIB object per PDU. This problem is resolved in Release 12.2(17d)SXB. (CSCed30335)

- If a single router mode with stateful switchover (SRM with SSO) switchover occurs when an interface is shut down that had ACLs or ACL features configured on it when it was in an admin up state, the newly active TCAM will have entries for the shutdown interface, which might result in TCAM exceptions if you apply features to active interfaces. This problem is resolved in Release 12.2(17d)SXB. (CSCed19296, CSCed15472)
  - To avoid a reload, do not remove any interfaces that have IPv6 features configured (for example, an IPv6 ACL) or revert any interfaces that have IPv6 features configured to the default configuration.
- Workaround:** Remove the IPv6 feature from the interface before you enter the **no interface** command. This problem is resolved in Release 12.2(17d)SXB. (CSCec74016)
- All ingress IPv6 traffic on an IPv4 VRF-enabled interface is routed in software on the MSFC3. (CSCec03707)

- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

## Resolved General Caveats in Release 12.2(17b)SXA2

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

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

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>

This problem is resolved in Release 12.2(17b)SXA2. (CSCed93836, CSCdz84583, CSCed27956, CSCed38527)

- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an intrusion detection system (IDS) signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.2(17b)SXA2. (CSCed35253)

## Resolved General Caveats in Release 12.2(17b)SXA

- A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

This vulnerability is documented as Cisco bug ID CSCed30113. There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsn.shtml>

This problem is resolved in Release 12.2(17b)SXA. (CSCed30113)

- The Supervisor Engine 720 may fail to detect an OIR of the Compact Flash and reset. This problem is resolved in Release 12.2(17b)SXA. (CSCec68645)
- In Release 12.2(17a)SX, the **WS-X6408-GBIC** switching module is not supported with a Supervisor Engine 720. This problem is resolved in Release 12.2(17b)SXA. (CSCec65943)

- Traffic loss may occur with **distributed EtherChannels (DECs)** because of a race condition when the EtherChannels are formed after the VLAN SVI is up. This problem is resolved in Release 12.2(17b)SXA. (CSCec55168)

- A supervisor engine alignment error causes the MSFC3 to reset with the following error message:

```
%CPU_MONITOR-3-PEER_EXCEPTION: CPU_MONITOR peer has failed due to exception ,
resetting [5/0]
```

This problem is resolved in Release 12.2(17b)SXA. (CSCec54433)

- Spurious memory access tracebacks might occur during configuration. This problem is resolved in Release 12.2(17b)SXA. (CSCec42594)
- The **vlan mapping dot1q dot1q\_vlan isl isl\_vlan** command is inadvertently hidden. The command is still present and can be used. This problem is resolved in Release 12.2(17b)SXA. (CSCec40198)
- Do not use port 1/1 if a FlexWAN module is installed or if private VLANs (PVLANS) are configured. This problem is resolved in Release 12.2(17b)SXA. (CSCec36382)
- With high traffic levels and when the reverse forwarding path (RPF) towards the rendezvous point and the multicast source are different, partially hardware-switched multicast flows might not be forwarded correctly. This problem is resolved in Release 12.2(17b)SXA. (CSCec80654)
- When Automatic Protection Switching (APS) is not configured on a POS interface, ignore an incrementing “COAPS” counter. This problem is resolved in Release 12.2(17b)SXA. (CSCec89414)
- NetFlow Data Export (NDE) does not support multicast traffic, but NDE might export some multicast data. This problem is resolved in Release 12.2(17b)SXA. (CSCec37069)
- New vulnerabilities in the OpenSSL implementation for SSL have been announced.

An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml>

This problem is resolved in Release 12.2(17b)SXA. (CSCec46274)

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

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

This problem is resolved in Release 12.2(17b)SXA. (CSCdu53656)

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

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

This problem is resolved in Release 12.2(17b)SXA. (CSCea28131)

- VACL capture does not work on WAN ports. This problem is resolved in Release 12.2(17b)SXA. (CSCec75140)
- A reload might occur if you remove a network command from an interface where OSPF is configured and there is OSPF traffic from the interface in the OSPF queue. This problem is resolved in Release 12.2(17b)SXA. (CSCec48816)
- The **show controller serial** command output is not complete. This problem is resolved in Release 12.2(17b)SXA. (CSCin60835)
- Caveat CSCdz27200 is resolved in Release 12.2(14) and in Release 12.2(14)SX and later 12.2SX releases. In releases where caveat CSCdz27200 is resolved, a reload might occur when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, disk0). For example, this situation may occur when you enter the **show command\_name | tee /append url** privileged EXEC command. This problem is resolved in Release 12.2(17b)SXA. (CSCin57765)
- The following images do not support IPv6 dCEF:
  - s72033-jk9s-mz.122-17a.SX1
  - s72033-pk9s-mz.122-17a.SX1
  - s72033-ps-mz.122-17a.SX1

This problem is resolved in Release 12.2(17b)SXA. (CSCed22535)

- If you enter the **ip flow-export destination** command to configure multiple flow export destinations, you might observe high CPU utilization and dropped control packets, which can result in routing protocol timeouts and slowed response during console access. This problem is resolved in Release 12.2(17b)SXA. (CSCed15587)
- If multiple users attempt to configure QoS simultaneously, the system might pause indefinitely. This problem is resolved in Release 12.2(17b)SXA. (CSCea84387)
- The default Operation Administration and Maintenance (OAM) intercept configuration drops OAM F5 END loopback cells. This problem is resolved in Release 12.2(17b)SXA. (CSCdw41639)
- The [WS-X6548-RJ-21](#) module does not support the **mdix auto** command. This problem is resolved in Release 12.2(17b)SXA. (CSCec50648)
- On OSMs, Cisco IOS software disables some GBICs when the software incorrectly reports that the GBIC has a faulty EEPROM instead of type 25 or type 29 media (“unknown media type”). This problem is resolved in Release 12.2(17b)SXA. (CSCeb86171)
- Because the Rivest, Shamir, and Adelman (RSA) key is not stored, SSH does not work after a reload. This problem is resolved in Release 12.2(17b)SXA. (CSCeb54694)
- If you reconfigure an ATM VC bundle as a PVC, the VC stops forwarding traffic. This problem is resolved in Release 12.2(17b)SXA. (CSCdx79081)
- A user can enter a portion of a valid Virtual Private Network (VPN) group name, and if it is part of a valid Extended Authentication (Xauth) username, gain access to another VPN group. This problem is resolved in Release 12.2(17b)SXA. (CSCea51081)
- With Remote Access Server (RAS) and H225 Application Layer Gateway (ALG) processing enabled, Network Address Translation (NAT) might cause a reload. This problem is resolved in Release 12.2(17b)SXA. (CSCea81952)
- Enable passwords are not encrypted and do not work if you configure the enable password when service password encryption is already enabled. This problem is resolved in Release 12.2(17b)SXA. (CSCec42069)

- Because a multicast router might fail to send a register stop message, the designated router sends register messages continuously. This problem is resolved in Release 12.2(17b)SXA. (CSCec41693)
- The OSPF adjacencies in an area might reset if you enter the **area X stub** OSPF command or the **area Y nssa** OSPF command when the **area X stub** OSPF command or the **area Y nssa** OSPF command is already configured or if you enter a **copy startup-config running-config** command. This problem is resolved in Release 12.2(17b)SXA. (CSCec30212)
- Following an Open Shortest Path First version 3 (OSPFv3) interface number change, an OSPFv3 adjacency might go up and down after a reload. This problem is resolved in Release 12.2(17b)SXA. (CSCec29868)
- With Multiprotocol Label Switching (MPLS) configured, a reload might occur if the Label Distribution Protocol (LDP) peer address table is corrupt because three or more routers have advertised the same IP address in LDP address messages. This problem is resolved in Release 12.2(17b)SXA. (CSCeb86270)
- When an IPv4 prefix is learned through a Border Gateway Protocol (BGP) session and the prefix is deleted in the Label Information Base (LIB) and not allocated to any local label binding, an outgoing label might not be installed in the Label Forwarding Information Base (LFIB) for the prefix. This problem is resolved in Release 12.2(17b)SXA. (CSCeb79576)
- If you enter the **passive-interface default** IPv6 OSPF command on an interface, it is incorrectly configured on all IPv6 OSPF interfaces. This problem is resolved in Release 12.2(17b)SXA. (CSCeb61700)
- Following a reload with a large number of active interfaces, an Open Shortest Path First (OSPF) interface might be in the down state while the port and the line protocol might be in the up state, which causes missing OSPF neighbor adjacencies on the OSPF interface that is in the down state. This problem is resolved in Release 12.2(17b)SXA. (CSCeb04048)
- With Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configured, traceback errors might occur when a link goes up and down. This problem is resolved in Release 12.2(17b)SXA. (CSCea83647)
- With Virtual Private Network (VPN) routing and forwarding (VRF) configured, a reload might occur if you enter the **clear ip bgp \*** privileged EXEC command while interfaces go up and down continuously or if you enter the **clear ip bgp \*** privileged EXEC command and the **hw-reload reset EXEC** command. This problem is resolved in Release 12.2(17b)SXA. (CSCea29102)
- After a reload, OSPF might not pass traffic through tunnel interfaces. This problem is resolved in Release 12.2(17b)SXA. (CSCdz67496)
- With a large number of static multicast entries configured (approximately 8,000), some entries might not propagate to DFCs. This problem is resolved in Release 12.2(17b)SXA. (CSCec50577)
- With a **13-slot chassis**, a bus error and a reload might occur if you configure EtherChannels that include any slot 13 ports. This problem is resolved in Release 12.2(17b)SXA. (CSCec49438)
- Incorrect processing of received PIM packets causes IGMP snooping to fail. When this occurs, the system is unable to learn the correct outbound interface for the multicast traffic. This problem is resolved in Release 12.2(17b)SXA. (CSCec46892)
- With MPLS PE functionality, some IP-to-tag adjacencies might be incorrectly installed on the switch processor after interfaces go up and down and a large number of BGP routes need to be resolved. This problem is resolved in Release 12.2(17b)SXA. (CSCec30461)
- The MAC-move notification feature cannot be configured when there are EtherChannels formed from ports on different DFC-equipped modules. This problem is resolved in Release 12.2(17b)SXA. (CSCec15149)

- Some traffic that ingresses through one DFC-equipped module and egresses through another DFC-equipped module might be dropped. This problem is resolved in Release 12.2(17b)SXA. (CSCeb83650)
- If you enter the **shutdown** command and then the **no shutdown** command on an interface that is handling a high volume of Layer 3 hardware-switched multicast traffic, some of the multicast traffic is routed in software on the MSFC instead of being Layer 3 switched in hardware when the interface comes back up. This problem is resolved in Release 12.2(17b)SXA. (CSCeb67996)
- When fragmenting MPLS traffic, a reload might occur after display of a “SYS-2-GETBUF” message. This problem is resolved in Release 12.2(17b)SXA. (CSCeb16876)
- The PFC might not be programmed to provide Layer 3 switching for traffic that follows a static route to the null 0 interface. This problem is resolved in Release 12.2(17b)SXA. (CSCea86396)
- Layer 2 and Layer 3 switched counters remain at 0 after you enter the **show interface vlan** command. This problem is resolved in Release 12.2(17b)SXA. (CSCea69116)
- To avoid dropping into ROMMON, do not insert a [WS-X6816-GBIC](#) that does not have a DFC installed. This problem is resolved in Release 12.2(17b)SXA. (CSCed14506)
- [WS-X6502-10GE](#) switching modules do not support custom IEEE 802.1Q EtherTypes. This problem is resolved in Release 12.2(17b)SXA. (CSCec50469, CSCec35933, CSCec36553)



- Cisco products running Cisco IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and Cisco IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>

This problem is resolved in Release 12.2(17b)SXA. (CSCea19885, CSCea32240, CSCea33065, CSCea36231, CSCea46342, CSCea51076, CSCea51030, CSCea54851, CSCdx76632, CSCdx77253, CSCdw14262, CSCdx40184, CSCed28873, CSCdt50932, CSCdy61597, CSCeb78836, CSCin56408)

## FlexWAN Module Caveats in Release 12.2(17b)SXA and Rebuilds

- [Open FlexWAN Module Caveats in Release 12.2\(17b\)SXA2, page 416](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17b\)SXA, page 416](#)

### Open FlexWAN Module Caveats in Release 12.2(17b)SXA2

- Following a reload, modular QoS CLI (MQC) MPLS CoS classification does not work.  
**Workaround:** Remove and reapply the service policy. This problem is resolved in Release 12.2(18)SXD. (CSCed35900)
- MPLS on the FlexWAN module does not support Virtual Private LAN Service (VPLS). To avoid a reload, do not use a network topology where MPLS on the FlexWAN module receives VPLS traffic. This problem is resolved in Release 12.2(17d)SXB. (CSCed35405)

### Resolved FlexWAN Module Caveats in Release 12.2(17b)SXA2

None.

### Resolved FlexWAN Module Caveats in Release 12.2(17b)SXA

- With heavy traffic through a [PA-MC-T3](#) or [PA-MC-E3](#) port adapter, a FlexWAN module might reload. This problem is resolved in Release 12.2(17b)SXA. (CSCin62978)
- A FlexWAN module is not detected during the boot process, which causes it to be ignored during the startup configuration process. This problem is resolved in Release 12.2(17b)SXA. (CSCed00781)
- Ignore messages from a 1-port multichannel STM-1 port adapter ([PA-MC-STM-1](#)) that reports a large number of degraded minutes on an E1 controller. For example, after 15 minutes of operation since startup, 35,000,000 degraded minutes might be reported and these values might increase every second. Code violations might also be reported. This problem is resolved in Release 12.2(17b)SXA. (CSCec08973)



- Output queue packet drops might occur on the priority queue of an E1 serial interface on a 1-port multichannel E3 port adapter ([PA-MC-E3](#)), after which the E1 serial interface becomes congested. This problem is resolved in Release 12.2(17b)SXA. (CSCeb34203)
- The FlexWAN module might corrupt very small Frame Relay packets (for example, 2-byte X.25 SABM packets). This problem is resolved in Release 12.2(17b)SXA. (CSCec59440)

## Service Module Caveats in Release 12.2(17b)SXA and Rebuilds

- [Open Service Module Caveats in Release 12.2\(17b\)SXA2, page 417](#)
- [Resolved Service Module Caveats in Release 12.2\(17b\)SXA2, page 417](#)
- [Resolved Service Module Caveats in Release 12.2\(17b\)SXA, page 417](#)

### Open Service Module Caveats in Release 12.2(17b)SXA2

- To avoid reloads, do not configure the single router mode with stateful switchover (SRM with SSO) redundancy mode with a IPsec VPN Acceleration services module ([WS-SVC-IPSEC-1](#)) installed.

**Workaround:** Configure RPR or RPR+ redundancy mode with a WS-SVC-IPSEC-1 module installed. This problem is resolved in Release 12.2(17d)SXB. (CSCed17605)

- In a VPN module high-availability configuration, communication is lost between the standby and active supervisor engines when the state synchronization protocol (SSP) is transmitted over an IPsec tunnel that passes through a port configured with a nondefault MTU size.

**Workaround:** Use the default MTU size. (CSCed00020)

- A grouping of two active IPsec VPN Acceleration services modules ([WS-SVC-IPSEC-1](#)) that are failover partners is called a *blade failover group* (BFG). If you OIR or administratively disable a VPN module that does not have a failover partner, the BFG configuration may be inconsistent.

**Workaround:** Remove the module from the BFG and add it back to the BFG.

A similar problem may occur when a VPN module is removed physically from the chassis and the chassis is reloaded but the BFG configuration is not removed.

**Workaround:** Remove the BFG from the configuration, save the configuration change to the startup configuration, and reload the chassis.

This problem is resolved in Release 12.2(17d)SXB. (CSCed19505)

- In a blade failover group (BFG) with 2 IPsec VPN Acceleration services modules ([WS-SVC-IPSEC-1](#)) where the active VPN module has all the crypto connections configured, if you power down the active VPN module, save the configuration, and do a reload, the traffic may not go through the standby VPN module. (CSCed22645)

### Resolved Service Module Caveats in Release 12.2(17b)SXA2

None.

### Resolved Service Module Caveats in Release 12.2(17b)SXA

- The internal EtherChannel that connects the [WS-X6066-SLB-APC](#) incorrectly does not trust DSCP, which sets DSCP to zero in all packets from the [WS-X6066-SLB-APC](#) when QoS is enabled. This problem is resolved in Release 12.2(17b)SXA. (CSCec27686)

- User authentication might fail for a CiscoSecure VPN client when the client username includes a domain delimiter character (for example, @) and when the domain name does not match the authentication group name. This problem is resolved in Release 12.2(17b)SXA. (CSCdz55955)
- BPDU packets are not sent to Firewall Services Module (FWSM) ports. When transparent-firewall mode is used, this situation may cause packet-forwarding loops when redundancy is enabled or when two Firewall Services Modules share the same VLANs. This problem is resolved in Release 12.2(17b)SXA. (CSCec14054)

## OSM Caveats in Release 12.2(17b)SXA and Rebuilds

- [Open OSM Caveats in Release 12.2\(17b\)SXA2, page 418](#)
- [Resolved OSM Caveats in Release 12.2\(17b\)SXA2, page 418](#)
- [Resolved OSM Caveats in Release 12.2\(17b\)SXA, page 418](#)

### Open OSM Caveats in Release 12.2(17b)SXA2

- Changing the MTU size on a port might not change the MPLS MTU size.  
**Workaround:** Enter **shutdown** and **no shutdown** commands after configuring an MTU size on a port. This problem is resolved in Release 12.2(18)SXE. (CSCed17226, CSCed33822)

### Resolved OSM Caveats in Release 12.2(17b)SXA2

None.

### Resolved OSM Caveats in Release 12.2(17b)SXA

- [OSM-4GE-WAN-GBIC](#) interfaces remain in the up/up state when the other end of the link is inactive. This problem is resolved in Release 12.2(17b)SXA. (CSCec79460)
- The main interface counters on POS OSMs and the Gigabit Ethernet WAN OSMs are 32 bits instead of 64 bits. This problem is resolved in Release 12.2(17b)SXA. (CSCdx08807)
- Occasionally, OSM POS interfaces stop updating statistics while traffic is passing. This problem is resolved in Release 12.2(17b)SXA. (CSCea78519)
- For OC-12c OSMs, the **show controller pos interface pm** command displays incorrect optics information. This problem is resolved in Release 12.2(17b)SXA. (CSCec48974)
- Distributed CEF switching does not work for multilink interface egress traffic. This problem is resolved in Release 12.2(17b)SXA. (CSCec55650)
- An E3 link to an OC-12 channelized OSM might not come up. This problem is resolved in Release 12.2(17b)SXA. (CSCec39689)

## Caveats in Release 12.2(17a)SX and Rebuilds

- [General Caveats in Release 12.2\(17a\)SX and Rebuilds, page 419](#)
- [FlexWAN Module Caveats in Release 12.2\(17a\)SX and Rebuilds, page 423](#)
- [Service Module Caveats in Release 12.2\(17a\)SX and Rebuilds, page 425](#)

## General Caveats in Release 12.2(17a)SX and Rebuilds

- [Open General Caveats in Release 12.2\(17a\)SX4](#), page 419
- [Resolved General Caveats in Release 12.2\(17a\)SX3](#), page 419
- [Resolved General Caveats in Release 12.2\(17a\)SX3](#), page 420
- [Resolved General Caveats in Release 12.2\(17a\)SX2](#), page 420
- [Resolved General Caveats in Release 12.2\(17a\)SX1](#), page 421
- [Resolved General Caveats in Release 12.2\(17a\)SX](#), page 421

### Open General Caveats in Release 12.2(17a)SX4

- To avoid a reload, do not remove any interfaces that have IPv6 features configured (for example, an IPv6 ACL) or revert any interfaces that have IPv6 features configured to the default configuration.

**Workaround:** Remove the IPv6 feature from the interface before you enter a **no interface** command. This problem is resolved in Release 12.2(17d)SXB. (CSCec74016)

- [WS-X6502-10GE](#) switching modules do not support custom IEEE 802.1Q EtherTypes. This problem is resolved in Release 12.2(17b)SXA. (CSCec50469, CSCec35933, CSCec36553)
- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

### Resolved General Caveats in Release 12.2(17a)SX3

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

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

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>

This problem is resolved in Release 12.2(17a)SX4. (CSCed93836, CSCdz84583)

- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an intrusion detection system (IDS) signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.2(17a)SX4. (CSCed35253)

### Resolved General Caveats in Release 12.2(17a)SX3

- High-volume SNMP traffic might cause a reload. This problem is resolved in Release 12.2(17a)SX3. (CSCed79519)
- A [WS-X6748-GE-TX](#) module in slot 1 does not support speeds of 10 Mbps or 100 Mbps. This problem is resolved in Release 12.2(17a)SX3. (CSCed38862)

### Resolved General Caveats in Release 12.2(17a)SX2

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

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

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>

This problem is resolved in Release 12.2(17a)SX2. (CSCed27956, CSCed38527)

- The following images do not support IPv6 dCEF:
  - s72033-jk9s-mz.122-17a.SX1
  - s72033-pk9s-mz.122-17a.SX1
  - s72033-ps-mz.122-17a.SX1

This problem is resolved in Release 12.2(17a)SX2. (CSCed22535)

- If you enter the **ip flow-export destination** command to configure multiple flow export destinations, you might observe high CPU utilization and dropped control packets, which can result in routing protocol timeouts and slowed response during console access. This problem is resolved in Release 12.2(17a)SX2. (CSCed15587)
- With redundant Supervisor Engine 720s, a breakpoint exception might occur if you run a script over a Telnet session. This problem is resolved in Release 12.2(17a)SX2. (CSCed49091)

## Resolved General Caveats in Release 12.2(17a)SX1

- Enable passwords are not encrypted and do not work if you configure the enable password when service password encryption is already enabled. This problem is resolved in Release 12.2(17a)SX1. (CSCec42069)
- A reload might occur if you remove a network command from an interface where OSPF is configured and there is OSPF traffic from the interface in the OSPF queue. This problem is resolved in Release 12.2(17a)SX1. (CSCec48816)
- Spurious memory access tracebacks might occur during configuration. This problem is resolved in Release 12.2(17a)SX1. (CSCec42594)
- In Release 12.2(17a)SX, the [WS-X6408-GBIC](#) switching module is not supported with a Supervisor Engine 720. This problem is resolved in Release 12.2(17a)SX1. (CSCec65943)
- Do not use port 1/1 if a FlexWAN module is installed or if private VLANs (PVLANS) are configured. This problem is resolved in Release 12.2(17a)SX1. (CSCec36382)
- The **vlan mapping dot1q dot1q\_vlan isl isl\_vlan** command is inadvertently hidden. The command is still present and can be used. This problem is resolved in Release 12.2(17a)SX1. (CSCec40198)
- A supervisor engine alignment error causes the MSFC3 to reset with the following error message:  

```
%CPU_MONITOR-3-PEER_EXCEPTION: CPU_MONITOR peer has failed due to exception ,
resetting [5/0]
```

This problem is resolved in Release 12.2(17a)SX1. (CSCec54433)
- Traffic loss may occur with [distributed EtherChannels \(DECs\)](#) because of a race condition when the EtherChannels are formed after the VLAN SVI is up. This problem is resolved in Release 12.2(17a)SX1. (CSCec55168)
- The Supervisor Engine 720 may fail to detect an OIR of the Compact Flash and reset. This problem is resolved in Release 12.2(17a)SX1. (CSCec68645)

## Resolved General Caveats in Release 12.2(17a)SX



### Note

In Release 12.2(17a)SX and later releases, caveat CSCdy36604 disabled SNMP retrieval of dot1dBase group data on VLANs where the spanning tree protocol is not enabled. Caveat CSCdy36604 conflicts with RFC 1493 and the effect of caveat CSCdy36604 is removed with caveat CSCee39798 in Release 12.2(18)SXD.

- GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.  

As an RFC compliancy this DDTS adds the check for bits 4-5 (0 being the most significant) of GRE header.

This issue does not cause any problem for router operation.

This problem is resolved in Release 12.2(17a)SX. (CSCea22552)
- An in-band control (IBC) reset may cause the MSFC to drop packets. This problem is resolved in Release 12.2(17a)SX. (CSCec48379)
- If you configure an EtherChannel across DFCs, and then configure a trunk for VLANs that have been enabled for routing, traffic that is routed back on the trunk that the traffic arrived on may be dropped. This problem is resolved in Release 12.2(17a)SX. (CSCeb49514)

- With the Response Time Reporter (RTR) feature configured, spurious accesses might occur. This problem is resolved in Release 12.2(17a)SX. (CSCdy56859)
- A port in the STP loop guard loop-inconsistent state sends BPDUs and if is elected as the designated port on the segment, it does not recover from the loop-inconsistent state. This problem is resolved in Release 12.1(20)E. This problem is resolved in Release 12.2(17a)SX. (CSCeb06811)
- NAT receives traffic translated by itself. This problem is resolved in Release 12.2(17a)SX. (CSCdz18109)
- With the distribute-list command configured to filter redistributed EIGRP static routes, when you configure the filtering to permit additional static routes, the routes are not redistributed. This problem is resolved in Release 12.2(17a)SX. (CSCdz21986)
- Traffic might be dropped if you enter the **no ip cef** global configuration command. This problem is resolved in Release 12.2(17a)SX. (CSCin40371)
- OSPF might set the partial database flag without a partial shortest path first (SPF) occurring when a link-state advertisement (LSA) update received from a neighbor has a different mask from the mask in previous LSA updates. This situation might prevent the LSA from being deleted from the OSPF database. This problem is resolved in Release 12.2(17a)SX. (CSCdz82284)
- It is possible for an invalid **override-mac-address** command to be accepted at boot time if you use a configuration file from one system on another. This problem is resolved in Release 12.2(17a)SX. (CSCeb83558)
- The **squeeze** command might cause high CPU utilization for several minutes. This problem is resolved in Release 12.2(17a)SX. (CSCdz60750)
- An ATM interface might remain administratively down after “cmd failed” messages for ATM configuration commands are displayed. This problem is resolved in Release 12.2(17a)SX. (CSCin40163)
- The following message might be followed by a reload:  

```
%ALIGN-1-FATAL: Corrupted program counter pc=0xX, ra=0XXXXXXXXX, sp=0XXXXXXXXX
```

 This problem is resolved in Release 12.2(17a)SX. (CSCeb48670)
- When TTL propagation has been turned off by entering the **tag-switching ip propagate-ttl** command, MPLS TTLs are still copied to IP packets. This problem is resolved in Release 12.2(17a)SX. (CSCdy47341)
- MPLS does not work if you configure fall-back bridging on the MPLS subinterface. This problem is resolved in Release 12.2(17a)SX. (CSCdz75507)
- Occasionally, characters that you enter over a virtual terminal connection are not echoed. This problem is resolved in Release 12.2(17a)SX. (CSCdz36877)
- Address overloading might fail if you manually clear the NAT translation table. This problem is resolved in Release 12.2(17a)SX. (CSCdt95129)
- With a complex Spanning Tree topology (for example, a high number of blocked ports in the same VLAN), if an inferior BPDU is received at approximately the same time that the message age timer expires, STP might send out BPDUs with obsolete information (for example, the previous root ID) for the duration of the maximum age timer, which can delay STP convergence. This problem is resolved in Release 12.2(17a)SX. (CSCea68988)
- Bootstrap router rendezvous point (RP) candidates that are configured with different priorities on a Catalyst 6500 series switch or Cisco 7600 series router do not work with bidirectional PIM. If the RP candidates are configured with different the priorities, an RP other than the elected RP might be chosen for a given multicast route when the multicast-route entry is created. Because a Catalyst 6500 series switch or Cisco 7600 series router configured for bidirectional PIM installs only the

elected RP in hardware, hardware forwarding for bidirectional-PIM groups might become disabled if the RP chosen by that group for a particular multicast route is not elected as the RP. This problem is resolved in Release 12.2(17a)SX. (CSCea37241)

- If QoS configuration fails because of a flow mask resource conflict and you change the configuration to remove the conflict, the **show mls qos ip** command output still shows a configuration failure. This problem is resolved in Release 12.2(17a)SX. (CSCea64620)
- A partially switched bidirectional PIM flow may cause traffic not to be forwarded to the route processor. This problem occurs only if the system boots up when one of the following occurs:
  - Bidirectional PIM has not yet been configured on any of the interfaces
  - If an interface with bidirectional PIM configured is shut down
  - If multicast MLS is disabled

Under these circumstances, packets that need to be software processed will not reach the route processor. This problem is resolved in Release 12.2(17a)SX. (CSCea69837)

- If both a NetFlow table hash collision and a FIB exception occur simultaneously, the PFC3 might not provide hardware support for NAT. This problem is resolved in Release 12.2(17a)SX. (CSCea67226)
- The **show mls cef ip rpf** command returns the “longest match” prefix entry and you cannot specify the mask to use. In some cases, you cannot view the RPF information for a prefix. This problem is resolved in Release 12.2(17a)SX. (CSCea43954)
- Occasionally on bootup, a Supervisor Engine 720 reports minor and major temperature alarms with shutdown scheduled in 300 seconds (5 minutes), followed by alarm conditions recovery and shutdown cancellation 30 seconds later. You can safely ignore these messages. To display temperature readings, enter the **show environment temperature** command. To display alarm thresholds, enter the **show environment alarm threshold** command. This problem is resolved in Release 12.2(17a)SX. (CSCdy78989)
- If you configure PFC QoS **policy-map class** commands in a policy-map class (for example, a microflow policer, an aggregate policer, or commands that set the trust state) and attach the policy map to a LAN interface, a reload might occur if you remove the policy-map class from the policy map. This problem is resolved in Release 12.2(17a)SX. (CSCea67091)
- With more than one DFC-equipped switching module installed and many entries in the routing table, a switching module that receives an incorrect FIB IPC packet might reload. This problem is resolved in Release 12.2(17a)SX. (CSCea71219, CSCeb70232)
- With the Protocol Independent Multicast (PIM) Dense-Mode State Refresh feature enabled, a reload might occur if the group mode changes from PIM dense mode to PIM sparse or bidirectional mode. This problem is resolved in Release 12.2(17a)SX. (CSCea09302)

## FlexWAN Module Caveats in Release 12.2(17a)SX and Rebuilds

- [Open FlexWAN Module Caveats in Release 12.2\(17a\)SX4, page 424](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17a\)SX4, page 424](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17a\)SX3, page 424](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17a\)SX2, page 424](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17a\)SX1, page 424](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(17a\)SX, page 424](#)

**Open FlexWAN Module Caveats in Release 12.2(17a)SX4**

None.

**Resolved FlexWAN Module Caveats in Release 12.2(17a)SX4**

None.

**Resolved FlexWAN Module Caveats in Release 12.2(17a)SX3**

None.

**Resolved FlexWAN Module Caveats in Release 12.2(17a)SX2**

None.

**Resolved FlexWAN Module Caveats in Release 12.2(17a)SX1**

- To avoid a reload, do not configure distributed NBAR (dNBAR) on FlexWAN module interfaces. Caveat CSCdy84624 is not seen in Release 12.2(17a)SX1. (CSCdy84624)

**Resolved FlexWAN Module Caveats in Release 12.2(17a)SX**

- The output packet counter for multilink and distributed link fragmentation and interleaving (dLFI) interfaces displays double the actual traffic count. This problem is resolved in Release 12.2(17a)SX. (CSCin40374)
- The main interface counters on POS port adapters are 32 bits instead of 64 bits. This problem is resolved in Release 12.2(17a)SX. (CSCdx08807)
- All high-capacity counters remain at 0 for FlexWAN module POS interfaces. This problem is resolved in Release 12.2(17a)SX. (CSCdz46845)
- After a few weeks of normal operation, the interface on a PA- MC-8E1 port adapter begins going up and down and finally pauses with the output queue stuck as follows:

```
Serial1/1:1 is up, line protocol is up
Encapsulation HDLC, crc 16, Data non-inverted
Keepalive set (120 sec)
Last input 00:00:03, output 04:14:23, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 21952
Queueing strategy: weighted fair
Output queue: 30/4000/64/21855 (size/max total/threshold/drops)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
43903807 packets input, 3646461183 bytes, 0 no buffer
Received 0 broadcasts, 321 runts, 0 giants, 0 throttles
5160 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 2945 abort
42026998 packets output, 2185017012 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets 0 output buffer failures,
0 output buffers swapped out 31 carrier transitions
no alarm present
Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
```



The following traceback is observed in the log:

```
%LINK-4-TOOBIG: Interface Serial60:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
%LINK-4-TOOBIG: Interface Serial20:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
```

This problem is resolved in Release 12.2(17a)SX. (CSCdz72292)

- When you attach an output policy, Cisco IOS fair queuing is incorrectly not disabled. This problem is resolved in Release 12.2(17a)SX. (CSCdz32751)
- ATM port adapters do not support hardware-assisted NAT. This problem is resolved in Release 12.2(17a)SX. (CSCea71196)

## Service Module Caveats in Release 12.2(17a)SX and Rebuilds

- [Open Service Module Caveats in Release 12.2\(17a\)SX4, page 425](#)
- [Resolved Service Module Caveats in Release 12.2\(17a\)SX4, page 425](#)
- [Resolved Service Module Caveats in Release 12.2\(17a\)SX3, page 425](#)
- [Resolved Service Module Caveats in Release 12.2\(17a\)SX2, page 425](#)
- [Resolved Service Module Caveats in Release 12.2\(17a\)SX1, page 425](#)
- [Resolved Service Module Caveats in Release 12.2\(17a\)SX, page 426](#)

### Open Service Module Caveats in Release 12.2(17a)SX4

None.

### Resolved Service Module Caveats in Release 12.2(17a)SX4

None.

### Resolved Service Module Caveats in Release 12.2(17a)SX3

None.

### Resolved Service Module Caveats in Release 12.2(17a)SX2

None.

### Resolved Service Module Caveats in Release 12.2(17a)SX1

None.

## Resolved Service Module Caveats in Release 12.2(17a)SX

- A reload might occur following an RPR or RPR+ switchover if more than one service module is installed. This problem is resolved in Release 12.2(17a)SX. (CSCeb11966)
- The **analysis module slot\_num data-port port\_num capture** command that enables [WS-SVC-NAM-2](#) or [WS-SVC-IDSM2-K9](#) data port capture is not synchronized to the redundant supervisor in RPR+ mode. This problem is resolved in Release 12.2(17a)SX. (CSCeb17522)
- Release 12.2(14)SX1 incorrectly allows you to configure on-demand diagnostics for the Firewall Services module, the Intrusion Detection System module, and the Network Analysis Modules (NAMs), but the service modules do not support on-demand diagnostics. If you configure on-demand diagnostics for a service module, ignore any test failure messages for the service module. This problem is resolved in Release 12.2(17a)SX. (CSCeb03525)

## Caveats in Release 12.2(14)SX and Rebuilds

- [General Caveats in Release 12.2\(14\)SX and Rebuilds, page 426](#)
- [FlexWAN Module Caveats in Release 12.2\(14\)SX and Rebuilds, page 428](#)
- [Open Service Module Caveats in Release 12.2\(14\)SX1, page 429](#)

## General Caveats in Release 12.2(14)SX and Rebuilds

- [Open General Caveats in Release 12.2\(14\)SX1, page 426](#)
- [Resolved General Caveats in Release 12.2\(14\)SX1, page 427](#)
- [Resolved General Caveats in Release 12.2\(14\)SX, page 428](#)

## Open General Caveats in Release 12.2(14)SX1

- If QoS configuration fails because of a flow mask resource conflict and you change the configuration to remove the conflict, the **show mls qos ip** command still reports a configuration failure. This problem is resolved in Release 12.2(17a)SX. (CSCea64620)
- If both a NetFlow table hash collision and a FIB exception occur simultaneously, the PFC3 might not provide hardware support for NAT. This problem is resolved in Release 12.2(17a)SX. (CSCea67226)
- With more than one DFC-equipped switching module installed and many entries in the routing table, a switching module that receives an incorrect FIB IPC packet might reload. This problem is resolved in Release 12.2(17a)SX. (CSCea71219)
- A partially switched bidirectional PIM flow may cause traffic not to be forwarded to the route processor. This problem occurs only if the system boots up when one of the following occurs:
  - Bidirectional PIM has not yet been configured on any of the interfaces
  - If an interface with bidirectional PIM configured is shut down
  - If multicast MLS is disabled

Under these circumstances, packets that need to be software processed will not reach the route processor. This problem is resolved in Release 12.2(17a)SX. (CSCea69837)

- Configuring bootstrap router (BSR) rendezvous point (RP) candidates with different priorities on a Catalyst 6500 series switch or Cisco 7600 series router does not work with Bidirectional PIM. When different priorities are configured for different RP candidates, a different RP is chosen for a given multicast route when the multicast-route entry is created. Because Bidirectional PIM installs only the elected RP in hardware, hardware forwarding for bidirectional-PIM groups could become disabled if the RP chosen by that group for a particular multicast route might not be the elected RP from the RP-mapping perspective.

**Workaround:** Use BSR without priority or use Auto-RP or static RP. Entering the **clear mls ip multicast bidir-rp** command after the RP configuration changes causes the corresponding RP changes to be reflected quickly in hardware. This problem is resolved in Release 12.2(17a)SX. (CSCe37241)

- Occasionally on bootup, a Supervisor Engine 720 reports minor and major temperature alarms, with shutdown scheduled in 300 seconds (5 minutes), followed by alarm conditions recovery and shutdown cancellation 30 seconds later. You can safely ignore these messages. Use the **show environment temperature** command to display temperature readings. Use the **show environment alarm threshold** command to display alarm thresholds. This problem is resolved in Release 12.2(17a)SX. (CSCdy78989)
- If you configure PFC QoS policy-map class commands in a policy-map class (for example, a microflow policer, an aggregate policer, or commands that set the trust state) and attach the policy map to a LAN interface, a reload might occur if you remove the policy-map class from the policy map.

**Workaround:** Remove the PFC QoS policy-map class commands before you remove the policy-map class from the policy map or remove the policy map from the interface before making changes. This problem is resolved in Release 12.2(17a)SX. (CSCe67091)

- The **show mls cef ip rpf** command returns the “longest match” prefix entry and you cannot specify the mask to use. Therefore, in some cases, you cannot view the RPF information for a prefix. This problem is resolved in Release 12.2(17a)SX. (CSCe43954)
- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

**Workaround:** Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

## Resolved General Caveats in Release 12.2(14)SX1

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

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

This advisory is available at:

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

This problem is resolved in Release 12.2(14)SX1. (CSCdz71127)

- If you OIR modules and reconfigure them, the SNMP ifIndexes might not be maintained after an RPR+ switchover. This problem is resolved in Release 12.2(14)SX1. (CSCe69334)

- In a topology that uses VLAN interfaces for intermediate router connections, PIM register and PIM register stop messages might loop between the intermediate routers until the TTL count expires. This problem is resolved in Release 12.2(14)SX1. (CSCea82353)
- Occasionally, EtherChannels do not work after an RPR+ switchover. This problem is resolved in Release 12.2(14)SX1. (CSCeb11932)
- Occasionally, a FIB TCAM exception causes a reload. This problem is resolved in Release 12.2(14)SX1. (CSCeb17471)
- After you enable IEEE 802.1Q tunneling, you cannot disable it. This problem is resolved in Release 12.2(14)SX1. (CSCdy11767)
- The ISIS routing protocol does not work over GRE tunnels. This problem is resolved in Release 12.2(14)SX1. (CSCea71481)
- With a redundant supervisor engine installed and with the system operating in bus mode, a reload might occur. This problem is resolved in Release 12.2(14)SX1. (CSCea92287)
- A reload occurs if you delete the Layer 3 VLAN interface of a private VLAN. This problem is resolved in Release 12.2(14)SX1. (CSCea76891)
- A redundant supervisor engine might not reload if you enter the **reload** command on the redundant supervisor engine's console or physically remove and reinsert the redundant supervisor engine. This problem is resolved in Release 12.2(14)SX1. (CSCea66858)
- STP-related traps for new root, topology change, and inconsistency are not generated. This problem is resolved in Release 12.2(14)SX1. (CSCea35846)
- All packets that have the same IP address for source and destination are dropped even if the destination address is valid. This problem is resolved in Release 12.2(14)SX1. (CSCea66067)

### Resolved General Caveats in Release 12.2(14)SX

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

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

This advisory is available at:

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

This problem is resolved in Release 12.2(14)SX. (CSCea02355)

### FlexWAN Module Caveats in Release 12.2(14)SX and Rebuilds

- [Open FlexWAN Module Caveats in Release 12.2\(14\)SX1, page 428](#)
- [Resolved FlexWAN Module Caveats in Release 12.2\(14\)SX1, page 429](#)

#### Open FlexWAN Module Caveats in Release 12.2(14)SX1

- To avoid a reload, do not configure distributed NBAR (dNBAR) on FlexWAN module interfaces. (CSCdy84624)

- ATM port adapters do not support hardware-assisted NAT. This problem is resolved in Release 12.2(17a)SX. (CSCe71196)

## Resolved FlexWAN Module Caveats in Release 12.2(14)SX1

- A FlexWAN module might reload if you configure distributed MLP bundles. This problem is resolved in Release 12.2(14)SX1. (CSCe65695)
- When one FlexWAN port adapter reloads, traffic might be incorrectly interrupted. This problem is resolved in Release 12.2(14)SX1. (CSCin32872)
- After an OIR, PVCs configured for operations, administration, and maintenance (OAM) cells on PA-A3-OC3 ATM subinterfaces remain inactive, which keeps the interface shut down. This problem is resolved in Release 12.2(14)SX1. (CSCin41295)
- After a reload, some PVCs on PA-A3-8T1/8E1 IMA port adapter interfaces might remain inactive. This problem is resolved in Release 12.2(14)SX1. (CSCin33669)
- After a reload, a FlexWAN module with a [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) port adapter installed might reload. This problem is resolved in Release 12.2(14)SX1. (CSCin34322)
- A reload might occur if you configure an ATM User Network Interface (UNI) link on a [PA-A3-8T1IMA](#) or [PA-A3-8E1IMA](#) port adapter. This problem is resolved in Release 12.2(14)SX1. (CSCin33561)
- A FlexWAN module might reload if you configure Link Fragmentation and Interleaving (LFI) on an ATM interface while the interface is handling traffic. This problem is resolved in Release 12.2(14)SX1. (CSCe73586)
- With multilink PPP configured on links on multiple FlexWAN modules, a reload might occur if the multilink egress IP packets need to be fragmented. This problem is resolved in Release 12.2(14)SX1. (CSCe60211)
- After you enter the **no shutdown** command, a [PA-MC-STM-1](#) port adapter might remain shut down. This problem is resolved in Release 12.2(14)SX1. (CSCin35854)
- RFC1483 hardware bridging over AAL5SNAP encapsulation does not work on FlexWAN. This problem is resolved in Release 12.2(14)SX1. (CSCe70308)

## Open Service Module Caveats in Release 12.2(14)SX1



### Note

With a [WS-SVC-IDSM2-K9](#) (fabric-enabled Intrusion Detection System Module 2) installed, be aware of intrusion detection system (IDS) software caveat CSCe75321.

- The **analysis module slot\_num data-port port\_num capture** command that enables [WS-SVC-NAM-2](#) or [WS-SVC-IDSM2-K9](#) data port capture is not synchronized to the redundant supervisor in RPR+ mode.  
**Workaround:** Enter the command again after the switchover. This problem is resolved in Release 12.2(17a)SX. (CSCeb17522)
- Ignore “%SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host” messages. (CSCeb11906)



**Note** Caveat CSCeb11906 is not seen in later releases.

- Release 12.2(14)SX1 incorrectly allows you to configure on-demand diagnostics for the Firewall Services module, the Intrusion Detection System module, and the Network Analysis Modules (NAMs), but the service modules do not support on-demand diagnostics. If you configure on-demand diagnostics for a service module, ignore any test failure messages for the service module. This problem is resolved in Release 12.2(17a)SX. (CSCeb03525)
- A reload might occur following an RPR or RPR+ switchover if more than one service module is installed. This problem is resolved in Release 12.2(17a)SX. (CSCeb11966)

## Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:

- [System Troubleshooting, page 430](#)
- [Module Troubleshooting, page 431](#)
- [VLAN Troubleshooting, page 431](#)
- [Spanning Tree Troubleshooting, page 431](#)
- [Additional Troubleshooting Information, page 432](#)



**Note** To attempt recovery from MSFC ROMMON, enter the **confreg 0x2102** and **reset** ROMMON commands.

## System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the redundant supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.
- If you have an interface whose speed is set to **auto** connected to another interface whose speed is set to a fixed value, configure the interface whose speed is set to a fixed value for half duplex. Alternately, you can configure both interfaces to a fixed-value speed and full duplex.

## Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module into a chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

## VLAN Troubleshooting



### Note

Catalyst 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and sends no DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

## Spanning Tree Troubleshooting

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches receive spanning tree bridge protocol data units (BPDUs) periodically from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree vlan *vlan\_ID* hello-time** command (the default frequency is set to 2 seconds). If a switch does not receive a BPDU in the time period defined by the **spanning-tree vlan *vlan\_ID* max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree vlan *vlan\_ID* forward-time** command (15 seconds by default) in each of these intermediate states. If a blocked spanning tree interface does not receive BPDUs from its neighbor within 50 seconds, it moves into the forwarding state.



### Note

We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs. The convergence time might be unacceptably long with more than 20 active VLANs.

To debug STP problems, follow these guidelines:

- The sum of all logical interfaces equals the number of trunks on the switch times the number of active VLANs on the trunks, plus the number of nontrunking interfaces on the switch.
- The **show spanning-tree summary totals** command displays the number of logical interfaces in the STP Active column.
- These maximum numbers of logical interfaces are supported:

MST	RPVST+	PVST+
50,000 total	10,000 total	13,000 total
30,000 total with Release 12.2(17b)SXA (CSCed33864 <sup>1</sup> )		
6,000 <sup>2</sup> per switching module	1,800 <sup>2</sup> per switching module	1,800 <sup>2</sup> per switching module

1. CSCed33864 is resolved in Release 12.2(17d)SXB and later releases.
2. 10 Mbps, 10/100 Mbps, and 100 Mbps switching modules support a maximum of 1,200 logical interfaces per module.



#### Note

Cisco IOS software displays a message if you exceed the maximum number of logical interfaces.

- After a switchover from the active to the redundant supervisor engine, the ports on the redundant supervisor engine take longer to come up than other ports.
- Record all spanning tree-blocked ports in each switch in your network. For each of the spanning tree-blocked ports, record the output of the **show interface** command. Check to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs. If the input queue counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.
- On trunks, make sure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions under heavy traffic conditions.

## Additional Troubleshooting Information

For additional troubleshooting information, refer to the publications at this URL:

[http://www.cisco.com/en/US/partner/products/hw/switches/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/partner/products/hw/switches/tsd_products_support_category_home.html)

## System Software Upgrade Instructions

See this publication:

[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_configuration\\_example09186a0080116ff0.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_configuration_example09186a0080116ff0.shtml)



## Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with the documents and tools described in the following sections:

- [Release-Specific Documents, page 433](#)
- [Cisco Feature Navigator, page 434](#)
- [Cisco IOS Software Documentation Set, page 434](#)

## Release-Specific Documents

The following document is specific to Cisco IOS Release 12.2 and is located on Cisco.com:

- Caveats for Cisco IOS Release 12.2

See *Caveats for Cisco IOS Release 12.2* for caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Release Notes: 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 this URL:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## Platform-Specific Documents

These publications are available for the Catalyst 6500 series switches running Cisco IOS on the supervisor engine and MSFC:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS System Message Guide*

## Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

### 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.

The Cisco IOS software documentation set is available on Cisco.com.

On Cisco.com at:

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

### Release 12.2 Documentation Set

[Table 1](#) lists the contents of the Cisco IOS Release 12.2 software documentation set.



#### Note

You can find the most current Cisco IOS documentation on Cisco.com.

On Cisco.com at:

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

**Table 1** *Cisco IOS Release 12.2 Documentation Set*

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i></li> </ul>	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
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Technologies Configuration Guide</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i></li> </ul>	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk Novell IPX

**Table 1** *Cisco IOS Release 12.2 Documentation Set (continued)*

Books	Major Topics
<ul style="list-style-type: none"> <li><i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li><i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <li><i>Cisco IOS Voice, Video, and Fax Configuration Guide</i></li> <li><i>Cisco IOS Voice, Video, and Fax Command Reference</i></li> </ul>	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> <li><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li><i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
<ul style="list-style-type: none"> <li><i>Cisco IOS Security Configuration Guide</i></li> <li><i>Cisco IOS Security Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li><i>Cisco IOS Switching Services Configuration Guide</i></li> <li><i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> <li><i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li><i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Command Reference</i></li> </ul>	General Packet Radio Service

**Table 1** *Cisco IOS Release 12.2 Documentation Set (continued)*

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Terminal Services Configuration Guide</i></li> <li>• <i>Cisco IOS Terminal Services Command Reference</i></li> </ul>	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• <i>New Features in 12.2-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.2 T</i></li> <li>• <i>Release Notes</i> (Release note and caveat documentation for 12.2-based releases and various platforms)</li> </ul>	

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

## Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

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

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

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

- For emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

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

- For nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

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

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



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

# Obtaining Technical Assistance

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

## Cisco Technical Support & Documentation Website

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

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

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

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



### Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



### Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.



## Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and the *Catalyst 6500 Series Cisco IOS Command Reference* publications.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

© 2003–2006, Cisco Systems, Inc.  
All rights reserved.

---

