# Release Notes for Cisco IOS Release 12.2SXF and Rebuilds

March 29, 2011

## Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases

For Release 12.2(33)SXH and later releases, see this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

## Release Notes for Cisco IOS Release 12.2(18)SXF and Rebuilds

This publication applies to these platforms with Release 12.2(18)SXF and rebuilds:

- 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)

See this product bulletin for information about the standard maintenance and extended maintenance 12.2SX releases:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd804f0694.html

These release notes are for Cisco IOS Release 12.2(18)SXF and rebuilds 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/en/US/prod/collateral/switches/ps5718/ps708/prod_end-of-life_notice0900aecd80699ddb.html

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

The most current version of these release notes are available on Cisco.com at this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

**Tip** For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

**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.

# Chronological List of Releases

**Note**

- See the "Feature Sets" section on page 115 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:

- 29 Mar 2011—Release 12.2(18)SXF17b
- 19 Mar 2010—Release 12.2(18)SXF17a
- 30 Sep 2009—Release 12.2(18)SXF17
- 05 Mar 2009—Release 12.2(18)SXF16
- 29 Oct 2008—Release 12.2(18)SXF15a
- 05 Sep 2008—Release 12.2(18)SXF15
- 09 May 2008—Release 12.2(18)SXF14
- 17 Feb 2008—Release 12.2(18)SXF13
- 15 Jan 2008—Release 12.2(18)SXF12a
- 19 Nov 2007—Release 12.2(18)SXF12
- 21 Sep 2007—Release 12.2(18)SXF10a
- 18 Sep 2007—Release 12.2(18)SXF11
- 16 Jul 2007—Release 12.2(18)SXF10
- 21 May 2007—Release 12.2(18)SXF9
- 07 Mar 2007—Release 12.2(18)SXF8
- 30 Jan 2007—Release 12.2(18)SXE6b
- 12 Dec 2006—Release 12.2(18)SXD7b

- 30 Nov 2006—Release 12.2(18)SXF7
- 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

These releases support the hardware listed in the "Supported Hardware" section on page 33:

- Release 12.2(18)SXF17b:
  - Date of release: 29 Mar 2011
  - 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)SXF17a
- Release 12.2(18)SXF17a:
  - Date of release: 19 Mar 2010
  - 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)SXF17
- Release 12.2(18)SXF17:
  - Date of release: 30 Sep 2009
  - 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)SXF16
- Release 12.2(18)SXF16:
  - Date of release: 05 Mar 2009
  - 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)SXF15a
- Release 12.2(18)SXF15a:
  - Date of release: 29 Oct 2008
  - 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)SXF15
- Release 12.2(18)SXF15:
  - Date of release: 05 Sep 2008
  - 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)SXF14

- Release 12.2(18)SXF14:
  - Date of release: 09 May 2008
  - 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)SXF13
- Release 12.2(18)SXF13:
  - Date of release: 17 Feb 2008
  - 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)SXF12
- Release 12.2(18)SXF12a:
  - Date of release: 15 Jan 2008
  - 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)SXF12
- Release 12.2(18)SXF12:
  - Date of release: 19 Nov 2007
  - 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)SXF11
- Release 12.2(18)SXF11:
  - Date of release: 18 Sep 2007
  - 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)SXF10
- Release 12.2(18)SXF10a:
  - Date of release: 21 Sep 2007
  - 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)SXF10
- Release 12.2(18)SXF10:
  - Date of release: 16 Jul 2007
  - 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)SXF9
- Release 12.2(18)SXF9:
  - Date of release: 21 May 2007
  - 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)SXF8
- Release 12.2(18)SXF8:
  - Date of release: 07 Mar 2007
  - 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)SXF7
- Release 12.2(18)SXF7:
  - Date of release: 30 Nov 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)SXF6
- 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)SXE6b:
  - Date of release: 30 Jan 2007
  - 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)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)SXD7b:
  - Date of release: 12 Dec 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)SXD7a
- 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/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html

- 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/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

- 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/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

- 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/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
- 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/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html

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 193 and refer to this publication:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_release_notes_list.html

For a list of the Release 12.2 S caveats that apply to Release 12.2SX, see the "Caveats" section on page 193 and refer to this publication:

http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html

# 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 13
- FPD Upgrades, page 13

## 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 Upgrades

**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)

See this publication:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76fpd.html

# Cisco IOS Software Modularity

These sections describe Cisco IOS Software Modularity:

- Cisco IOS Software Modularity Documentation, page 13
- Cisco IOS Software Modularity Unsupported Features, page 14

**Note** To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

## 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/en/US/docs/ios/swmod/configuration/guide/sw_mod_instl_cfg.html

- Cisco IOS Software Modularity Command Reference:

  http://www.cisco.com/en/US/docs/ios/swmod/command/reference/sm_book.html
- Embedded Event Manager:

  http://www.cisco.com/en/US/docs/ios/12_2sx/sw_modularity/configuration/guide/evnt_mgr.html

## Cisco IOS Software Modularity Unsupported Features

Cisco IOS Software Modularity does not support these features:

- Hardware:
  - All Optical Services Modules (OSMs)
  - With releases earlier than Release 12.2(18)SXF7, all SIPs and SPAs

  **Note** In Release 12.2(18)SXF7 and later releases, Cisco IOS Software Modularity supports 7600-SIP-400 and 7600-SIP-200. 7600-SIP-600 remains unsupported.

  - 7600-SSC-400 Services SPA Carrier (SSC) and SPA-IPSEC-2G IPsec SPA
  - ACE10-6500-K9 Application Control Engine (ACE) module
  - CE20-MOD-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, the WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)

  **Note** In Release 12.2(18)SXF5 and later releases, Cisco IOS Software Modularity supports the WS-SVC-WISM-1-K9 Wireless Services Module (WiSM).

- Software:

  **Note** With releases Cisco IOS software modularity image earlier than Release 12.2(18)SXF8, to avoid a reload, do not enter any IP SLA **rtr** commands. This problem is resolved in Release 12.2(18)SXF8 by CSCek65370**.** (CSCek58966)

  - 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)

# 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 15
- General Limitations and Restrictions, page 16
- FlexWAN Limitations and Restrictions, page 24
- OSM Limitations and Restrictions, page 25
- Service Module Limitations and Restrictions, page 26

## 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:

- CSCtc06097: VPNSM: %ACE-3-TRANSERR for more than 4 deny ACEs in a crypto ACL
- CSCse75774: Slow multicast traffic recovery for sup uplinks after switchover
- CSCsx32355:Policy base routing broken due to log keyword on outgoing interface
- CSCtb09290: Problem with accounting Giant packets at FW
- With a channelized T3 SPA that is configured for MLP, packets or fragments on a multilink interface with a differential delay that is larger than 70 ms are dropped, and the counters in the output of the **show ppp multilink** command are not updated. There is no workaround. Sequential fragments on different T1 links can be delayed only up to 70 ms. A delay of up to 100 ms is currently not supported, nor is accounting for fragments (good, reordered, or lost). (CSCef82225)
- With releases Cisco IOS software modularity image earlier than Release 12.2(18)SXF8, to avoid a reload, do not enter any IP SLA **rtr** commands. This problem is resolved in Release 12.2(18)SXF8 by CSCek65370. (CSCek58966)
- 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. Enter a **logging event link status** command on each interface where you want the messages enabled. (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)
- Encryption in software on the MSFC is supported only for administrative connections (SSH) to Catalyst 6500 series switches and Cisco 7600 series routers. Software-based IPsec features are not supported.
- 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/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_iosswrel_TSD_Products_Feature_Guide.html

  (CSCed30692)
- The PFC3A and PFC3BXL incorrectly apply egress IP ACLs to MPLS-tagged traffic. (CSCed29392, CSCed16560)
- With an ingress policer, the PFC3BXL overpolices 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 MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (CSCse86399)

- 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 unreachables** 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 unreachables** 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 ip access-list** and **show ipv6 access-list** commands display statistics only for traffic that matches ACLs processed in software on the MSFC. The commands do 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)
- With the tunnel MTU size configured to 9216 bytes, tunnel packets larger than 9211 bytes are corrupted.

  **Workaround**: None. (CSCec04627)
- 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)

## 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)

- 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)

## 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)
- On a system configured with a Supervisor Engine 720 and an OSM-1CHOC12/T1-SI, the output of the **show policy-map interface** command might display a packet counter of 0 for a serial interface. This problem occurs when packets have been process-switched in software on the MSFC instead of fast-switched, and then a reload occurs with one of these saved configurations:
  - When you enter these commands to configure an ACL:
    **access-list** *199* **permit ip any any log**
    **interface** *s1/1.1/1:0.2*
    **ip access-group** *199* **out**

- When you enter these commands to configure IP header-compression:
  **interface** *Serial1/1.1/1:0*
  **encapsulation frame-relay**
  **frame-relay ip tcp header-compression**
  **service-policy output TEST**

**Workarounds**:

- Enter the **no frame-relay ip tcp header-compression** command or the **no frame-relay ip rtp header-compression** command, and then reload the system.
- Avoid using the **log** keyword in an IP ACL with a QoS LLQ or a CBWFQ policy. If you use the **log** keyword, counters may stay at 0 in the output of the **show policy-map interface** command.

(CSCsg58652)

## Service Module Limitations and Restrictions

- DHCP snooping does not work properly if DHCP packets to or from a WS-SVC-WLAN-1-K9 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.

- 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, continous 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
```

(CSCse67713, CSCse53484)

- 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)

- 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)

# Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:

**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 **show vlan virtual-port** command displays the number of virtual interfaces.
- These maximum numbers of virtual interfaces are supported:

| MST | RPVST+ | PVST+ |
|---|---|---|
| 50,000 total<br>30,000 total with Release 12.2(17b)SXA (CSCed33864[1]) | 10,000 total | 13,000 total |
| 6,000[2] per switching module | 1,800[2] per switching module | 1,800[2] 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/products/hw/switches/ps708/tsd_products_support_troubleshoot_and_alerts.html

# System Software Upgrade Instructions

See this publication:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080116ff0.shtml

# Notices

The following notices pertain to this software license.

## OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

### OpenSSL License:

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.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.