Release Notes for Cisco MGX 8880 VXSM Software Release 5.4.20

Revised: August 20, 2010, OL-11772-01

Contents

The content of this document is arranged into the following major sections:

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

About This Release

This release note describes the system requirements, new features, and limitations that apply to Release 5.4.20 of the Cisco Multiservice Switch (MGX) 8880 Media Gateway, and provide Cisco support information.

Note As part of this release package, VXSM 5.4.20 is compatible with PXM 5.4.30.

Note To verify that you have the latest version of Cisco IOS required to support the new features included in this release, please check Cisco IOS availability status at Cisco.com.

For information about new Cisco Voice Switch Service Module (VXSM) features, refer to the *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.4.20*.

For information about new Cisco Voice Inernetworking Service Module (VISM)-Premium (PR) features, refer to the *Release Notes for the Cisco Voice Interworking Service Module (VISM), Release 3.3.30*.

Type of Release

Release 5.4.20 is a VXSM release for the Cisco MGX 8880 media gateway.

Locating Software Updates

Release 5.4.20 software is located at:

http://www.cisco.com/kobayashi/sw-center/wan/wan-planner.shtmlnp

Route processor module (RPM) Cisco IOS software images are located at:

http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml

Features in VXSM Release 5.4.20

No new features are introduced in VXSM Release 5.4.20. For information about open and resolved caveats, refer to *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.4.20*

Release 5.4.00 Features

This release includes the following new features for the Cisco MGX 8880 platform:

DTMF Squelching

This release contains the enhancements to completely squelch DTMF digits. This feature can be provisioned using the CLI commands shown below.

Note These CLI commands are not new for this release. They already exist in the product.

For H.248

Syntax Description **cnfh248profdtmf <Index> <DigitOnDuration> <DtmfPauseDuration> <DetectLongDigitDuration> <SuppressBearerDigit>**

Option SuppressBearerDigit should be set to **1** to enable DTMF squelching.

For XGCP

Syntax Description **cnfxgcpprofdtmf <ProfileIndex> <SuppressBearerDigit>**

Option SuppressBearerDigit should be set to **1** to enable DTMF squelching.

Call Rate Performance Support

VXSM OC3 Card supports the following call rates:

- In MGCP, the maximum CPS supported is 60 (without signaling). If signaling (M3UA/IUA/RUDP) is configured, then the maximum supported CPS is 35.
- In H.248, the maximum CPS supported is 85 (without signaling). If signaling (M3UA/IUA) is configured, then the maximum supported CPS is 35.

V.110 Support for AAL2 Trunking Applications

VXSM supports the detection and handling of V.110 traffic used for modem and fax devices on mobile networks. This feature is used in conjunction with the AAL2 Trunking function. Upon detection of a V.110 bit pattern, VXSM provides a Clear Channel circuit for the duration of the V.110 (data) session.

The V.110 feature adds the following commands:

cnfeventmapping -v110	Configure V.110 events mapping
dspeventmapping -v110	Display V.110 events mapping
addccdprof	Add clear channel data profile
cnfccdprof	Configure clear channel data profile
delccdprof	Delete clear channel data profile
dspccdprof	Display clear channel data profile
dspccdprofs	Display clear channel data profiles

Unique Virtual Gateway Domain Name for H.248

For H.248 applications, a VXSM card has the capability of being partitioned into a number of virtual media gateways (VMGs); where each VMG is a logical entity residing within a physical VXSM card. This feature permits each virtual gateway to be assigned its own unique domain name.

The Unique Virtual Gateway Domain Name feature modifies the following commands:

addh248assoc	Add H.248 association
cnfh248mg	Configure H.248 media gateway
dsph248assoc	List configuration of H.248 Association
dsph248mg	List configuration of H.248 Gateway

ptime Support for H.248

The **ptime** (packet period) attribute is defined in RFC 2327 as “the length of time in milliseconds represented by the media in a packet.” **ptime** specifies the packet period for a codec, and **maxptime** specifies the maximum packet period.

The **ptime** and **maxptime** attributes are optional SDP attributes that can be sent down by the MGC in the local or remote descriptor SDP.

In release earlier than 5.4.00, the values of **ptime** and **maxptime** were ignored and the values configured on the platform were used.

Bidirectional Forwarding Detection Version 1

Bidirectional Forwarding Detection version 1 (BFDv1) improves protocol convergence times by rapidly detecting failures in the path between routers. This is especially important for media that does not provide failure signaling, such as Ethernet, because the OSPF protocol can take a second or more to detect a signaling loss using hello messages. This is too long for some applications and can result in excessive data loss, especially at gigabit rates. BFDv1 quickly detects a media failure so that the OSPF protocol can quickly update routes.

DSCP Marking on RPM-XF Management Interface

Cisco IOS Release 12.4(14)T supports Differentiated Services Code Point (DSCP) or IP Precedence marking for quality of service (QoS) configurations on the RPM-XF management back cards. With this enhancement, the RPM-XF supports Layer 3 QoS on the Fast Ethernet management back card.

Limitations

The following limitations apply to the DSCP marking of management packets on the RPM_XF management back card:

- The RPM-XF does not support DSCP marking for the interface to the MGX switch cell bus.
- The RPM-XF management back card can be used for only management traffic, not data traffic.

Flash MIB Support

Network management systems (NMS) can manage software images stored in boot flash using SNMP when the device supports the CISCO-FLASH-MIB. The RPM-XF supports the CISCO-FLASH-MIB in Cisco IOS Release 12.4(14)T and later releases. For MGX 8800/8900 multiservice switches, the NMS can query objects defined in the CISCO-FLASH-MIB through the PXM management interface or the RPM-XF management interface.

SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) is an standards-based protocol for network management. SNMPv3 provides secure access to devices using a combination of authentication and encryption of packets over the network. This assures that data can be collected securely from SNMP devices and that configuration messages cannot be viewed or altered.

The security features provided in SNMPv3 are:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being seen by an unauthorized source.

Trap Squelch Feature

The large number of traps a large system can generate can degrade the performance of a network management system. The trap squelch feature helps limit the number of traps that Cisco MGX switches generate. You can either block all traps of a specific type or limit the rate of specified traps.

Limitations

The following limitations apply:

- The squelch list holds up to 200 trap types.
- The minimum value of the sampling interval is five minutes and the maximum value is 30 minutes.

MPSM Licensing Changes

This release enforces licenses through sales and support, rather than through software locks. You must purchase licenses for the services and features that you plan to use on each Multiprotocol Service Module (MPSM) card.

For more information, see *Cisco MGX 8800/8900 Series Software Configuration Guide*.

Release 5.3.10 Features

Release 5.3.10 includes the following new features and warnings.

Enhanced VXSM Card Support

Release 5.3.10 supports the Processor Switch Module Hard Disk Voice (PXM-HDV) back card, which supports four or more VXSM cards on an MGX 8880 media gateway. The size of the D partition on the PXM-HDV back card is 2000 Mb.

Non-redundant Upgrade Procedure

To migrate from PXM-HD to PXM-HDV back cards in a non-redundant configuration, perform the following steps:

Step 1 Upgrade the PXM boot and runtime images to release 5.3.10 using the normal upgrade procedure.

Step 2 Upgrade boot and runtime to 5.3.10.

Step 3 Enter the **saveallcnf** command and the saved configuration file to another host using FTP.

Step 4 Replace the PXM-HD back card with the PXM-HDV back card.

Step 5 Retrieve the saved configuration file using FTP.

Step 6 Enter the **restoreallcnf** command.

Redundant Upgrade Procedure

To migrate from PXM-HD to PXM-HDV back cards in a redundant configuration, perform the following steps:

Step 1 Upgrade the PXM boot and runtime images to release 5.3.10 using the normal upgrade procedure.

Step 2 Replace the standby card back card with a PXM-HDV back card and wait for the PXM-HDV back card to retrieve configuration information from the active PXM-HD back card.

Step 3 Enter the **switchcc** command to force a switchover.

Step 4 Replace the remaining back card with a PXM-HDV back card.

Cisco MGX 8800 Series Operating and Storage Environment

This section describes the operating and storage environments for the Cisco MGX 8880 media gateway, and explains how to prevent oxidation and corrosion problems.

Guidance for Operating and Storage Environments

Dew points indicate the amount moisture in the air. The higher the dew point, the higher the moisture content of the air at a given temperature. Dew point temperature is defined as the temperature to which the air would have to cool (at constant pressure and constant water vapor content) in order to reach saturation. A state of saturation exists when the air is holding the maximum amount of water vapor possible at the existing temperature and pressure

When the Relative Humidity is high, the air temp and dew point temperatures are very close. The opposite it true when the Relative Humidity is low. When the dew point temperature and air temperature are equal, the air is saturated with moisture. Locations with high relative humidities have air that is close to being saturated with moisture. When saturated air cools it cannot hold as much moisture and can cause moisture migration and penetration into the system. This moisture can cause corrosion of internal components.

A storage environment that experiences temperature and/or humidity variations over a short period of time can create a condensing environment, and this is considered an uncontrolled environment. An environment that maintains constant temperature and humidity is considered and climate controlled environment. *A temperature and humidity controlled operating and storage environment is required at all times to prevent condensation that can subsequently lead to oxidation of plated metal parts.* Cisco recommends that both long term and short term storage environments be climate controlled to prevent humidity and temperature variations that create condensation. Buildings in which climate is controlled by air-conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for system equipment.

Note Consult your facilities engineers to evaluate and ensure your storage environment meets the definition of a non-condensing environment.

To prevent oxidation, avoid touching contacts on boards and cards, and protect the system from extreme temperature variations and moist, salty environments.

Operating Environment Specifications

The following specifications define the operating environment:

- Temperature, ambient
  - Minimum Temperature: 32 degrees Fahrenheit (0 degrees Celsius)
  - Maximum Temperature: 104 degrees Fahrenheit (40 degrees Celsius)
- Humidity, ambient (non-condensing)
  - Minimum: 10%
  - Maximum: 85%
- Altitude
  - Minimum: Sea level
  - Maximum: 10,000 feet (3,050 meters)

Non-operating and Storage Environment Specifications

The following specifications define the non-operating and storage environments:

- Temperature, ambient
  - Minimum: -4 degrees Fahrenheit (-20 degrees Celsius)
  - Maximum: 149 degrees Fahrenheit (65 degrees Celsius)
- Humidity, ambient (non-condensing)
  - Minimum: 5%
  - Maximum: 95%
- Altitude
  - Minimum: Sea level
  - Maximum: 10,000 feet (3,050 meters)

Release 5.3.00 Features and Enhancements

This release includes the following new features for the Cisco MGX 8880 platform:

VXSM Enhancements

For information about VXSM enhancements, refer to *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.4.20*.

Security Enhancements

This release introduces the following security enhancements:

- PXM45—Secure File Transfer (SFTP).
- RPM-XF—Secure Shell (SSH) for RPM-XF.
- Access control for the shellcon command.

SFTP and SSH Features

Cisco MGX switches currently support the following remote access applications and protocols:

- Telnet, FTP, and SSH on the PXM45 controllers
- Telnet and FTP on the RPM-XF and RPM-PR cards

This release adds SFTP to the PXM45 card and SSH to the RPM-XF card. SFTP is an alternative to FTP that provides for secure (and authenticated) file transfer between a PXM card and a remote host.

For more information about managing Telnet and SSH features, see the following:

- *Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Configuration Guide, Release 5.2*
  - Managing Telnet Access Features section
  - Starting and Managing Secure (SSH) Access Sessions Between Switches section
- *Release Notes for Cisco MGX Route Processor Module (RPM-XF) Cisco IOS Release 12.4(14)T for PXM45-based Switches, Release 5.4.00*
  - Secure Shell (SSH) section

SFTP Limitations

The SFTP feature has the following limitations:

- Maximum of 4 simultaneous sessions
- Sessions have an infinite timeout
- Must use forward slash (/) for path names
- The following SFTP commands are not supported:
  - chown
  - chmod
  - chgrp
  - ln
  - rename, with absolute filenames
  - Symlink

Disabling Telnet and FTP

By default, the PXM45 permits unsecured access from Telnet and FTP clients, as well as secure access from SSH and SFTP clients. A new option (16) of the **cnfndparm** command, along with an existing option (15), disables unsecured Telnet and FTP access from remote hosts, while permitting secure SFTP and SSH sessions.

Option 15	Type **yes** to disable Telnet access to this switch. Type **no** to enable Telnet access. Default: no (Telnet access is enabled)
Option 16	Type **yes** to disable unsecured access to this switch, either Telnet or FTP. Changing this option from **no** to **yes** automatically changes Option 15 to **yes**. Changing from **yes** to **no** has no affect on Option 15. Default: no (Unsecured access is enabled)

If you plan to use SFTP and SSH on the PXM45, you should consider disabling FTP and Telnet access to improve security. Telnet and FTP transfer all user ID, password, and session management information between the client and the PXM45 using clear text. Clear, or unencrypted, text can be read by network analysis and snooping tools.

Initializing SFTP

Upgrading PXM software is not sufficient to initialize and enable the SFTP feature. You must initialize the *sshd_config* file and reset the MGX chassis. Because resetting a chassis can interrupt traffic, you should initialize SFTP before upgrading software so you don't need to reset it later.

To initialize SFTP, perform the following steps:

Step 1 Initiate an FTP session with the PXM card.

Step 2 Change to the F:/SSHD directory.

Step 3 Get the *sshd_conf* file from the F:/SSHD directory.

Step 4 Append the line *subsystem sftp sftp* to the file.

Step 5 Put the *sshd_conf* file into the F:/SSHD directory.

Step 6 Proceed with the normal software upgrade procedure. Alternatively, enter the **resetsys** command to reset the chassis.

Note The **resetsys** command interrupts all traffic on the MGX chassis.

Remote IP Management Connection Enhancements

You can manage an MGX 8850 node directly from an Ethernet or console port on the PXM, or you can configure a remote path to the PXM through a service module or route processor module. The following management paths are supported in prior releases:

- AXSM or MPSM to PXM
- RPM-XF or RPM-PR to PXM

Earlier releases supported intranode connections only, and you could only have one PVC between an RPM and PXM. Release 5.3.00 enhances the atm0 feature to internode connections, where an RPM on one MGX switch connects to PXMs on other MGX switches using PNNI. And now you can manage multiple PXMs from a single RPM.

Management Connection Limitations

The IP addresses of hosts accessing the MGX 8850 node are stored in a RAM cache. Because this cache has a limit of 50 entries, only 50 IP hosts can actively access the node at one time. New IP hosts are blocked until the cache clears (as result of inactivity from some hosts) to make room for new entries.

Multiple RPMs can connect to the same PXM, but each RPM can have only one connection to the PXM. This is because the PXM has a single atm0 address.

Note If you are connected to the MGX switch using the RPM and accidentally delete the SPVC, the connection drops. To restore RPM access, you must re-add the SPVC using the console port or Ethernet port.

Note The **clrallcnf**, **clrcnf**, or **clrsmcnf** commands clear management connections. To restore RPM access, you must reconfigure the RPM and PXM cards for IP connectivity using the console port or Ethernet port.

Configuring an RPM Management Connection

The following quick start procedure summarizes the RPM configuration procedure. This procedure assumes the RPM already has a switch partition configured for the management connection.

	Command	Action
Step 1	**switch partition**	Create and configure a partition for switch 1, as necessary.
Step 2	**interface sw1**.<subif> **point-to-point**	Configure a point-to-point subinterface on switch 1.
Step 3	**ip address** <address> <mask>	Assign an IP address to the switch subinterface. This IP address must be in the same subnet as the atm0 port of the PXM card.
Step 4	**pvc** <vpi>/<vci> **ubr** <rate>	Configure a PVC on the switch subinterface. **Note** Specify 0 for the VPI. **Note** In Release 5.3.00, the rate is configurable.
Step 5	**switch connection vcc** <vpi> <vci> **master remote**	Add a slave endpoint to the switch subinterface.
Step 6	**show switch connection vcc** <vpi> <vci>	Display the slave connection parameters, which include the NSAP address.

The following quick start procedure summarizes the PXM configuration procedure.

	Command	Action
Step 1	**dspndparm**	Verify that the PXM is configured for atm0 as a switch management interface.
Step 2	**ipifconfig atm0** <address> <mask>	Assign an IP address to the atm0 port, as necessary. This IP address must be in the same subnet as the switch interface on the RPM card.
Step 3	**svcifconfig atm0 remote** <nsap> **pvc** <vpi>.<vci>	Add a master connection endpoint. Use the NSAP address and VPI/VCI of the slave endpoint.
Step 4	**dspsvcif**	Verify that the connection is up.
Step 5	**routeshow**	Verify that the RPM IP address is displayed in the route table.

Example Management Configuration

This example shows how to configure a management connection between an RPM-XF on one switch and the PXM on another switch. In this example, the RPM-XF switch partition and the PXM atm0 interface are already available.

The following example configures the RPM-XF switch interface, adds a slave connection, and displays the NSAP address.

```
Router(config)#interface switch1.100 point-to-point
Router(config-subif)#ip address 10.10.10.200 255.255.255.0
Router(config-subif)#pvc 0/100
Router(config-if-atm-vc)#ubr 1544
Router(config-if-atm-vc)#switch connection vcc 0 100 master remote
Router(config-if-swconn)#end
Router#show switch connection vcc 0 100
----------------------------------------------------------
Alarm state           : No alarm
Local Sub-Interface   : 100
Local VPI             : 0
Local VCI             : 100
Remote NSAP address   : default
Local NSAP address    : 47.009181000104000ABCD7777.000001011802.00
Remote VPI            : 0
Remote VCI            : 0
```

The following example configures the atm0 interface of the PXM card, adds a master connection to the RPM-XF, and verifies that the connection is state is *up*. The NSAP address and VPI/VCI entered are the values previously displayed at the RPM-XF.

```
LA.8.PXM.a > ipifconfig atm0 10.10.10.144 netmask 255.255.255.0
LA.8.PXM.a > svcifconfig atm0 remote 47.009181000104000ABCD7777.000001011802.00 pvc 0.100
LA.8.PXM.a > dspsvcif
M8850_LA                          System Rev: 05.02   Apr. 25, 2006 16:36:38 PST
MGX8850                                               Node Alarm: NONE
IP CONNECTIVITY SVC CACHE
-----------------------------------------------------------------------
atm (unit number 0):
    Remote AESA: 47.0091.8100.0104.0000.abcd.7777.0000.0101.1802.00
        SPVC VPI.VCI:    0.100 (PCR=3642 cps)
        Flags:           (0x6) ATMARP,LLCENCAP
        State:           (0x1) UP
        RxLCN:           1505          TxLCN:            1505
        LCNindex:        766           LCNcallid:        0x80000001
        Input Frames:    1             Output Frames:    1
        Input Errors:    0             Output Errors:    0
        Input ArpReq:    0             Output ArpReq:    0
        Input ArpRply:   0             Output ArpRply:   0
        Input InArpReq:  0             Output InArpReq:  0
        Input InArpRply: 1             Output InArpRply: 0
...
```

Platform Enhancements

This release adds the following MGX platform enhancements.

- DB Server/Client enhancement

  The server automatically copies database tables to the new directory for a release.

- Software FPGA upgrade on PXM45/C

  Cisco uses this feature to upgrade hardware (Field Programmable Gate Array) FPGA images without introducing new hardware versions. This simplifies the process of adding or changing features and can reduce hardware costs for both Cisco and customers.

- PXM to MPSM QoS enhancement

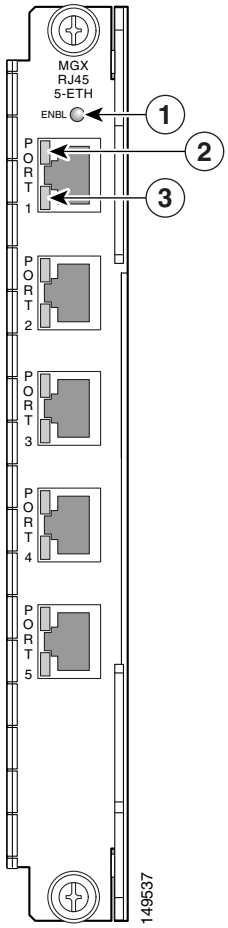
  Currently, traffic sent to the MPSM-T3E3-155 and MPSM-16-T1/E1 cards is managed by the class of service only. For example, the CBR traffic class is always given priority over the VBR.RT traffic class, even if VBR.RT connections are committed and data received is within the SCR limit.

  Through this QoS enhancement, the PXM QE1210 is programmed using information from the MPSM so it can manage traffic dynamically based on the committed rate of the connections and interface policy.

RPM-PR Ethernet Backcard

The MGX-RJ45-5-ETH is a single-height back card for the RPM-PR that provides five RJ-45 connectors for Gigabit Ethernet, Fast Ethernet, or Ethernet lines. Figure 1 shows the MGX-RJ45-5-ETH faceplate.

Figure 1 MGX-RJ45-5-ETH Back Card



1	ENABLE LED • Green—The back card is active. • Off—The back card is not active.	**3**	Port 0 status LED • Green—Data present (flashing). • Orange—The link is up.
2	Port 0 speed LED • Green—1000 Mbps. • Orange—10 Mbps or 100 Mbps.		

Release 5.2.10 Features

Maintenance Release 5.2.10 does not introduce new Cisco MGX 8880 features or enhancements.

Release 5.2.00 Features

Release 5.2.00 introduced the following hardware:

- MGX-VXSM-T3 front card
- VXSM-BC-3T3 back card

MGX-VXSM-T3 Card

Cisco MGX 8880 Release 5.2.00 introduced a third VXSM card for the support of T3 lines. The card consists of a front card with six T3 ports and a half-height back card with three T3 ports. The front card can be configured with either one back card or two back cards.

System Requirements

Table 1 lists Cisco WAN or Cisco IOS products that are compatible with Release 5.4.20.

Table 1 Release 5.4.20 Compatibility Matrix

Switch or Component	Compatible Software Release
MGX 8880 (PXM45/C)	MGX 5.4.30
VXSM	VXSM 5.4.20.201
VISM-PR	VISM 3.3.30
Cisco IOS RPM-XF	12.4(15)T1
Cisco IOS RPM-PR (supported only with VISM-PR cards)	12.4(6)T5
AXSM	AXSM 5.4.30
MPSM	MPSM 5.4.30

MGX 8880 Software Version Compatibility Matrix

Table 2 lists the software that is compatible for use in a switch running Release 5.4.20 software.

Table 2 MGX 8880 Software Version Compatibility Matrix

Board Pair	Boot Software	Runtime Software
PXM45/C	pxm45_005.004.030.200_bt.fw	pxm45_005.004.030.200_mgx.fw
MGX-VXSM-155 MGX-VXSM-T3 MGX-VXSM-T1E1	vxsm_005.004.020.201_bt.fw	vxsm_005.054.020.201.fw (CALEA image) vxsm_005.004.020.201.fw (non-CALEA image)
MGX-VISM-PR-8T1 MGX-VISM-PR-8E1	vism_8t1e1_VI8_BT_3.2.00.fw	vism-8t1e1-003.053.030.200.fw (CALEA image) vism-8t1e1-003.003.030.200.fw (non-CALEA image)
MGX-SRME/B	N/A (obtains from PXM)	N/A (obtains from PXM)
MGX-RPM-PR-512 (supported only with VISM-PR cards)	rpm-boot-mz.124-6.T5	rpm-js-mz.124-6.T5
MGX-RPM-XF-512	rpmxf-boot-mz.124-15.T1	rpmxf-k9p12-mz.124-15.T1 (Crypto image) rpmxf-p12-mz.124-15.T1 (non-Crypto image)
AXSM-1-2488/B AXSM-16-T3/E3/B	axsm_005.004.030.200_bt.fw	axsm_005.004.030.200.fw
AXSM-8-622-XG	axsmxg_005.004.031.200_bt.fw	axsmxg_005.004.031.200.fw
AXSM-16-155-XG	axsmxg_005.004.031.200_bt.fw	axsmxg_005.004.031.200.fw
MPSM-16-T1E1	mpsm16_t1e1_005.004.030.200_bt.fw	mpsm16_t1e1_005.004.030.200.fw mpsm16t1e1ppp_005.004.030.200.fw

SNMP MIB Release

The SNMP MIB release for Release 5.4.20 is *mgx8XXXrel5400mib.tar*.

Note SNMP user guides are replaced by the online MIB tool at: http://tools.cisco.com/ITDIT/MIBS/jsp/index.jsp.

Supported Hardware

This section lists the Cisco MGX 8880 product IDs, 800 part numbers, and revision levels.

Release 5.4.20 Hardware

Release 5.4.20 introduces no new hardware.

Release 5.4.00 introduces no new AXSM-XG hardware.

Release 5.3.10 introduced the following PXM45/C hardware:

PXM-HDV—Back card with 2000-MB hard disk partition

Release 5.3.00 introduced the following RPM-PR back card:

MGX-RJ45-5-ETH—Five-port Ethernet back card

MGX 8880 Product IDs and Card Types

Table 3 lists product IDs, minimum 800 part numbers, and the minimum revision levels for the MGX 8880.

Table 3 MGX Chassis, Card, and Automatic Protection Switching Configurations

Front Card Type	Min. 800 Part Number and Revision	Back Card Types	APS Con	Min. 800 Part Number and Revision
PXM45/C (processor switch module)	800-20217-04-A0	PXM-HDV	—	800-28566-01-A0
		PXM-HD	—	800-05052-03-A0
		PXM-UI-S3/B	—	800-21557-01-A0
MGX-VXSM-155	800-15121-06-A0	VXSM-BC-4-155		800-21428-06-A0
MGX-VXSM-T3	800-4074-02-A0	VXSM-BC-3T3		800-3095-03
MGX-VXSM-T1E1	800-24073-02-A0	VXSM-BC-24T1E1		800-23088-03-A0
MGX-VISM-PR-8T1	800-07990-02-A0	AX-RJ-48-8T1		800-02286-01-A0
		AX-R-RJ-48-8T1		800-02288-01-A0
MGX-VISM-PR-8E1	800-07991-02-A0	AX-SMB-8E1		800-02287-01-A0
		AX-R-SMB-8E1		800-02410-01-A0
		AX-RJ-48-8E1		800-02286-01-A0
		AX-R-RJ-48-8E1		800-02409-01-A0
MGX-SRME/B	800-21629-03-A0	MGX-BNC-3T3-M	—	800-03148-02-A0
		MGX-STM1-EL-1	—	800-23175-03-A0
		MGX-SMFIR-1-155	—	800-14460-02-A0

Table 3 MGX Chassis, Card, and Automatic Protection Switching Configurations (continued)

Front Card Type	Min. 800 Part Number and Revision	Back Card Types	APS Con	Min. 800 Part Number and Revision
MGX-RPM-XF-512	800-09307-06-A0	MGX-XF-UI	—	800-09492-01-A0
		MGX-XF-UI/B	—	800-24045-01-A0
		MGX-1-GE	—	800-18420-03-A0
		MGX-2-GE	—	800-20831-04-A0
		MGX-1OC-12 POS-IR	—	800-08359-05-A0
		MGX-2OC-12 POS-IR	—	800-21300-04-A0
		GLC-LH-SM (was MGX-GE-LHLX)	—	30-1301-01-A0
		GLC-SX-MM (was MGX-GE-SX1)	—	30-1299-01-A0
		GLC-ZX-SM (was MGX-GE-ZX1)	—	10-1439-01-A0
MGX-RPM-PR-512 (supported only with VISM-PR cards)	800-07656-02-A0	MGX-RJ-45-4E/B	—	800-12134-01-A0
		MGX-RJ-45-FE	—	800-02735-02-A0
		MGX-RJ45-5-ETH	—	800-27602-01-A0
AXSM-1-2488/B	800-07983-02-A0	SMFSR-1-2488/B	Yes	800-07255-01-A0
		SMFLR-1-2488/B	Yes	800-08847-01-A0
		SMFXLR-1-2488/B	Yes	800-08849-01-A0
AXSM-16-T3E3/B	800-07911-05-A0	SMB-8-T3	—	800-05029-02-A0
AXSM-8-622-XG	800-21445-06-A0	SMB-8-E3	—	800-04093-02-A0
		SFP-4-622	Yes	800-22143-05-A0

Service Class Template Files

This section contains Service Class Template (SCT) file information for Release 5.4.00.

AXSM and AXSM/B

The AXSM and AXSM/B SCTs have the following characteristics:

- SCT 2—Policing enabled, PNNI
- SCT 3—Policing disabled, PNNI
- SCT 4—Policing enabled, MPLS and PNNI
- SCT 5—Policing disabled, MPLS and PNNI

The file names and checksums for the SCT files are as follows:

- AXSM_SCT.PORT.0.V1: Checksum is = 0x6aadd6c6= 1789777606

- AXSM_SCT.PORT.2.V1: Checksum is = 0x78ccfb22= 2026699554
- AXSM_SCT.PORT.3.V1: Checksum is = 0x987919a7= 2558073255
- AXSM_SCT.PORT.4.V1: Checksum is = 0x775bfaa2= 2002516642
- AXSM_SCT.PORT.5.V1: Checksum is = 0xe84c696a= 3897321834
- AXSM_SCT.CARD.0.V1: Checksum is = 0x6aadd6c6= 1789777606
- AXSM_SCT.CARD.2.V1: Checksum is = 0x78ccfb22= 2026699554
- AXSM_SCT.CARD.3.V1: Checksum is = 0x987919a7= 2558073255
- AXSM_SCT.CARD.4.V1: Checksum is = 0x775bfaa2= 2002516642
- AXSM_SCT.CARD.5.V1: Checksum is = 0xe84c696a= 3897321834

To confirm that the checksum of the SCT file and the file on the node match, enter **dspsctchksum** <filename>.

AXSM-E

The AXSM-E SCTs have the following characteristics:

- CARD and PORT SCT 5—Policing enabled for PNNI, disabled for MPLS
- PORT SCT 6—Policing disabled, used for PNNI ports.
- CARD and PORT SCT 52—Policing enabled on PNNI, disabled on MPLS
- PORT SCT 53—Policing disabled on PNNI and MPLS
- PORT SCT 54— Policing enabled on PNNI, disabled on MPLS
- PORT SCT 55—Policing disabled on PNNI and MPLS

The following are checksums for the new AXSM-E SCT file:

- AXSME_SCT.PORT.5.V1: Checksum is = 0x793c56d0= 2033997520
- AXSME_SCT.PORT.6.V1: Checksum is = 0xe92db9a5= 3912087973
- AXSME_SCT.PORT.52.V1: Checksum is = 0x51241b7a= 1361320826
- AXSME_SCT.PORT.53.V1: Checksum is = 0x34bdf8b9= 884865209
- AXSME_SCT.PORT.54.V1: Checksum is = 0xb5df2c5c= 3051301980
- AXSME_SCT.PORT.55.V1: Checksum is = 0xc5d355c8= 3318961608
- AXSME_SCT.CARD.5.V1: Checksum is = 0x793c56d0= 2033997520
- AXSME_SCT.CARD.52.V1: Checksum is = 0x972810ac= 2535985324

Limitations, Restrictions, and Notes for 5.4.20

This section includes information about limitations, restrictions, and notes pertaining to Cisco MGX Release 5.4.20.

- Due to granularity limitations in the AXSM-E hardware, cell traffic does not reach the configured peak cell rate (PCR) rate when weighted fair queuing (WFQ) is enabled. You must configure connections that have WFQ enabled with a PCR of 101 percent of the actual required rate. Available bit rate (ABR) has the same Qbin priority as the unspecified bit rate (UBR) in the SCT tables. In this case, ABR and UBR share excess bandwidth if WFQ is enabled.

- The VXSM cards, when installed for the first time or after clearing the slot configuration, create a default configuration. The creation of a default configuration involves writing large amount of data to the hard disk in the node.

  When multiple VXSM cards are installed simultaneously or the configuration of multiple VXSM slots are cleared simultaneously, one or more VXSM cards could fail to be installed. This potential failure results in following recommendations (refer to CSCed12646):

  – Install VXSM cards, using the **setrev** command, one at a time. Install another VXSM after the earlier one is completely installed and is Active.

  – Clear the VXSM slot configuration using the **clrsmcnf** command (with no option where the slot primary software version is preserved) one at a time. Wait until the VXSM rebuilds after clearing its slot configuration (without clearing the slot primary software version) before clearing the slot configuration of another VXSM slot.

Upgrading the VISM-PR Image

If you are upgrading the VISM-PR image to Release 3.2.1x or later and the PXM1E or PXM45 image from Release 4.x or earlier to Release 5.x, first upgrade the VISM-PR cards. Then, upgrade the PXM1E or PXM45 cards in the same node.

Do not configure the new VISM features until you have fully upgraded the network. After you upgrade your network to PXM1E or PXM45 Release 5.x or later and VISM-PR to Release 3.2.1x or later, apply the standard upgrade process.

Higher Level Logical Link Limits

The numbers of logical links in the higher levels of the PNNI hierarchy is limited to 30 per level when the complex node configuration is turned on. The limit is essential to reduce the processing time involved in finding the bypasses between the logical links. Each time a significant change occurs in bandwidth in one of the links within the peer group, the bypass calculation is triggered and the bypasses are usually found from one logical link to another.

If there are *n* logical links, the calculation involves finding *n***n* bypasses.

If the number of logical links *n* is large, a lot of processing time is used to calculate the bypasses. Limit the number of logical links per level to 30. To control the number, configure the appropriate number of aggregation tokens for the outside links for that peer group.

Command Line Interface Access Levels

The following notes pertain to configuring command access levels:

- Not all command line interface (CLI) commands are changeable, and a command cannot be changed to CISCO_GP group access level.
- Only the switch software is allowed to generate the binary file. This binary file has an authentication signature which has to be validated before the binary file can be used. Any manual changes to the file make the file void.
- If the binary file becomes corrupted, then the command access levels revert back to the default values during the card bring-up. To recover, repeat the installation process or retain a copy of the binary file and execute a **cnfcli accesslevel install** command on that service module.

- Currently, command names are verified, but an invalid command name might be parsed and added to the binary file. However, this invalid name is ignored later.
- If replication to standby failed, the installation process failed.
- The **cnfcli accesslevel default** command restores all command access levels to default for the service module that this command is executed on. This command does not remove the binary file, and this change is not persistent. If the command is executed on the active card of a redundancy pair, the standby card is not affected. When the card is reset and the binary file exists, it configures from the binary file when it is brought up.

Disk Space Maintenance

Because the firmware does not audit the disk space usage nor remove unused files, the disk space in C: and E: drives must be manually monitored.

Manually delete any unused saved configuration files, core files and firmware files, and the configuration files of the MGX-RPM-PR-512 and MGX-RPM-XF-512 cards to avoid a shortage of disk space required to store event logs: configuration upload files in the C: drive and the configuration of MGX-RPM-PR-512 and MGX-RPM-XF-512 cards in the E: drive.

The following steps are recommended to remove files on the system from the active controller card:

Step 1 Change to the directory that needs grooming.

CLI: **cd** <directory_name>

Step 2 List the directory to identify old files that can be removed and available disk space.

CLI: **ll**

Step 3 Remove any old files (you might also use wild cards in the filename).

CLI: **rm** <complete_filename>

Step 4 List the directory to see if the file was removed and disk space is available.

CLI: **ll**

Saving Configurations

The system keeps only the two most recent copies of the saved system configuration under the C:/CNF directory. You can use FTP to transfer all of the saved configurations under C:/CNF to their local server for future reference. All files under C:/CNF are not replicated over to the standby controller card under any circumstances.

Using the clrsmcnf Command

These notes pertain to the **clrsmcnf** command:

- We do not recommend executing **clrsmcnf** on more than one card at a time
- For the clear service module configuration feature, if there is a controller card switchover before the clear service module configuration operation is complete, the **clrsmcnf** command must be re-issued to ensure that the configuration is completely cleared to avoid an incomplete cleanup.

- For the clear service module configuration feature, using the **clrsmcnf** command might result in discrepancy in the PNNI configuration. For example, some connections might be in the mismatch state.
- If the **clrsmcnf** command is given with the <*all*> option to clear the software version for the slot as well, then the card enters the boot/empty state after the operation is complete.
- If the **clrsmcnf** command is given with the <*all*> option, for cell bus service module, the card enters boot/empty state. For a broadband service module (for example, AXSM or MPSM-155-T3E3), the card enters fail/active state.
- While using the **clrsmcnf** command, the card in the specified slot is not usable until the operation is successfully completed.

AXSM Card Automatic Protection Switching Limitations

These notes pertain to the Automatic Protection Switching (APS) feature:

- For AXSM APS, the back card of the active card must be present for APS to function.
- AXSM cards need the back card of the active front card for the APS to work. This implies that AXSM cards do not support the cross backcard removal—the upper backcard of one AXSM and lower backcard of another AXSM.
- If you remove the upper back card of the active front AXSM, it triggers switching active card. The APS is OK. However, if the lower back card of the current active AXSM is removed at this time, it does not trigger switching the active card because the standby card is missing one of the back cards. The lower backcard APS does not work because the back card of the active front card is missing.
- Port LED lights on AXSM-E front cards indicate the receive status of the physical line connected to it only when the card is in active state. For standby AXSM-E cards, the LEDs always remain green when the lines are in loss of signal (LOS) irrespective of which lines are active (refer to anomaly CSCdv68576).

Path and Connection Trace Features

These notes pertain to the path and connection trace features:

- Path trace is not supported on the control port.
- Path trace does not have the accurate information when there is a crankback on the connect path.
- Path and connection trace support point to point connections.
- Path and connection trace support MPG (multiple peer group) and SPG (single-peer group).

Priority Routing Feature

These notes pertain to the priority routing feature:

Prioritized reroute of soft permanent virtual connection (SPVCs) is not guaranteed if the SPVCs originate on a signaling port. SPVCs might get routed out of order. In-order routing of SPVCs is guaranteed on non-signaling ports.

- RPM does not support configuration of routing priority. All RPM mastered SPVCs are assigned a routing priority of 8 by the PXM.

- Changing the routing priority for DAX connections does not change the priority of the associated SVCs. The SPVCs are not derouted and rerouted if just the endpoint parameters are changed, and routing priority is an endpoint parameter. Also, because DAX connections are never derouted even if the user-network interface (UNI) port stops responding and the **rrtcon** command is not supported for DAX connections, the routing priority change is never reflected. The only way for the routing priority change to be reflected is to execute the **dncon** and **upcon** commands. Because DAX connections are never derouted, the effect of this limitation is voided.
- Priority routing operates in a best effort manner for the following reasons:
  - Two in-order releases can still arrive out of order at the master node if they take two different paths.
  - Under congestion scenarios releases can be expected to be transmitted out-of-order. This is because releases of other calls must not be held up if you are not able to send releases on one of the interfaces because it is congested. The calls that were not released could be higher priority calls.
  - Lower priority SPVCs can be routed ahead of higher priority SPVCs. This can happen if you have repeatedly failed to route higher priority SPVCs. To prevent starvation of lower priority SPVCs, the software starts to route lower priority SPVCs. The software eventually addresses the higher priority SPVCs later.

Soft Permanent Virtual Connection Interoperability

These notes pertain to SPVC interoperability:

- Network-to-Network Interface (NNI) SPVC Addendum Version 1.0 is not supported.
- CC (Continuity Check) is not available at the slave end of a single-end SPVC.
- Reporting AIS detection to Cisco Wide Area Network Manager (CWM) is not available at the slave end of a single-end SPVC.
- The slave end of a single-end SPVC is not visible to CWM.
- If single-end SPVCs originated from MGX switches, they can only be configured through CLI and not from CWM in the current release.
- Single-end provisioning is not supported for DAX connections.
- SPVC statistics are not available for the slave endpoint of a single-end SPVC because this endpoint is nonpersistent.
- When the persistent slave endpoint of an existing SPVC connection is deleted and the master endpoint is allowed to remain, the connection might become established as a single-end SPVC connection. In this case, CWM shows the connection as Incomplete.
- Override of SVC connections on a virtual path identifier (VPI) due to an incoming SPVP request for that VPI is not supported. The following override options are supported only:
  - **spvcoverridesvc**
  - **spvcoverridesvp**
  - **spvpoverridesvp**

Manual Clocking

When **resetcd** is invoked, the primary and secondary (if configured) clock sources are recommitted. However, the clock to which the node is latched is not requalified. Only the backup clock is qualified if present. Recommitted means that the primary and secondary are requalified, and the node temporarily latches onto the internal oscillator. After the clock is requalified, the node locks onto the primary clock source once again.

Enabling Priority Bumping

When you enable priority bumping on the node, you cannot change the booking factor for AXSM signaling ports. You can change the booking factor for non-signaling ports.

Other Limitations and Restrictions

Other limitations and restrictions are as follows:

- When configuring virtual interfaces (for example, VUNI, VNNI, EVUNI, EVNNI), the physical interface must be of all one ATM header type, either UNI or NNI. The signaling that is applied to a virtual port is independent of the actual virtual port ATM header. The only limit is that the VPI value must be within the UNI ATM header limitations.
- If command **clrchancnt** is executed while a **dspchancnt** command is currently active, the displayed data is incorrect. To display correct data, restart the **dspchancnt** after the previous one is complete.
- The **clrsmcnf** command does not work:
  - For redundant service modules.
  - If an upgrade is in progress.
- If RPM-XF is configured as a Label Switch Controller (LSC), execution of **clrsmcnf** command on those LSC slots is rejected.
- Configuration information is not synchronized between processor switch modules (PXMs) during upgrades. If any changes are made to the configuration during upgrades, the standby PXM must be rebooted. The standby PXM must be rebooted when it is in a stable state.

Clearing the Configuration on Redundant PXM45 Card

These notes apply to redundant cards.

- Due to checks to prevent an inserted card from affecting the system, an additional step might be required when inserting two non native PXM45 cards in a shelf. Insert the first PXM45, use the **clrallcnf** command, and allow this to become active before inserting the second PXM45.
- After a **clrallcnf**, explicitly clean up stale SCT files (see anomaly CSCdw80282).

Known MGX 8880 Media Gateway Anomalies

For information about anomalies in MGX Release 5.4.20 on other platforms, refer to the *Release Notes for Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Switches, Release 5.4.10*.

For information about anomalies with the VXSM card, refer to *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.4.20*.

For information about anomalies with the VISM card, refer to *Release Notes for the Cisco Voice Interworking Service Module (VISM), Release 3.3.30*.

Known Route Processor Module Anomalies

For information about anomalies with the MGX-RPM-XF-512 card, refer to *Release Notes for Cisco MGX Route Processor Module (RPM-XF) for PXM45-based Switches, Release 5.4.00*.

For information about anomalies with the MGX-RPM-PR-512 card, refer to *Release Notes for Cisco MGX Route Processor Module (RPM-PR) for MGX Releases 1.3.16 and 5.4.00*.

Related Documentation

A *Guide to Cisco Multiservice Switch Documentation* ships with your product. That guide contains general information about how to locate Cisco MGX, broadband and packet exchange (BPX), service expansion shelf (SES), and CWM documentation online.

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