Cisco IOS Software Release 12.2SX New Features and Hardware Support

PB424302

Last Updated: August, 2007

This Product Bulletin introduces Cisco IOS® Software Release 12.2SX and includes the following sections:

1) Cisco IOS Software Release 12.2SX Introduction

2) Release 12.2(33)SXH Migration, Service Module Support, and Cisco IOS Software Modularity Considerations

3) Release 12.2(33)SXH Highlights

4) Release 12.2SX Additional Information

1) Cisco IOS Software Release 12.2SX Introduction

Cisco IOS Software Release 12.2S is designed for Enterprise campus and Service Provider edge networks that require world-class IP and Multiprotocol Label Switching (MPLS) services.

Derived from Release 12.2(30)S, Release 12.2(33)SXH provides Release 12.2S functionality and new features and hardware support for the Cisco Catalyst 6500 Series Switch.

For detailed information about the features and hardware supported in Release 12.2SX and 12.2(33)SXH, refer to the Cisco IOS Software Release 12.2SX release notes and customer documentation at the following website:

http://www.cisco.com/en/US/products/ps6017/tsd_products_support_series_home.html

Not all features may be supported on all platforms. Use the Cisco Feature Navigator to find information about platform support and Cisco IOS Software image support. Access the Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. You must have an account on Cisco.com.

Cisco IOS Release 12.2(33)SXH is developed for and intended to run on Cisco Catalyst 6500 Series Switches only.

2.1) Release 12.2(33)SXH Migration

Cisco IOS Software Release 12.2(33)SXH is the next Extended Maintenance release, and will be supported for a period of 24 months for Cisco Catalyst 6500 Series Switches. For more details on Release 12.2SX Standard and Extended Maintenance releases please visit:

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

Starting with Cisco IOS Software Release 12.2(33)SXH, the Cisco Catalyst 6500 will be offering the Cisco IOS Software Modular images as a feature set in addition to the Cisco IOS Native

images with full feature parity between them. The 12.2(33) SXH Software Release provides new feature functionality and introduces additional hardware support for the Cisco Catalyst 6500 Series Switch which allows customers to deploy it within the Enterprise campus, Data Center, WAN aggregation and Service Provider edge networks.

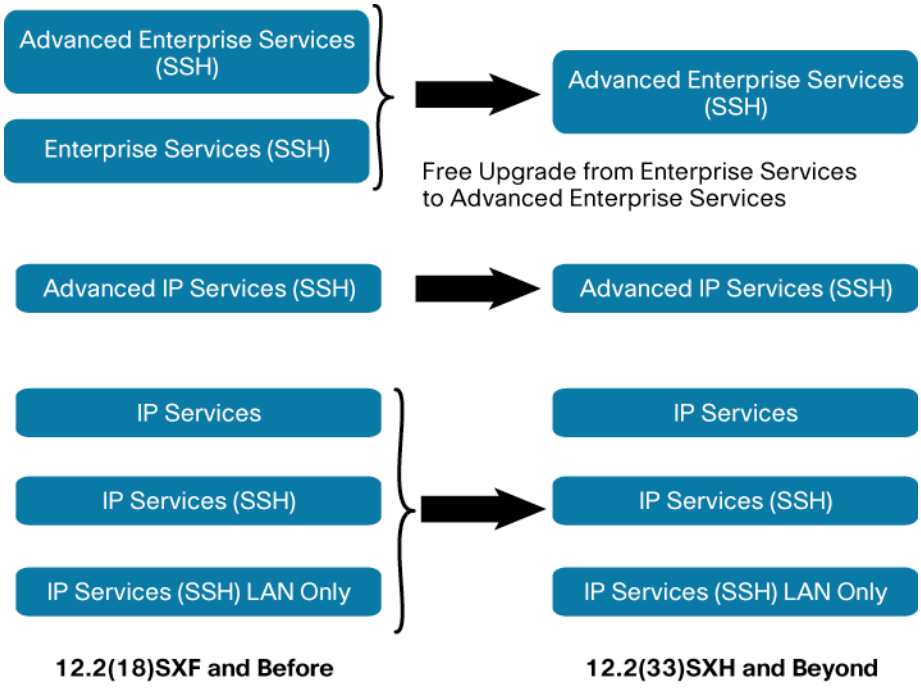
Beginning with Release 12.2(33)SXH, the Cisco Catalyst 6500 Supervisor 720 Enterprise Services software image will no longer be offered. Existing customer's running Cisco IOS Enterprise Services image can receive a free license upgrade to Cisco IOS Advanced Enterprise Services for Supervisor-720 and Supervisor-32 until January 29th 2008.

Cisco IOS Software Release 12.2(33)SXH offers the following images for the Cisco Catalyst 6500 Supervisor Engine 720, Supervisor Engine 32, and ME 6524:

Supervisor-720 IOS Software images:

- Cisco Catalyst 6500 Supervisor 720 IOS IP Services
- Cisco Catalyst 6500 Supervisor 720 IOS IP Services (MODULAR)
- Cisco Catalyst 6500 Supervisor 720 IOS IP Services (SSH) LAN ONLY
- Cisco Catalyst 6500 Supervisor 720 IOS IP Services (SSH) LAN ONLY (MODULAR)
- Cisco Catalyst 6500 Supervisor 720 IOS IP Services (SSH)
- Cisco Catalyst 6500 Supervisor 720 IOS IP Services (SSH) (MODULAR)
- Cisco Catalyst 6500 Supervisor 720 IOS Advanced IP Services (SSH)
- Cisco Catalyst 6500 Supervisor 720 IOS Advanced IP Services (SSH) (MODULAR)
- Cisco Catalyst 6500 Supervisor 720 IOS Advanced Enterprise services (SSH)
- Cisco Catalyst 6500 Supervisor 720 IOS Advanced Enterprise services (SSH) (MODULAR)

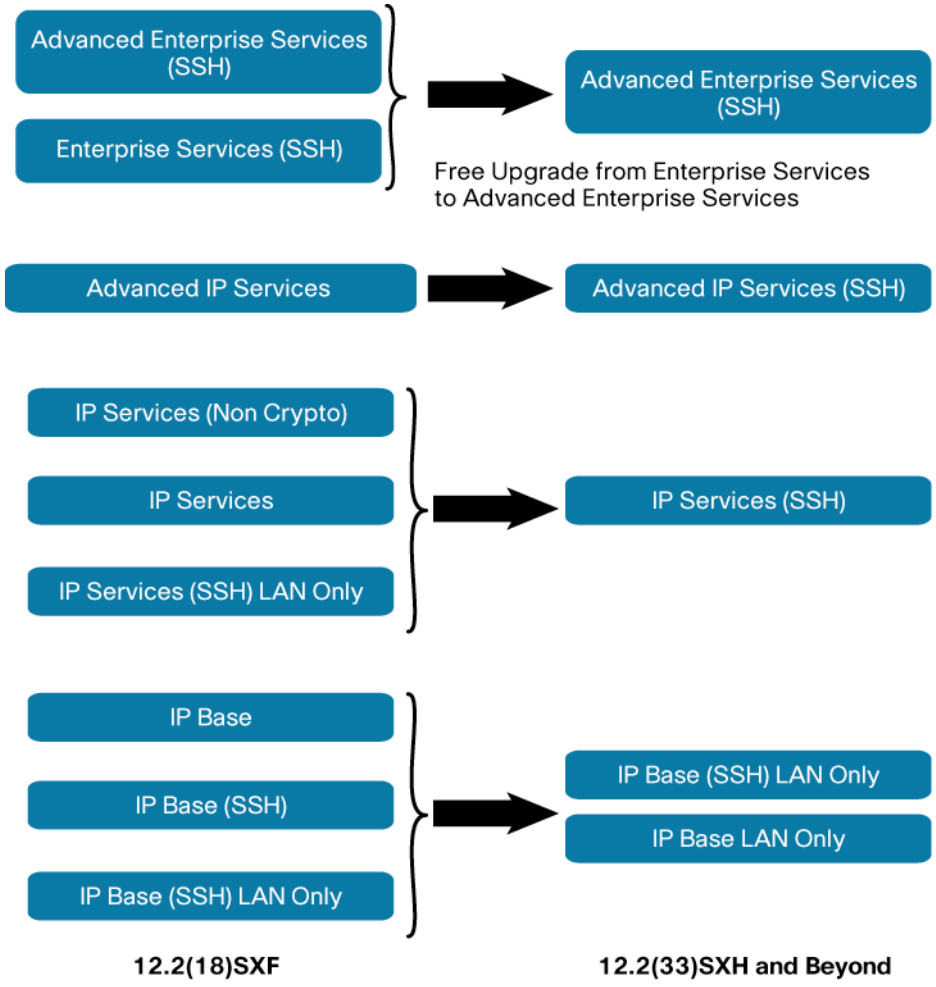
Figure 1. Supervisor-720 Software Image Upgrade to Release 12.2(33)SXH



Supervisor-32 IOS Software images:

- Cisco Catalyst 6500 Supervisor 32 IOS IP Base LAN ONLY
- Cisco Catalyst 6500 Supervisor 32 IOS IP Base LAN ONLY (MODULAR)
- Cisco Catalyst 6500 Supervisor 32 IOS IP Base (SSH) LAN ONLY
- Cisco Catalyst 6500 Supervisor 32 IOS IP Base (SSH) LAN ONLY (MODULAR)
- Cisco Catalyst 6500 Supervisor 32 IOS IP Services SSH
- Cisco Catalyst 6500 Supervisor 32 IOS IP Services SSH (MODULAR)
- Cisco Catalyst 6500 Supervisor 32 IOS Advanced IP Services (SSH)
- Cisco Catalyst 6500 Supervisor 32 IOS Advanced IP Services (SSH) (MODULAR)
- Cisco Catalyst 6500 Supervisor 32 IOS Advanced Enterprise Services (SSH)
- Cisco Catalyst 6500 Supervisor 32 IOS Advanced Enterprise Services (SSH) (MODULAR)

Figure 2. Supervisor-32 Software Image Upgrade to Release 12.2(33)SXH

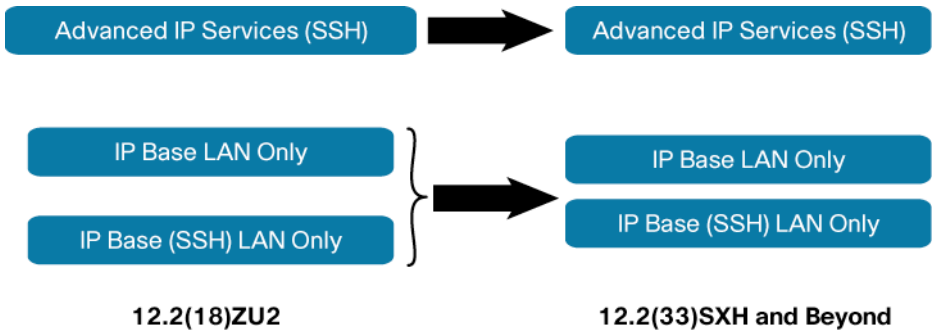


ME6524 Software Feature sets:

- Cisco ME 6524 IOS IP Base (SSH) LAN ONLY
- Cisco ME 6524 IOS IP Base (SSH) LAN ONLY (MODULAR)
- Cisco ME 6524 IOS IP Base LAN ONLY
- Cisco ME 6524 IOS IP Base LAN ONLY (MODULAR)

- Cisco ME 6524 IOS Advanced IP Services (SSH) LAN ONLY
- Cisco ME 6524 IOS Advanced IP Services (SSH) LAN ONLY (MODULAR)

Figure 3. Catalyst 6500 ME-6524 Software Image Upgrade to Release 12.2(33)SXH



Benefits

- Simplifies the total number of software feature set images available to customers.
- Free software license upgrade for customers running Enterprise Services to Advanced Enterprise Services (SSH) for Cisco Catalyst 6500 Supervisor 720 and Supervisor 32. This applies to Cisco IOS Software Release 12.2(33)SXH (and later 12.2SX releases).

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder S Sambi, msambi@cisco.com

2.2) Catalyst 6500 Series Switch Service Module Support In Release 12.2(33)SXH

Release 12.2(33)SXH provides supports for the following Service and WAN modules:

Service Module	Description
ACE10-6500-K9	Application Control Engine Service Module
ACE20-MOD-K9	Application Control Engine 20 Hardware
WS-SVC-CMM	Communication Media Module
WS-SVC-FWM-1-K9	Firewall blade for 6500 and 7600, VFW License Separate
WS-SVC-IDS2-BUN-K9	600M IDSM-2 Mod for Cat
WS-SVC-NAM-1	Catalyst 6500 Network Analysis Module-1
WS-SVC-NAM-2	Catalyst 6500 Network Analysis Module-2
WS-SVC-WiSM-1-K9	Cisco Wireless Services Module (WISM)
7600-SSC-400	Cisco 7600/Catalyst 6500 Services SPA Carrier Card
SPA-IPSEC-2G	Cisco 7600/Catalyst 6500 IPsec VPN SPA, DES/3DES/AES
WS-X6582-2PA	Cisco7600/Catalyst6500 Enhanced FlexWAN, Fabric-enabled
7600-SIP-200	Cisco 7600 Series SPA Interface Processor-200
7600-SIP-400	Cisco 7600 Series SPA Interface Processor-400

The service modules that were supported in Release 12.2(18)SXF (and prior releases) and not supported in Release 12.2(33)SXH are shown below with migration path:

Service Module	Description	Migration Path	Description

Service Module	Description	Migration Path	Description
WS-SVC-AGM-1-K9	Catalyst 6500 Cisco Anomaly Guard Module	AGXT-5650-MMF-B-K9 For more information, please visit: http://www.cisco.com/en/US/netsol/ns615/networking_solutions_sub_solution.html	Cisco Guard XT 5650, 1000Base-SX MMF, Dual AC, RAID
WS-SVC-ADM-1- K9	Catalyst 6500 Cisco Anomaly Detector Module	ADXT-5600-MMF-B-K9 For more information, please visit: http://www.cisco.com/en/US/netsol/ns615/networking_solutions_sub_solution.html	Cisco Traffic Anomaly Detector XT 5600,1000Base MMF
WS-SVC-IPSEC-1	IPSec VPN Services Module for Cisco Catalyst 6500 and Cisco 7600 series	SPA-IPSEC-2G and 7600-SSC-400 For more information, please visit: http://cisco.com/en/US/products/hw/modules/ps2706/prod_eol_notice0900aecd80349e2c.html	Cisco 7600/Catalyst 6500 IPSec VPN SPA with DES/3DES/AES; Cisco 7600/Catalyst 6500 Services SPA Carrier Card
WS-SVC-WLAN-1-K9	Wireless LAN Services Module, CEF256	WS-SVC-WISM-1-K9 For more information, please visit: http://cisco.com/en/US/products/hw/modules/ps2706/prod_eol_notice0900aecd80550b4c.html	Cisco Wireless Services Module (WiSM)
WS-X6066-SLB-S-K9	Content Switching Module with SSL daughter card	ACE10-6500-K9 And ACE20-MOD-K9	Cisco Application Control Engine (ACE-10) Module And Cisco Application Control Engine (ACE-20) Module
WS-X6066-SLB-APC	Catalyst 6000 Content Switching Module	ACE10-6500-K9 And ACE20-MOD-K9	Cisco Application Control Engine (ACE-10) Module And Cisco Application Control Engine (ACE-20) Module
WS-SVC-WEBVPN-K9	WebVPN Services Module (WebVPN or SSLVPN)	See http://www.cisco.com/en/US/products/hw/modules/ps2706/prod_eol_notice0900aecd805813b1.html	See http://www.cisco.com/en/US/products/hw/modules/ps2706/prod_eol_notice0900aecd805813b1.html
WS-SVC-CSG-1	Content Services Gateway	WS-SVC-SAMI-BB with Cisco 7600	Service and Application Module for IP (CSG II)
WS-SVC-PSD-1	Persistent Storage Device Module (PSD)		

2.3) Release 12.2(33)SXH Software Modularity Deployment Considerations

Cisco IOS Software Modularity provides customers multiple benefits in areas of high availability and manageability. The Software Modularity on the Cisco Catalyst 6500 platform has been available to customers starting from Release 12.2SXF4.

Catalyst 6500 Series, Cisco IOS Release 12.2(33)SXH Software Modularity Feature Set Deployment considerations:

Cisco IOS Software Modularity provides customers multiple benefits in areas of high availability and manageability. The Software Modularity feature set option on the Cisco Catalyst 6500 platform has been available to customers since Cisco IOS Software Release 12.2(18)SXF4. With 12.2(33)SXH, the Cisco IOS Software Modularity images will have the following attributes:

- Hardware and software feature consistency between modular and non-modular features sets: while there were certain support restrictions in Release 12.2(18)SXF4, Cisco IOS Software Modularity images (such as no support for IPv6 or MPLS), these have been lifted in Release 12.2(33)SXH.
- The Cisco IOS Software Modularity images will continue to be offered as an optional feature set of Cisco IOS Software Native images.
- The Cisco IOS Software Modular images can be deployed across all the different places in the network including Enterprise Campus, Data Centers, WAN and Carrier Ethernet deployments. However, the new modular infrastructure introduces a few scalability considerations which should be evaluated before selecting the Cisco IOS Software Modularity feature set:

Feature	Scalability Consideration
Multicast	16000 mroutes (PIM Sparse-mode), 8000 mroutes (Bi-Dir PIM), 2000 IGMP groups. 6000 mroutes across 100 mVPN tunnels.
MPLS L3 VPNs (OSPF VRF's)	400 VRFs
Aggressive Protocol Timers	It is recommended that only default timers be used for all IPv4, IPv6 routing and multicast protocols.

3) Release 12.2(33)SXH Feature Highlights

The following sections include Release 12.2(33)SXH hardware and software feature highlights.

Release 12.2(33)SXH, like all 12.2SX releases, integrates innovations that span multiple technology areas, including Cisco IOS High Availability, Quality of Service, MPLS and VPNs, IP Addressing and Services, IP Multicast and Routing, and Infrastructure and Embedded Management.

Table 1. Release 12.2(33)SXH Highlights

Hardware	IP Routing	IP Multicast	MPLS and VPN, AToM
• Catalyst 6500 Series Distributed Forwarding Card • IP 16-way Equal-Cost Multipath (ECMP) • Switched Port Analyzer (SPAN) Enhancements • Cisco IOS Software Modularity Support for SIP-200, SIP-400, and Enhanced FlexWAN SPAs • 50 ms Fabric Stand-by Hot Sync • Cisco IOS Software Modularity for the Catalyst 6500 ME 6524 Ethernet Switch • Inline 802.3af Power Classification Override	• OSPF Graceful Restart (RFC 3623) • Reliable Static Routing Backup Using Object Tracking • OSPF Area Transit Capability • EIGRP Route Map Support • BGP Multicast Inter-AS (IAS) VPN Support • BGP Dual AS Configuration support • BGP IP Prefix Import from Global to VRF Table • BGP Support for Named Extended Community Lists • BGP Support for TCP Path MTU Discovery • BGP Support for Next Hop Address Tracking • Supress BGP Advertisement for Inactive Routes • Per-VRF Assignment of BGP Router-ID • BGP Dynamic Neighbors • Optimized Edge Routing • Cisco IOS Software Modularity for IPv6 Routing (RIPng, OSPFv3)	• MVPN Inter-AS Support • MVPN Extranet • Multicast IPv6 Enhancements • Auto-RP Enhancements • IPv4 Extended ACL for IGMP to Support SSM • IP Multicast Route Standard MIB (IPMROUTE-STD-MIB) • Multicast VPN MIB (CISCO-MVPN-MIB) • MSDP Compliance with IETF RFC 3618 • Triggered PIM Joins • Multicast Router Guard • IGMP Filtering and Snooping Enhancements	• Cisco IOS Software Modularity for L3 VPN Control Plane • AToM: ATM AAL5 over MPLS • AToM: ATM OAM Cell Emulation • AToM: ATM Cell Relay over MPLS • AToM: Ethernet over MPLS • Multiplexed UNI • MPLS Graceful Restart • MPLS LDP Support • VRF Aware Syslog • MPLS Traffic Engineering Enhancements: ◦ AutoTunnel Primary and Backup ◦ Class-based Tunnel Selection ◦ Inter-AS Feature ◦ Fast Reroute (FRR) Link and Node Protection ◦ Fast Reroute (FRR) Prefix Independence ◦ Label Switched Path (LSP) Attributes ◦ Verbatim Path Support ◦ Autotunnel Mesh Groups ◦ Shared Risk Link Groups (SRLG) ◦ NSF/SSO: MPLS TE and RSVP Graceful Restart

MPLS Management	IP Services (including QoS features)	Embedded Management	Integrated Security
• MPLS TE FRR MIB, IETF draft version 01 • MPLS LSP Ping/Trace for MPLS core (LDP IPv4 and RSVP IPv4 FEC support), IETF draft version 03 • IP SLA automation for MPLS LSP Ping/Trace for MPLS core • MPLS LSP Ping for Layer-2 VPNs (via VCCV), IETF draft version 03 • PW-E3 MIB	• Enhanced Object Tracking • (SSO) for HSRP and GLBP • MD5 Authentication for HSRP and GLBP • TCP Maximum Segment Size (MSS) Adjustment • Cisco IOS Auto QoS • CBQOSMIB Index Persistency	• IOS Configuration Rollback • IPv6 Default Router Selection • NetFlow Egress Multicast Enhancement • NetFlow for IPv6 Unicast Traffic • NetFlow MIB and TopNTalkers • NetFlow: per-interface/sub-interface NetFlow • Contextual Diff Utility • Config Logger Persistency • Configuration Change Logging • Exclusive Config Change Access • IPv6 Default Router Selection • Cisco IOS TCL • Embedded Syslog Manager • IP Service Level Agreements (IP SLAs) • Ethernet OAM Protocols: IEEE 802.1ag and 802.3ah • Smart Call Home	• IBNS (802.1x, MAC Authentication Bypass and Web Auth) enhancements • NAC Enhancements • IEEE 802.1x based L2 NAC • Auto Secure • IP Source Guard • Wake on LAN • Policy-Based ACLs (PBACL) • Private Hosts

Hardware

Cisco® Catalyst® 6500 Series Distributed Forwarding Card

The new Cisco® Catalyst® 6500 Series Distributed Forwarding Card (DFC), including WS-F6700-DFC3C and WS-F6700-DFC3XL is an optional daughter card for CEF720-based line cards such as WS-X6704-10GE, WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX. The new Distributed Forwarding Card supports the System Virtualization, provides localized forwarding decisions for each line card and scales the aggregate system performance to reach up to 400+ Mpps.

The key highlights of the new Distributed Forwarding Card are:

- Supports System Virtualization
- Supports all the functions that DFC3B and DFC3BXL support
- Deployed in CEF720 line cards such as WS-X6704-10GE, WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX

Table 2. DFC 3 Supported Combinations

	WS-F6700-DFC3A	WS-F6700-DFC3B	WS-F6700-DFC3BXL	WS-F6700-DFC3C	WS-F6700-DFC3CXL
WS-SUP720	PFC3A functionality	PFC3A functionality	PFC3A functionality	PFC3A functionality	PFC3A functionality
WS-SUP720-3B	PFC3A functionality	PFC3B functionality	PFC3B functionality	PFC3B functionality	PFC3B functionality
WS-SUP720-3BXL	PFC3A functionality	PFC3B functionality	PFC3BXL functionality	PFC3B functionality	PFC3BXL functionality

Table 3 gives specifications of the distributed forwarding card.

Table 3. Specifications of Distributed Forwarding Card

Feature	Cisco Distributed Forwarding Card (DFC3C)	Cisco Distributed Forwarding Card (DFC3CXL)
MAC Entries	96,000	96,000
Memory	512M	1G
IP Routes	256,000 entries	1,000,000 entries
NetFlow Entries	128,000 entries	256,000 entries

Product Numbers

Table 4 gives product numbers and pricing information for Distributed Forwarding Card.

Table 4. Product Numbers

Product Number	Description
WS-F6700-DFC3C	Catalyst 6500 Dist Fwd Card for WS-X67xx modules
WS-F6700-DFC3CXL	Catalyst 6500 Dist Fwd Card-3CXL, for WS-X67xx modules

Minimum Software Requirements

Minimum software requirements for Distributed Forwarding Cards are listed in Table 5.

Table 5. Minimum Software Requirements for New Distributed Forwarding Cards

Product Number	Software Release
WS-F6700-DFC3C	• Cisco IOS Software Release 12.2(18)SXF5 and later with Cisco Supervisor 720 3B if using with WS-X6708-10G-3C line card • Cisco IOS Software Release 12.2(33)SXH and later with all the line cards mentioned above
WS-F6700-DFC3CXL	• Cisco IOS Software Release 12.2(18)SXF5 and later with Cisco Supervisor 720 3B if using with WS-X6708-10G-3CXL line card • Cisco IOS Software Release 12.2(33)SXH and later with all the line cards mentioned above

Benefits

Reduces the Supervisor switch over time from 1.5 seconds to less than 50ms.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

For more information about the Cisco Catalyst 6500 Series Switch, visit http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

Product Management Contact: Pallavi Srinivasa, palsrini@cisco.com

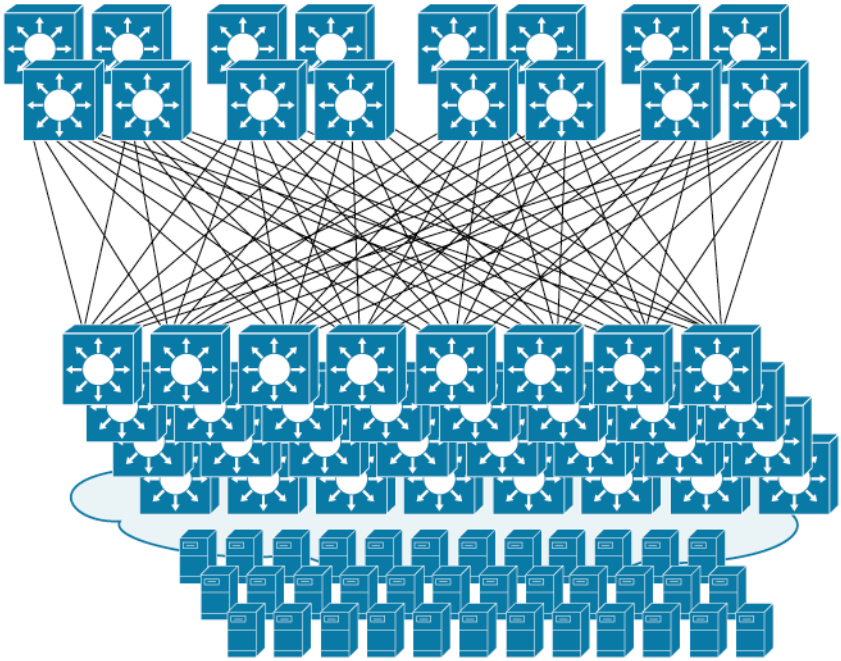
IP 16-way Equal-Cost Multipath (ECMP)

In today's data centers where large content providers need to cluster computers for massive search applications or other data crunching applications using parallel processing, a scalable way of distributing packets across multiple parallel links is needed. Prior to Release 12.2(33)SXH, the Catalyst 6500 supported up to eight equal cross paths in the routing table.

Starting with Release 12.2(33)SXH, the Catalyst 6500 will support a 16-way Equal-Cost Multipath (ECMP) on supervisors for all versions of the Policy Feature Card 3 (PFC3).

An example of the IP 16-way Equal-Cost Multipath feature is shown below in Figure 4. A cluster of server farms is connected to the Catalyst 6500 switches in the access layer, and the access layer is in turn connected to the Distribution layer through 16 parallel paths, either through GigE or 10 GigE. Traffic will be distributed across these 16 parallel paths using the IP 16-way ECMP feature.

Figure 4. IP 16-way Equal-Cost Multipath Feature Topology



This feature is enabled by specifying "maximum-paths" under routing protocols, or it can be configured via static routes.

Benefits

The IP 16-way ECMP feature provides customers optimal traffic scalability, with the capability of pushing more than160 Gigs of throughput between the two switches.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Sanjib HomChaudhuri, sanjib@cisco.com

Switched Port Analyzer (SPAN) Enhancements

There are several enhancements in Release 12.2(33)SXH to SPAN features to make it easier for network operators to monitor and troubleshoot their network environments.

Increase of Egress SPAN ports. The Catalyst 6500 now can deliver 14 Tx-only SPAN ports plus 2 Tx/Rx/Both ports, for a total of 16 SPAN ports. Customers can now monitor their traffic with TX, looking at traffic leaving the port, or RX, looking at traffic entering the port, or both.

RP/SP CPU Inband SPAN feature adds the ability to capture CPU-bound and CPU-generated traffic. This feature gives customers the ability to monitor traffic destined to either the RP or the SP CPU and monitor it to a SPAN destination port. By monitoring traffic coming to and going out of the CPU, customers can now have a very clear picture of what type of traffic and how much is going to the RP CPU to determine what causes the CPU to go high. Control Plane Policing policy then can be applied to alleviate the high CPU usage problem.

Distributed Egress SPAN helps scale the SPAN feature by performing Tx SPAN replication locally on the line card instead of relying on the Supervisor for SPAN replication. Today with the bandwidth of the interfaces, as well as the density of ports on the line cards increasing, distributed Egress SPAN will help with scalable SPAN designs using both RX and Tx SPAN.

Benefits

These SPAN enhancements provide a more scalable suite of tools that allow customers to more effectively manage Catalyst 6500 Series Switches in their networks.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Sai Pakkam, spakkam@cisco.com

Cisco IOS Software Modularity Support for SIP-200, SIP-400, and Enhanced FlexWAN

The Catalyst 6500 is a high-speed modular switch and router ideal for convergence of Data Center, Campus and WAN in a single system. It offers a rich Enterprise WAN feature set such as MPLS, HA, QoS, and a wide range of WAN interfaces.

Starting with Release 12.2(33)SXH, Enhanced FlexWAN, SIP-200, and SIP-400 will be supported in IOS with Software Modularity, bringing all of the IOS modularity benefits to Enterprise WAN deployments. Those benefits include memory protection, fault containment, stateful process restart, and subsystem ISSU, all important features to ensure maximum high availability necessary for WAN deployments. Customers can deploy SIP/SPA and Enhanced FlexWAN today in Release 12.2(33)SXF, but will not get the same advantages that IOS Modularity offers.

Figure 5. SIP-200, SIP-400, and Enhanced FlexWAN SPAs

Table 6. Comparison between Enhanced FlexWAN, SIP-200, and SIP-400

Feature	Enhanced FlexWAN	SIP-200	SIP-400
Aggregate Performance	~ 625 Kpps	~1.1Mpps	~ 6 Mpps
Switch Fabric Enabled	Yes	Yes	Yes
Memory per bay, Default/Max	256MB/512MB	512Mb/1Gb	1Gb
PAs/SPAs	Majority of Port Adapters	Low-Speed SPAs	High-Speed SPAs
Congestion Avoidance, Tail Drop	Yes	Yes	Yes
Congestion Avoidance, WRED	IPPRec/DSCP/EXP	IPPRec/DSCP/EXP	Yes
Maximum # Policers	8,000	16,000	1023
Ingress Shaping	Yes	Yes	No
Egress Shaping	Yes	Yes	Yes

The SPA WAN adapter is shared across high end Cisco routers from the Catalyst 6500 to the flagship CRS-1. Customers can purchase SPAs with the knowledge that these SPAs can be used in Cisco 7300, Cisco 10000, Cisco 7600, Cisco 12000, CRS-1, in addition to the Catalyst 6500.

Table 7. SPAs Supported in Release 12.2(33)SXH

Product ID	12.2(18)SXF SIP-200 Support	12.2(18)SXF SIP-400 Support	12.2(18)SXH SIP-200 Support	12.2(18)SXHSIP-400 Support
SPA-8XCHT1/E1	12.2(18)SXE	No	12.2(33)SXH	No
SPA-2XT3/E3	12.2(18)SXE	No	12.2(33)SXH	No
SPA-4XT3/E3	12.2(18)SXE	No	12.2(33)SXH	No
SPA-2XCT3/DS0	12.2(18)SXE	No	12.2(33)SXH	No
SPA-4XCT3/DS0	12.2(18)SXE	No	12.2(33)SXH	No
SPA-1xCHSTM1/OC3	No	No	12.2(33)SXH	No
SPA-2XOC3-POS	12.2(18)SXE	12.2(18)SXE	12.2(33)SXH	12.2(33)SXH
SPA-4XOC3-POS	12.2(18)SXE	12.2(18)SXE	12.2(33)SXH	12.2(33)SXH
SPA-1XOC12-POS	No	12.2(18)SXE	No	12.2(33)SXH
SPA-1XOC48POS/RPR	No	No	No	12.2(33)SXH
SPA-2X1GE (Gila ASIC)	No	12.2(18)SXF	No	12.2(33)SXH
SPA-4X1FE-TX-V2 (Fugu ASIC)	No	No	12.2(33)SXH	No
SPA-8X1FE-TX-V2 (Fugu ASIC)	No	No	12.2(33)SXH	No
SPA-2XOC3-ATM	12.2(18)SXE	12.2(18)SXE	No	No
SPA-4XOC3-ATM	12.2(18)SXE	12.2(18)SXE	No	No
SPA-1XOC12-ATM	No	12.2(18)SXE	No	No
SPA-1XOC48-ATM	No	12.2(18)SXE	No	No

To maximize investment protection on Cisco products, the Catalyst 6500 offers the Enhanced FlexWAN solution so customers can re-use Port Adapters purchased for Cisco 7500 or 7200 on the Catalyst 6500.

Table 8. Port Adapters Support in Release 12.2(33)SXH

T1/E1	T3/E3 and STM-1	ATM	POS and High-Speed Serial Interface (HSSI)
• PA-4T+ • PA-8T-V35 • PA-8T-232 • PA-8T-X21 • PA-MC-2T1 • PA-MC-4T1 • PA-MC-8T1 • PA-MC-8TE1+ • PA-MC-8E1/120 • PA-MC-2E1/120 • PA-4E1G/120 • PA-4E1G/75	• PA-T3 • PA-T3+ • PA-E3 • PA-2T3 • PA-2T3+ • PA-2E3 • PA-MC-T3 • PA-MC-2T3+ • PA-MC-E3 • PA-MC-STM-1MM • PA-MC-STM-1SMI	• PA-A3-T3 • PA-A3-E3 • PA-A3-OC3MM • PA-A3-OC3SMI • PA-A3-OC3SML • PA-A3-8T1IMA • PA-A3-8E1IMA • PA-A6-OC3MM • PA-A6-OC3SMI • PA-A6-OC3SML • PA-A6-T3 • PA-A6-E3	• PA-POS-OC3MM • PA-POS-OC3SMI • PA-POS-OC3SML • PA-POS-2OC3MM • PA-POS-2OC3SMI • PA-POS-2OC3SML • HSSI • PA-H • PA-2H

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chris Le, cle@cisco.com

Standby Fabric Hot Sync

The Standby Fabric Hot Sync feature lowers the Supervisor 720 switch over time from about 1.5 seconds to about 50 milliseconds (ms). This is achieved by allowing the channels to maintain sync to both active and stand-by switch fabrics. DFC equipped cards achieve the 50 ms switchover whereas the CFC equipped cards achieve 300 ms switchover with Cisco IOS Software Release 12.2(33)SXH. The hot-sync feature is supported on all Catalyst 6500 E-Series chassis (it is not supported by Catalyst 6500 non-E-Series chassis).

Figure 6. Standby Fabric Hot Sync Mode

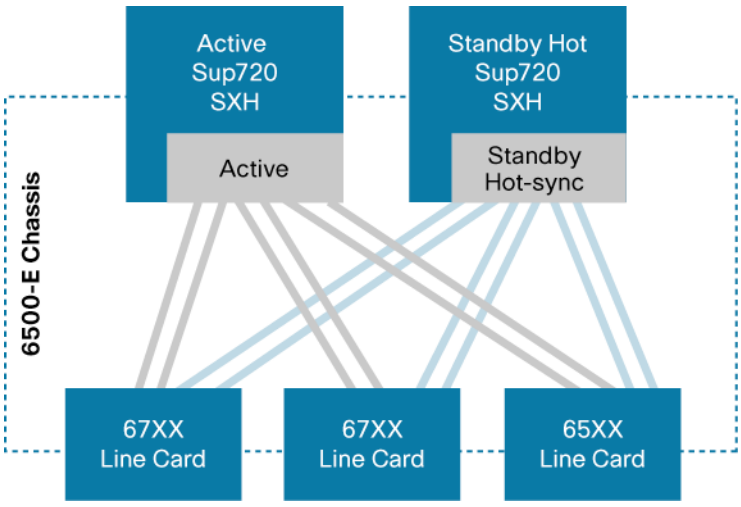


Figure 6 above illustrates that the line card maintains the channel in sync with both active and standby fabrics at the same time. Upon switchover, the active fabric goes down and the link to the standby fabric can be used to switch traffic without any re-sync involved.

Benefits

Reduces the Supervisor switchover time from 1.5 seconds to less than 50ms.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Pallavi Srinivasa, palsrini@cisco.com

Cisco IOS Software Modularity Support for the Catalyst 6500 ME 6524 Ethernet Switch

The ME 6524 switch will now be offering Cisco IOS Software Modularity as a feature set with Cisco IOS Native. This will be similar to the offering on the other Supervisor Engine family. The majority of the features listed in this product bulletin refers to ME 6524 systems as well.

Please visit the ME 6524 Release Notes for details on features supported on the ME 6524:

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

Hardware

Switches	Catalyst 6500 Series ME 6524 Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

Inline 802.3af Power Classification Override

When an IEEE 802.3af Power over Ethernet (PoE) device is connected to a linecard with the Luhai-A (WS-F6K-48-AF) daughter card on the Catalyst 6500, a fast link pulse is used to detect the type of PoE device and its IEEE class. For Cisco PoE devices, Cisco Discovery Protocol (CDP) is then used to allocate the appropriate amount of power to the port on which the device is connected. For PoE devices which do not have CDP capability, maximum power (15.4W at the switch level) is allocated to the port by default.

Since the actual power drawn by the device could be lower than the power allocated to the port from the power budget, Release 12.2(33)SXH introduces the following CLI commands to override the default inline power allocation and hard code it to a lower number:

"power inline allocation initial <milli-watts>"— overrides the default power allocation

"power inline allocation initial default"—restores the default power allocation

Note: These commands have been supported in CatOS since CatOS Release 8.5(1).

Benefits

Allows optimization of power allocated to PoE devices with no CDP capability

Hardware

Power over Ethernet (PoE) daughter card WS-F6K-48-AF, Cisco Catalyst 6500 Series Switch

Additional Information

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd80233a77.shtml

Product Management Contact: Mala Srivastava, malasri@cisco.com

IP Routing

OSPF Graceful Restart Functionality (RFC 3623)

OSPF graceful restart functionality, as described in RFC 3623, supports nonstop forwarding enhancements to the OSPF routing protocol when a peer OSPF router restarts. An OSPF nonstop forwarding (NSF) capable router that is reloading and attempting a graceful restart originates grace link state advertisements (grace-lsas) to notify its neighbors that it will perform graceful restart within the specified amount of time. During this grace period, the neighboring OSPF routers, called helper routers, continue to announce the restarting router in their LSAs as if it were fully adjacent, as long as the network topology remains static.

Once the router comes up, it will synchronize with the neighbor router (helper router). Once it is synchronized, the router withdraws the grace-lsas from the neighbor. If network topology changes while a router is being restarted, then the entire synchronization is required between the restarted router and its neighbors.

This process ensures that the network does not notice any changes when a router is being restarted. During this period, the traffic is being forwarded appropriately throughout the network.

Benefits

Non stop forwarding during a router restart: by limiting the knowledge of a router restart to only immediate neighbors in a network, the entire network continues to be fully functional and forwards the traffic appropriately.

Improved network reliability: When a router restarts, it quickly converges with only its neighbors without disrupting the network. This quick convergence allows minimal to no impact on services.

Hardware

Routers	Cisco 7200, 7300, 7500, and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Reliable Static Routing Backup Using Object Tracking

The Reliable Static Routing Backup Using Object Tracking feature introduces the ability for Cisco IOS Software to use Internet Control Message Protocol (ICMP) pings to identify when a Point-to-Point over Ethernet (PPPoE) or IP Security Protocol (IPsec) Virtual Private Network (VPN) tunnel goes down, allowing the initiation of a backup connection from any alternative port. The Reliable Static Routing Backup Using Object Tracking feature is compatible with both preconfigured static routes and Dynamic Host Configuration Protocol (DHCP) configurations.

Benefits

PPPoE and IPsec VPN deployments provide cost-effective and secure Internet-based solutions that can replace traditional dialup and Frame Relay circuits.

- **Simplicity:** The Reliable Static Routing Backup Using Object Tracking feature can determine the state of the primary connection without enabling a dynamic routing protocol.
- **Reliability:** The Reliable Static Routing Backup Using Object Tracking feature introduces a reliable backup solution for PPPoE and IPsec VPN deployments, allowing these solutions to be used for critical circuits that must not go down without a backup circuit automatically engaging.

Hardware

Routers	Cisco 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

OSPF Area Transit Capability

OSPF area transit capability (RFC 2328) provides the ability for an OSPF area to carry data traffic that neither originates nor terminates in the OSPF area itself.

Benefits

Enables an OSPF Area Border Router (ABR) to discover shorter paths through the transit area and forward traffic along those paths rather than using the virtual link or path, which are not as optimal.

Considerations

This feature supports RFC 2328 OSPF Version 2 only.

Hardware

Routers	Cisco 7200, 7301, 7500, and 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional information

- http://www.cisco.com/go/routing
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/index.htm

Product Management Contact: Suresh Katukam, skatukam@cisco.com

EIGRP Route Map Support

The Enhanced Interior Gateway Routing Protocol (EIGRP) Route Map Support feature enables EIGRP to interoperate with other protocols by filtering inbound and outbound traffic based on complex route map options. EIGRP can process a permitted set and match parameters supplied by a route-map facility and extend filtering on an added EIGRP-specific set and match choices.

Benefits

- **Flexibility:** Allows complex inbound and outbound filtering with other routing protocols.
- **Robustness:** Enables the ability to match clauses based on entire source routing protocol or external routing protocol metrics or range of metrics.

Hardware

Routers	Cisco 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

BGP Multicast Inter-Autonomous System (IAS) VPN Support

The BGP Multicast Inter-AS (IAS) VPN feature introduces the IPv4 Multicast Distribution Tree (MDT) Sub-Address Family Identifier (SAFI) in Border Gateway Protocol (BGP). The MDT SAFI is a transitive multicast capable connector attribute that is defined as an IPv4 address family in BGP. The MDT SAFI is designed to support inter-autonomous system (inter-AS) Virtual Private Network (VPN) peering sessions.

Benefits

Enables multicast sessions across inter-AS VPNs: By allowing multicast distribution tree information exchange across inter-AS VPNs, one multicast receiver from one AS VPN can join another AS VPN.

Hardware

Routers	Cisco 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Border Gateway Protocol (BGP) Support for Dual Autonomous System Configuration for Network Autonomous System Migrations

When a Service Provider merges its Autonomous System (AS) with another (for example, via business acquisition), this features provides for a seamless way to transition the customers over to the new AS. This transition involves two integrated feature components:

- Maintaining the TCP session with the customer's router independent of AS.
- Modifying the inbound and outbound as-path lists so that this transition to a new AS is as transparent to the customer as possible.

Benefits

Enables the network to provide an easier transition for customers from one of their AS numbers to another during the transition phase. Customers can change the Service Provider AS number in their configurations at their convenience.

Hardware

Routers	Cisco 1700, 2600, 3600, 3700, 7200, 7300, 7400, and 7500 Series; 7600-MWAM
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Border Gateway Protocol Support for IP Prefix Import from Global Table into Virtual Routing and Forwarding Table

This feature allows customers to specify which specific prefixes from the global routing table are to be imported into a VPN routing and forwarding table (VRF).

Hardware

Routers	Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200, and 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Border Gateway Protocol Support for Named Extended Community Lists

Border Gateway Protocol (BGP) uses extended community lists to apply policies to groups of prefixes to distinguish routing paths. This enhancement introduces support for named extended community lists. Previously, extended community lists could only be numbered and were limited to a few hundred entries.

Benefits

- Improves customer's ability to manage and troubleshoot BGP policies by using name strings for extended community lists instead of numerical values.
- No inherent limit on the number of named extended community lists, provided that they are uniquely named.

Hardware

Routers	Cisco 1700, 2600, 3700, 7200, 7400, 7500, and 7600 Series; 7600-MWAM
Switches	Cisco Catalyst 6500 Series Switches

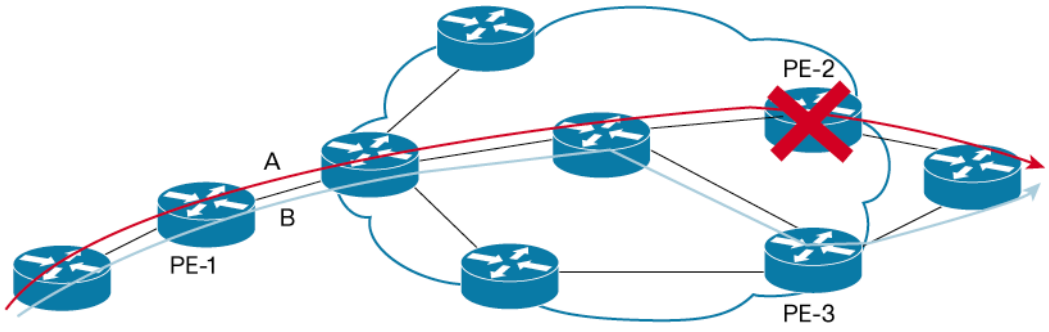
Product Management Contact: Suresh Katukam, skatukam@cisco.com

Border Gateway Protocol Support for Next-Hop Address Tracking

Border Gateway Protocol (BGP) Next-Hop Address Tracking allows BGP to converge quickly when a path to next-hop address changes. BGP speaker A learns routes from another BGP speaker B while the next-hop address for routes may be different from BGP speaker B. By tracking the next-hop address, BGP speaker A converges all routes associated with the next-hop addressed by speaker B very quickly.

An address-tracking filter mechanism is used to filter notifications to the routing information base. This mechanism allows for new path selection to begin as soon as the notification regarding the change in reachability state of the next hop occurs. This results in much faster convergence of traffic to a new path and less impact to traffic flows. All of these facts mean faster convergence, leading to improved reliability of the network for users.

Figure 7. Next-Hop Tracking Speeds Convergence



As illustrated in Figure 7 above, BGP Next-Hop Tracking will trigger the BGP scanner at PE-1 to run immediately on Interior Gateway Protocol (IGP) convergence, so the route through PE-3 will handle traffic upon failure to PE-2.

Benefits

- **Minimal impact to data forwarding:** By converging all routes associated with a next-hop, the BGP router forwards the data along the right path to the final destination.
- **Improved network reliability:** By quickly converging and keeping the latest routes, the impact on services is minimal.

Hardware

Routers	Cisco 7200, 7300, 7500, 7600, and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

BGP Support for TCP Path MTU Discovery per Session

BGP support for TCP path MTU discovery per session between two BGP speakers allows a BGP speaker to discover the maximum update size that the speaker should use to communicate with the other speaker. This will avoid fragmentation by any node in the network, and reassembly of fragments by a BGP speaker. The fragmentation and reassembly leads to delay in processing a message. By avoiding fragmentation and reassembly, BGP can avoid the delay in processing of messages and process updates quickly. This will lead to faster convergence of routes and improved performance of the network.

Benefits

- **Minimal impact to data forwarding:** By using appropriate packet sizes for updates, BGP speakers can converge routes quickly and forward the data along the right path to the final destination.
- **Improved router performance:** By avoiding reassembly of packets of a single update, a BGP speaker can avoid unnecessary CPU utilization.

Hardware

Routers	Cisco 7200, 7300, 7500, and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Supress BGP Advertisement for Inactive Routes

The Suppress BGP Advertisement for Inactive Routes feature allows BGP updates to be more consistent with routes used for data forwarding. When BGP learns a new route and selects the route as the best, it tries to insert it into the local routing table. The route may not be inserted into the routing table for many reasons ie: routing table may have a size limit imposed by an administrator or if the routing table already has a better router via static, then it does not install this route. With this feature, BGP does not advertise this route unless the nexthop is the same. This feature ensures that a BGP speaker does not advertise routes to other peers unless the BGP speaker uses the route in its data forwarding.

Benefits

- **Consistent Routing and Forwarding:** By suppressing inactive routes, BGP speakers advertise routes that are used for forwarding purposes which ensures routing and forwarding are consistent with each other.
- **Easier to Debug Network Issues:** This feature does not advertise any inactive routes, users can use BGP routes and corresponding routing tables for debugging purposes and be certain that the forwarding table reflects the routing table.

Hardware

Routers	Cisco 7200,7300, and 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Per-VRF Assignment of BGP Router-ID

Per-VRF BGP Router-ID enables a BGP speaker in one VRF to establish connection to itself via another VRF. This allows the exchange of routes between VRF-BGP speakers while they are able to use all the features and flexibility of the BGP.

Benefits

Flexible Redistribution of Routes Between VRFs: Using this feature, BGP can establish connection to itself via two VRFs and redistribute routes between these two VRFs. Users can configure all features available to control distribution of routes from one VRF to other VRF.

Hardware

Routers	Cisco 7200, 7300, 7500, and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

BGP Dynamic Neighbors

The BGP Dynamic Neighbors feature simplifies the configuration to allow connections from a large number of neighbors. Currently, BGP speaker A accepts a connection from another BGP speaker B only if the user configures neighbor information about speaker B. If there are a large number of neighbors, this approach requires the user to configure information about every neighbor. This feature allows users to configure a range of IP addresses and AS numbers that a BGP speaker should accept connections from. A BGP speaker accepts a connection request from a neighbor only if the neighbor's IP address and AS number belongs to the configured IP address range and AS numbers.

Benefits

- **Ease of Use and Simplified Configuration:** By allowing an IP address range and AS numbers, the user does not have to configure each neighbors information at a speaker. It simplifies configuration to allow BGP sessions among a large number of BGP speakers.
- **Improved Security and Flexible Configuration:** This features provides flexibility in configuring multiple IP address ranges and assigning different sets of properties for each range. In addition, it provides better security by accepting connections from only configured IP address ranges instead of accepting connections from everyone.
- **Improved Router Performance:** BGP relies on TCP to listen and accept connections from neighbors. By listening to an IP address range instead of each individual IP address, BGP avoids unnecessary CPU utilization.

Hardware

Routers	Cisco 7200, 7300, 7500, and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Product Management Contact: Suresh Katukam, skatukam@cisco.com

Cisco Optimized Edge Routing

Cisco Optimized Edge Routing (OER) automates routing in order to optimize network performance. In addition, Cisco OER allows customers to minimize both bandwidth costs and operational expenses. Cisco OER can select the best path based upon cost minimization, load distribution policy, and overall network performance.

Cisco OER enables intelligent network traffic load distribution and dynamic failure detection of data-paths at the WAN edge (ie: multi-homing to the Internet or for intranet connectivity). While traditional routing mechanisms can provide both load-sharing and failure mitigation, Cisco OER is unique in that it can make adaptive and dynamic routing adjustments based on criteria other than static routing metrics: response time, packet loss, jitter, MOS, path availability, traffic load distribution, and financial cost minimization policies.

Cisco OER is implemented in Cisco IOS Software as an integrated part of Cisco core routing functionality. It can be deployed with familiar simplicity via standard CLI configuration. Cisco OER offers increased Cisco product value and differentiation by leveraging various Cisco IOS Software features (such as Cisco IOS NetFlow and Cisco IOS IP SLAs) and cross product integration to support multiple hardware products and routing protocols.

Figure 8. Cisco OER Deployment Example

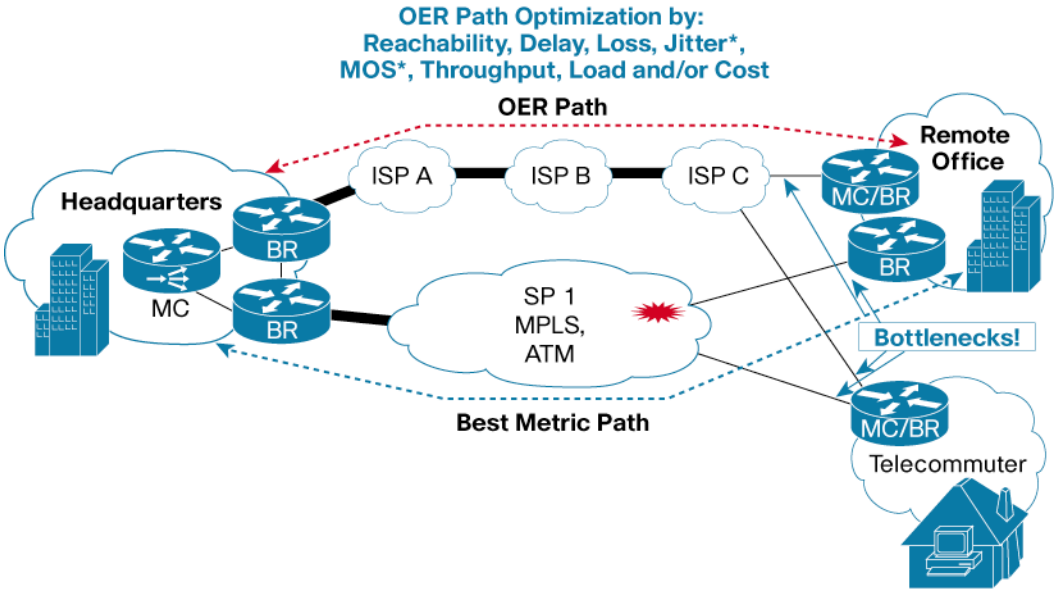


Table 9. Cisco OER Benefits

Features	Benefits
Automatic Performance, Cost Minimization, and Policy-Based Load Distribution	Instant routing adjustments based on performance, path availability, load share, Jitter, MOS or monetary cost measurements and business objectives.
Multiple Router Support	Delivers advanced networking capabilities and investment protection on many Cisco IOS Software based hardware products.
Multiple Routing Protocol Support	Delivers advanced networking capabilities and investment protection by integrating with IP core routing (ie: BGP, static routes, PBR) and network characterization features.
Internet and WAN Edge Traffic Optimization	Improve Internet and WAN edge traffic performance for content/application providers' customers.

Features	Benefits
Passive and Active Measurements	• Delivers advanced networking capabilities and investment protection by integrating with existing Cisco IOS Software features, such as Cisco IOS NetFlow and Cisco IOS IPSLA. • NetFlow passive measurements minimize active probing.
Control and Observation Modes for Different Prefixes	Allows non-disruptive observation of the behavior of OER before controlling prefixes.
Support Multiple Link Billing Models	Provides flexibility for bandwidth cost minimization and ISP selection.
CLI Configuration and Reporting on Cisco IOS Software Based Hardware Products	Provides consistent Cisco IOS CLI which leverages the existing CLI knowledge of IT staff.

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Scott Van De Houten, svandeho@cisco.com

Cisco IOS Software Modularity Support for IPv6 Routing Protocols (RIPng, OSPFv3)

Prior to Release 12.2(33)SXH, all IPv6 features were part of the ios-base within the software modular software image. Starting with Release 12.2(33)SXH, IPv6 RIPng and OSPFv3 have been moved into the “iprouting” process which allows these processes to be restarted to attain high availability.

The following IPv6 components will still continue to reside in the ios-base process:

- IPv6 neighbor discovery
- IPv6 Multicast

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder Sambi, msambi@cisco.com

IP Multicast

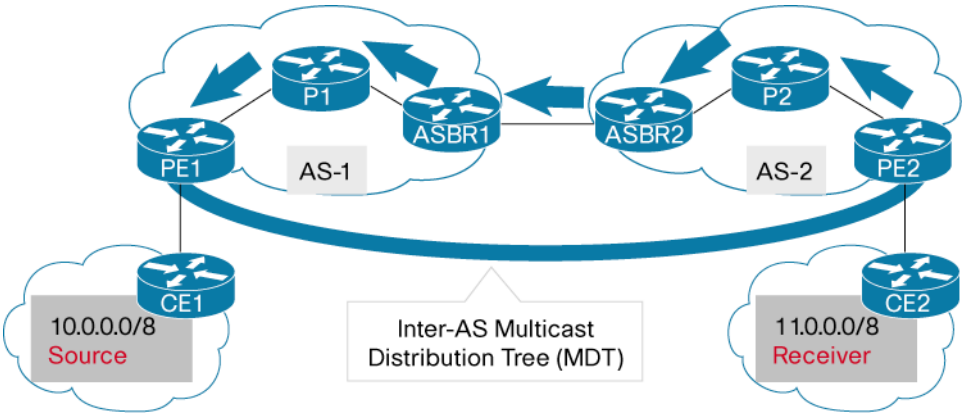
Multicast VPN (MVPN) Inter-AS Support

Multicast VPN (MVPN) technology is a method to dynamically provide multicast information across an MPLS enabled network. It is simple to set up, highly scalable, and has minimal administrative overhead. The MVPN architecture introduces an additional set of protocols and procedures that help enable services to support multicast traffic in a VPN. It allows for the transport of a customer’s IP Multicast traffic across a customer’s VPN backbone, and it is integrated transparently with the Cisco IOS Unicast MPLS VPN solution. It allows a service provider to offer multicast services to its VPN customers, in addition to its current Unicast VPN offering. The capability allows transparent connection of multiple multicast sites to be mapped and transported across common multicast tree’s built across the MPLS core network.

The Inter-Autonomous System (Inter-AS) feature allows two provider-edge routers to communicate with MVPN across autonomous systems. Support for the Multicast VPN feature can be configured on a VRF router, to enable forwarding of Multicast VPN traffic from one site of a VPN Red in Autonomous System 1 to another site of the VPN Red in Autonomous System 2. Using the Multicast Distribution Tree (MDT) autonomous system, provider-edge routers in different autonomous systems are able to learn about each others' existence and join each other. As defined in the IETF standards, all three options for Inter-AS MPLS VPN are supported with the Inter-AS MVPN. (See Figure 9 below).

The Reverse Path Forwarding (RPF) vector is needed for Inter-AS to function properly and allows devices in different AS's to be aware or find the origin of a route used for the RPF check. This is done by adding additional information in the PIM join packet, the intermediate routers are able to select a RPF interface by doing a direct lookup in a special BGP MDT table. The BGP MDT table is used only to set up the MDT tunnel. It is not used for the VPN traffic encapsulated in the MDT tunnel. For intermediate routers that do not run BGP, the RPF vector is used to find the RPF interface.

Figure 9. Diagram of MVPN Inter-AS: PIM Join sent from PE1 across AS's to PE1



Benefits

- Scalable and efficient method to transport and replicate customer multicast information across multiple BGP AS's in an Inter-AS Layer 3 MPLS VPN network
- Efficient support of all 3 inter-AS connection options:
  - Back to Back ASBR PE's
  - ASBR's exchanging VPNv4 routes
  - VPNv4 Routes via Multi-Hop MP-eBGP
- Integrated transparently with unicast MPLS VPN services

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd802aea84.shtml
- http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

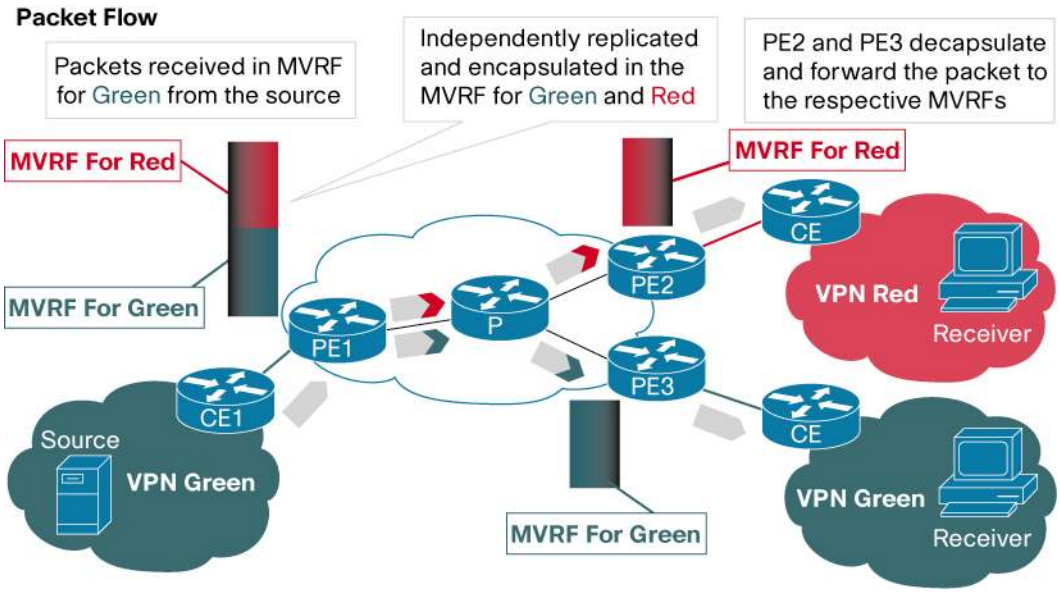
Multicast MVPN Extranet

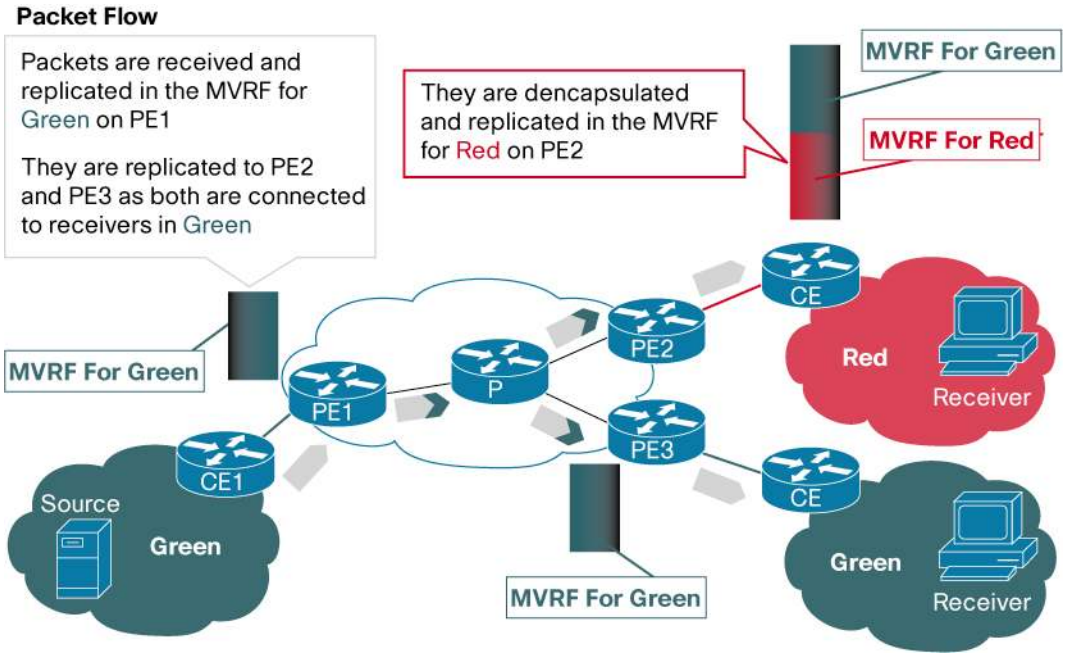
A new capability to allow extranet capabilities in MVPN is now available. Extranet allows VPN closed user groups to share information and common multicast information to be distributed across multiple VPN customers.

An extranet can be viewed as part of a company's intranet that is extended to users outside the company. An extranet is a VPN connecting the corporate site or sites to external business partners or suppliers, to securely share part of a business's information or operations among them. MPLS VPNs inherently provide security, ensuring that users access only appropriate information. The MPLS VPN Extranet service offers users unicast connectivity without comprising the integrity of their corporate data. Multicast VPN Extranet extends this service offering to include multicast connectivity to the extranet community of interest. It allows Service Providers to offer the next generation of flexible extranet services, helping to enable business partnerships between different Enterprises.

As shown in Figure 10 below, the Multicast VPN Extranet feature allows network providers to source multicast content from VPN Green into VPN Red.

Figure 10. Topology of Two Multicast VPN Extranet Use Case





Benefits

- Scalable and efficient method to transport and replicate customer multicast information across an MPLS network between different VPN's
- Extranet MVPN solves these business needs:
  - Efficient content distribution between Enterprises
  - Efficient sharing of multicast resources with external or business partners
  - Efficient content distribution from Service Providers or content provider to its different VPN customers
- Integrated transparently with unicast MPLS VPN services

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd802aea84.shtml
- http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

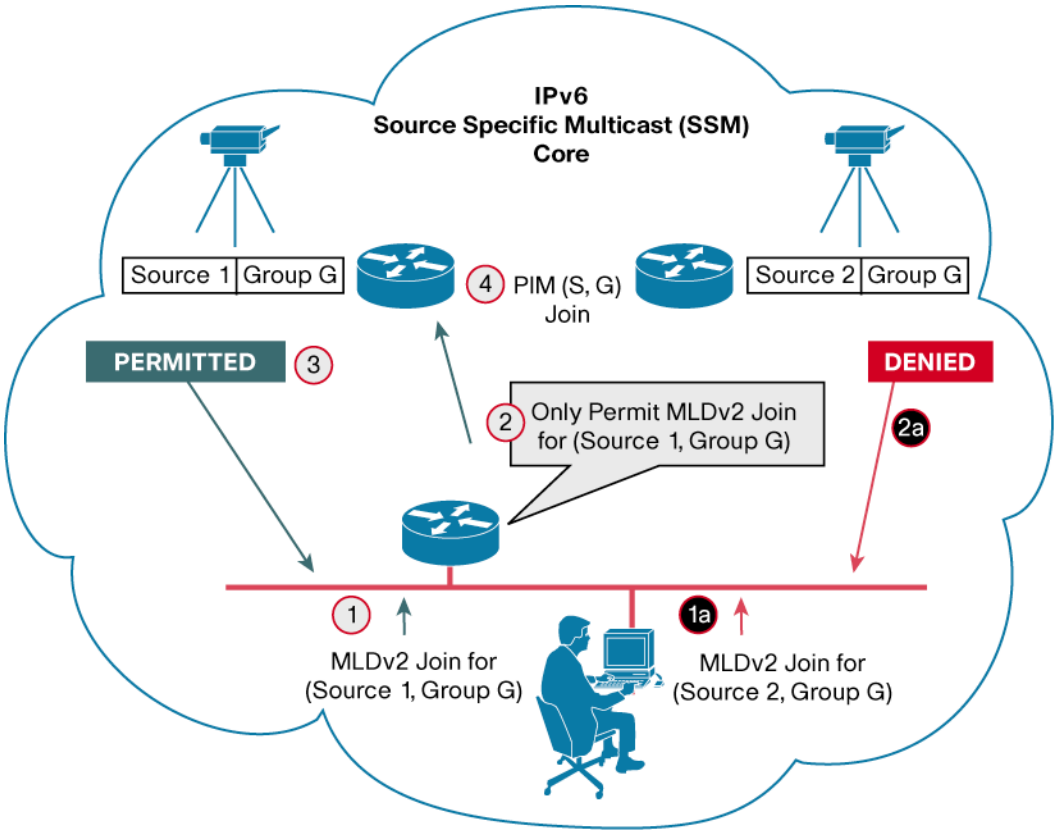
Multicast IPv6 Enhancements

Cisco is an established leader in multicast technology and supports multicast for IPv6, MPLS, IPv4 and VPN network environments. A series of features have recently been released to enhance IPv6 Multicast deployments.

Table 10. New Multicast IPv6 Features in Release 12.2(33)SXH

Feature Name	Functionality
Bootstrap Router (BSR)	Cisco has added Bootstrap Router (BSR) for Rendezvous Point (RP) information distribution. BSR is a standard method for RP information distribution in a multicast domain.
MLD Access Group	MLD access group allows Cisco edge routers to explicitly track Source and Group (S,G) joins and filters based on source or source and group pairs. Access lists are combined to permit and deny access to sources and groups in the network (see Figure 11 below).
Explicit Tracking of Receivers	The router can explicitly track the behavior of multicast hosts in the network and enable the fast leave when using MLDv2. If a group is no longer needed by the hosts it will be immediately removed from the MLD cache. This feature is applicable for fast channel change in an IPTV provided service.
PIM Accept Register	Filtering is now available at the RP for source register messages.
PIM Embedded RP	When enabled, the router will look for embedded RP group addresses in MLD reports/PIM messages and data packets. The router will learn the RP for the group from the address itself. It will then use this learned RP for all protocol activity for the group.
Routable Address Hello Option	This feature implements the hello option to advertise the routable addresses of an interface. These addresses are used by neighboring routers in RPF checks to map a routable address.
RPF Flooding of Bootstrap Router (BSR) Packets	This feature adds support for RPF flooding BSR packets. The router will do an RPF check for the BSR address and forward the packet only if it is received on the RPF interface.
Static Multicast Routing (mroute) for IPv6	Static routing is very useful in multicast environments to build multicast trees on specific interfaces not considered optimal by unicast routing. This feature brings support for IPv6 static multicast routing.

Figure 11. MLD Access Group Example



Benefits

- Enhanced features for IPv6 multicast deployments
- Comprehensive support for IPv6 multicast
- Committed support for IPv6 multicast standards

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

Auto Rendezvous Point (Auto-RP) Enhancements

Protocol Independent Multicast (PIM) sparse mode requires a Rendezvous Point (RP) to build multicast trees and forward traffic from multicast sources to receivers in the network. RP's are used by senders to a multicast group to announce their existence and by receivers of multicast packets to learn about new senders. There are various methods for distributing RP information in Cisco routers including static RP configuration, Auto-RP and Boot Strap Router (BSR). Many customers choose Cisco proprietary technology Auto-RP to distribute RP information. Auto-RP uses multicast groups to distribute RP information to devices in the network and the RP information is cached in the devices RP mapping cache. If the RP information is not available and the RP mapping cache is empty, then PIM Dense Mode will be enabled automatically to make sure the multicast information is flooded in the network. This behavior is called Dense Mode Fallback and is enabled by default. A new configuration command "no dense mode fallback" has been introduced to allow the router to continue operation in sparse mode.

Benefits

- Allow the user to enable or disable fallback to dense mode functionality
- Allow the user to block multicast traffic for groups not specifically configured. When a group is not specifically configured (that is, there is no RP for that group), multicast traffic does not flow across the network.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1e18.html

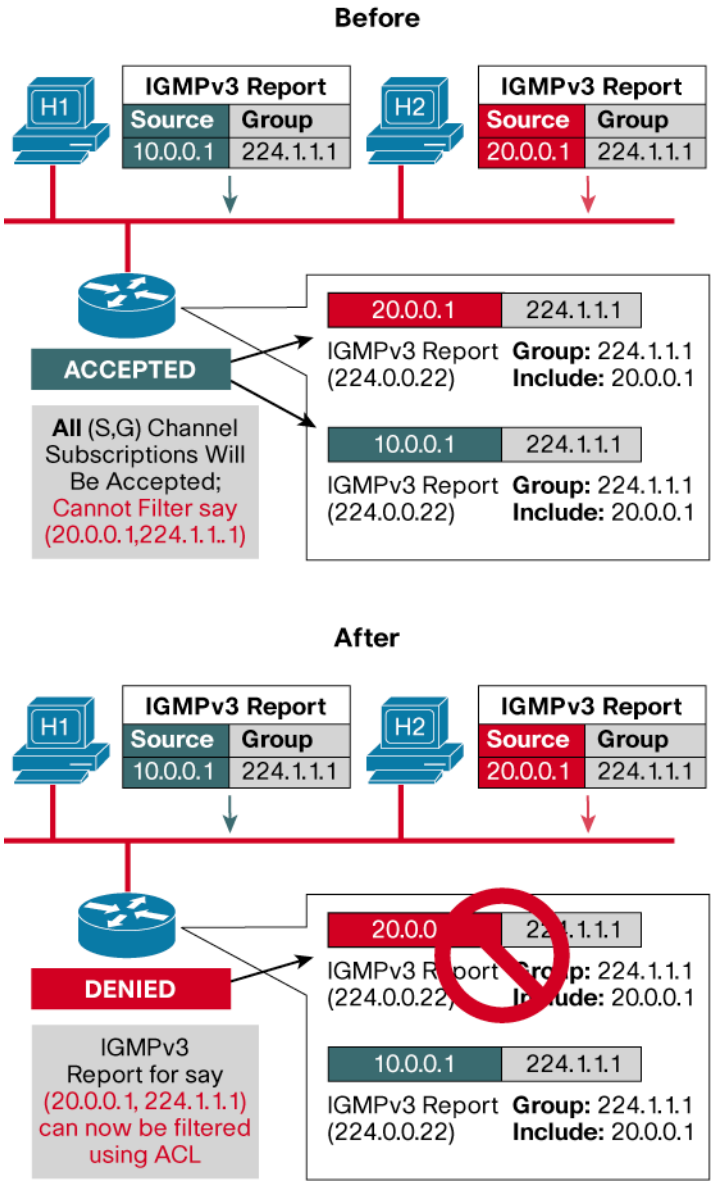
Product Management Contact: Scott Van de Houten, svandeho@cisco.com

IPv4 Extended ACL for IGMP to Support SSM

Source Specific Multicast (SSM) utilizes Source and Group (S,G) pairs to build multicast trees and forward traffic in the network. In general, SSM is used for one to many multicast applications and does not require Rendezvous Point (RP) in the network. SSM works with Internet Group Membership Protocol Version 3 (IGMPv3) reports that contain (S,G) information to build multicast trees to the source.

Cisco IOS Software now supports access lists that can specifically block an (S,G) pair being signaled by IGMPv3. This feature enables greater security for multicast SSM deployments. Prior to this feature, an IGMP access list accepted only a standard access list, allowing membership reports to be filtered based on a multicast group address. Using SSM with an IGMP extended Access Control List (ACL) allows you to permit or deny source S and group G (S,G) in IGMPv3 reports, thereby filtering SSM traffic based on source address and/or group address.

Figure 12. IPv4 Extended ACL for IGMP to Support SSM Topology Example



Benefits

- Added security for SSM deployments with IGMPv3
- Control of the multicast state in the network using enhanced IGMP filtering
- Utilize enhanced filtering to permit or deny specific source(s) or source and group pair(s)

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801fcdf6.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

IP Multicast Route Standard MIB (IPMROUTE-STD-MIB)

Cisco offers extensive support for multicast network management to understand how multicast is performing and operating in the network. Cisco also offers applications such as Cisco Multicast Manager (CMM) to read the Simple Network Management Protocol (SNMP) MIB data and present this to customers in tables and graphs.

Cisco historically supported a proprietary MIB to understand the multicast forwarding state in the network, the CISCO-IPMROUTE-MIB. Cisco has just introduced the IETF standard version of the IP MROUTE MIB for customers (IPMROUTE-STD-MIB). The new MIB allows users to understand the number of multicast routes available in the routing table, the byte count per multicast route or the byte count per interface per multicast route. This information is essential to understand how multicast is performing and operating in the network.

Benefits

- Enhanced network management to understand multicast performance and operation
- Specific support to understand the number of multicast routes and the amount of traffic forward per multicast route entry
- Committed support for IETF multicast standards

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/ps6337/index.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

Multicast Virtual Private Network (MVPN) MIB (CISCO-MVPN-MIB)

Cisco offers extensive support for multicast network management to understand how multicast is performing and operating in the network. Cisco also offers applications such as Cisco Multicast Manager (CMM) to read the SNMP MIB data and present this to customers in tables and graphs.

Multicast Virtual Private Network (MVPN) allows a Service Provider to support IP multicast traffic over a Multiprotocol Label Switching (MPLS) VPN network by using a unique multicast domain that has sources and receivers located in different sites. The Multicast VPN MIB (CISCO-MVPN-MIB_ introduces the capability for Simple Network Management Protocol (SNMP) monitoring of an MVPN. The MVPN MIB allows the user to understand the details of a multicast VPN deployment with external network management applications.

Table 11. Detailed Information About New Capabilities Introduced with the MVPN MIB

Capabilities
• Determine the number of multicast VRF's and the number of multicast enabled interfaces • Determine the multicast distribution tree groups joined and addresses allocated • Information on multicast distribution tree tunnels being utilized • Changes in creation and deletion of multicast VRF's on the PE device

Benefits

- Enhanced network management to understand multicast performance and operation of multicast VPN
- Extensive information to understand the usage of multicast groups and VRF's in the MPLS network

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/ps6337/index.html
- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805b5fca.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

Multicast Source Distribution Protocol (MSDP) Compliance with IETF RFC 3618

Multicast Source Distribution Protocol (MSDP) is used to signal multicast source information between multicast domains or between multicast RP's when using anycast RP for RP redundancy. MSDP allows multicast sources for a group to be known to all Rendezvous Points (RPs) in different domains. Each PIM-SM domain uses its own RPs and does not depend on RPs in other domains. An RP runs MSDP over the Transmission Control Protocol (TCP) to discover multicast sources in other domains.

The MSDP compliance with the IETF RFC 3618 feature enables you to configure compliance with the Internet Engineering Task Force (IETF) RFC 3618 specifications for MSDP. Compliance provides the following benefits:

- Border Gateway Protocol (BGP) route reflectors without running MSDP.
- Interior Gateway Protocol (IGP) for the Reverse Path Forwarding (RPF) checks and thereby run peering without BGP or Multiprotocol BGP (MBGP).
- Peering between routers in non-directly connected autonomous systems (that is, with one or more autonomous systems between them). This capability helps in confederation configurations and for redundancy.

Benefits

- IETF standard support for MSDP
- Committed support for IETF multicast standards

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

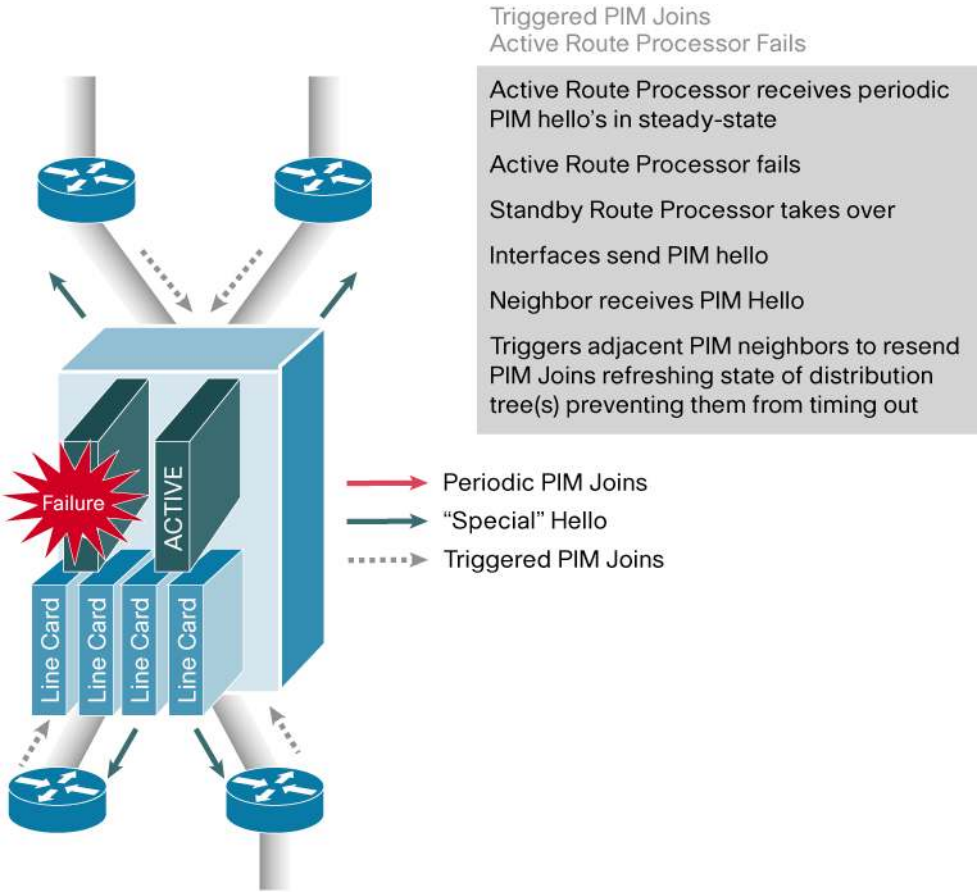
- http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00801d1d1c.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

Triggered Protocol Independent Multicast (PIM) Joins

Multicast high availability is a critical feature for customers requiring minimal network downtime for multicast traffic. Triggered PIM Joins is a new enhancement to the Cisco multicast high availability portfolio. Triggered PIM Joins protects the multicast state and prevents temporary black outs of multicast traffic upon supervisor failover. The use of a special PIM hello notifies PIM neighbors to trigger the refresh of multicast state in the router with supervisor failure. The triggered event of multicast routing and neighbor information minimizes outage time.

Figure 13. Triggered PIM Joins Functionality



Benefits

- Protection of multicast routing state using a new triggered mechanism
- Reduced downtime and the elimination of multicast traffic black holing during supervisor failure

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Product Management Contact: Scott Van de Houten, svandeho@cisco.com

Multicast Router Guard

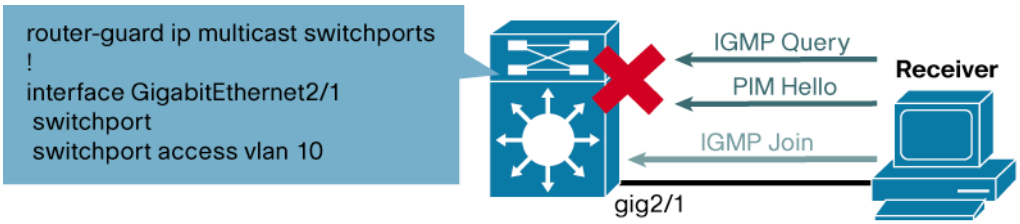
Prior to this feature, any Layer 2 port switchport on a Catalyst 6500 Series Switch could accept multicast control packets and allow PIM adjacency with a neighboring router.

With this feature in Release 12.2(33)SXH, customers can prevent unauthorized devices from becoming multicast routers, which can disrupt multicast traffic flow. This feature enables all Layer 2 ports within the switch to become “multicast” host ports which are capable of discarding multicast control packets such as IGMP query, PIM hello, IPv4 PIMv2, DVMRP, RGMP, and CGMP messages.

By discarding these packets, a particular interface cannot participate as a multicast router port and does not allow PIM adjacency to be established with neighboring routers. This feature can be enabled globally and can be disabled at any switchport interface level.

This feature is typically deployed on the Layer 2 ports of the access layer of a multi-tier network topology (see Figure 14).

Figure 14. Multicast Router Guard Topology



Hardware

Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder Singh Sambi, msambi@cisco.com

IGMP Filtering and Snooping Enhancements

In the current IGMP implementations, the customer does not have any concrete method of limiting IGMP joins in terms of version, limiting the number of IGMP groups, etc. With these new features in Release 12.2(33)SXH, the customer can now administratively filter and provide access control to the IGMP joins received on the switch interface.

The IGMP Filtering feature in Release 12.2(33)SXH allows the customer to administratively control multicast stream delivery within their networks. This feature works only in conjunction with the following IGMP snooping features to help control multicast traffic within the network:

- **IGMP snooping Access Control:** This feature enables customers to have more granular control of the multicast streams that can be allowed on a switch port or a VLAN by using either standard (group) or extended (source and group) access control lists. It also limits an interface to specific group membership or channel membership.
- **Number of IGMP Groups/Channels Limit:** The IGMP Snooping Group/Channel helps prevent oversubscription or bandwidth hogging by individual users and limits the number of IGMP groups or channels a single port can subscribe to.

- **IGMP Protocol Minimum-Version:** The IGMP snooping minimum protocol version helps prevent use of undesired IGMP versions in multicast network and enforces a minimum protocol version for IGMP hosts on VLAN. This can be applied to membership reports only and the configuration is allowed on the SVI only.

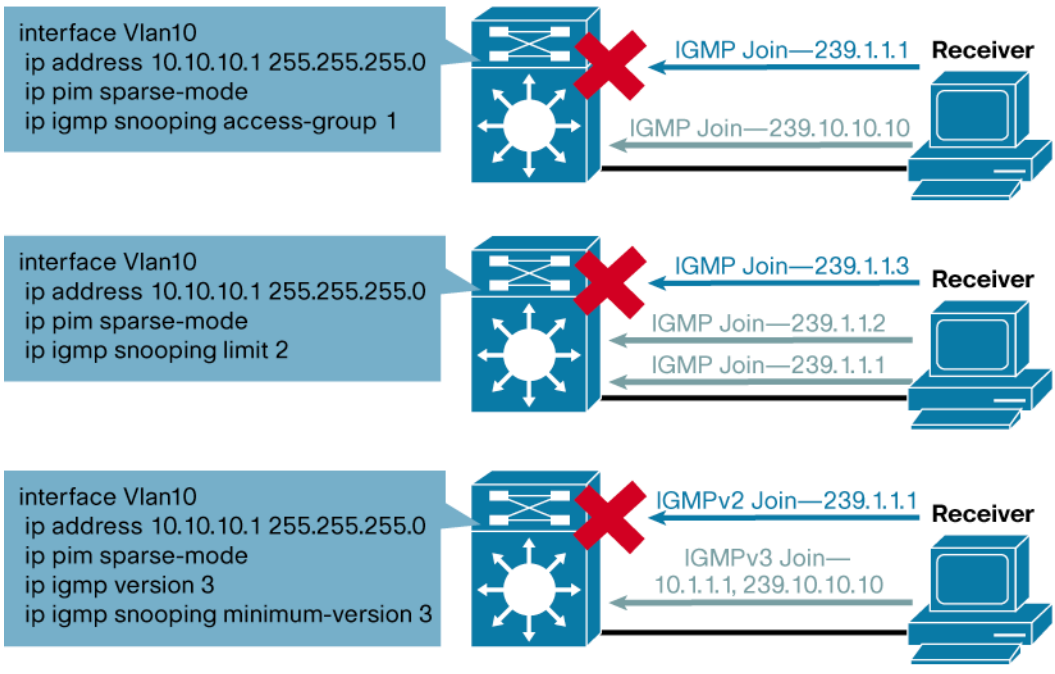
These features also provide additional security and control to routers by preventing undesired multicast streams from launching a denial of service attack. These features can be configured on either of the following interfaces.

- Per-SVI: Provides a default filter for all access switch ports in VLAN. For L2 only VLAN, SVI must exist but can be shut.
- Per-L2-switchport: Overrides any default SVI filter. On trunk, applies to all VLANs on trunk, overriding SVI filters
- Per-VLAN on L2 trunk port: Overrides any configured switch port filter for that VLAN

Deployment Scenarios

These features are applicable in multicast networks at the access layer switches in case of a Layer 3 access Layer. If the access-layer is layer 2, then only the per-L2-switchport and L2 trunk port configuration is applicable. In this case, these features need to be configured on the Distribution switches to allow control of the multicast streams (see Figure 15).

Figure 15. IGMP Filtering and Snooping Deployment Scenario



Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder Singh Sambi, msambi@cisco.com

MPLS and VPN, AtoM

Cisco IOS Software Modularity Support for MPLS Control Plane Components

Prior to Release 12.2(33)SXH, all MPLS features were part of the ios-based within the software modular software image. Starting with Release 12.2(33)SXH, the following software components for MPLS have been moved into the “iprouting” process which allow these processes to be restarted to attain high availability:

- L3 VPN control plane components (BGP MPLS/VRF related code)

The following MPLS components will still continue to reside in the ios-base process:

- MPLS Traffic Engineering (TE)
- MPLS Fast Reroute (FRR)
- Any Transport over MPLS (AToM)

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder Singh Sambi, msambi@cisco.com

MPLS Traffic Engineering (TE) Feature Enhancements

There are ten new MPLS Traffic Engineering (TE) features and enhancements in Cisco IOS Software Release 12.2(33)SXH:

1. **MPLS Traffic Engineering (TE): AutoTunnel Primary and Backup**

   The MPLS Traffic Engineering (TE): AutoTunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunnels. This support consists of the following features:

   - Backup AutoTunnel: Enables a router to dynamically build backup tunnels.
   - Primary One-Hop AutoTunnel: Enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

   If no backup tunnels exist, the following types of backup tunnels are created:

   - Next hop (NHOP)
   - Next-next hop (NNHOP)

   Benefits

   - Backup tunnels are built automatically, eliminating the need for users to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface.
   - The dynamic creation of one-hop primary tunnels eliminates the need to configure an MPLS TE tunnel with the Fast Reroute (FRR) option for the tunnel to be protected.
   - Protection is expanded; FRR does not protect IP traffic that is not using the TE tunnel or Label Distribution Protocol (LDP) labels that are not using the TE tunnel.

2. **MPLS Traffic Engineering (TE): Class-based Tunnel Selection**

   The MPLS Traffic Engineering (TE): Class-based Tunnel Selection feature enables you to dynamically route and forward traffic with different Class of Service (CoS) values onto different TE tunnels between the same tunnel headend and the same tailend. The TE tunnels can be regular TE or DiffServ-aware TE (DS-TE) tunnels.

   The set of TE (or DS-TE) tunnels from the same headend to the same tailend that you configure to carry different CoS values is referred to as a “tunnel bundle.” After configuration, CBTS dynamically routes and forwards each packet into the tunnel that:

   - Is configured to carry the CoS of the packet
   - Has the right headend for the destination of the packet

Benefits

- Because Class-Based Tunnel Selection (CBTS) offers dynamic routing over DS-TE tunnels and requires minimum configuration, it greatly eases deployment of DS-TE in large-scale networks.
- CBTS can distribute all CoS values on eight different tunnels
- CBTS also allows the TE tunnels of a tunnel bundle to exit headend routers through different interfaces.

3. **MPLS Traffic Engineering (TE): Inter-AS Feature**

   Inter-AS Traffic Engineering allows Service Providers to traffic engineer between networks and regions, this feature was previously not available. It involves the configuration of a single tunnel at the headend, as opposed to switching tunnels across each area that must be crossed, enabling Service Providers to deliver more robust, resilient and scalable networks.

   The MPLS TE Inter-AS feature in Cisco IOS Software Release 12.2(33)SXH provides Autonomous System Boundary Router (ASBR) node protection, loose path reoptimization, Stateful Switchover (SSO) recovery of Label-Switched Paths (LSPs) that include loose hops, ASBR forced link flooding, Cisco IOS Resource Reservation Protocol (RSVP) local policy extensions for Inter Autonomous System (Inter-AS), and per-neighbor keys.

Benefits

- **ASBR node protection:** Protects interarea and Inter-AS TE Label-Switched Paths (LSPs) from the failure of an Area Border Router (ABR) or ASBR.
- **Loose path reoptimization:** Allows a Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunnel’s LSPs to traverse hops that are not in the tunnel headend router’s topology database (that is, they are not in the same Open Shortest Path First (OSPF) area, Intermediate System-to-Intermediate System (IS-IS) level, or autonomous system as the tunnel’s head-end router).
- **Loose hop recovery:** Supports SSO recovery of LSPs that include loose hops.
- **ASBR forced link flooding:** Helps an LSP cross a boundary into another domain when information in the other domain is not available to the headend router.
- **Cisco IOS RSVP local policy extensions for Inter-AS:** Allows network administrators to create controlled policies for TE tunnels that function across multiple autonomous systems.
- **Per-neighbor keys:** Allows cryptographic authentication to be accomplished on a per-neighbor basis.

4. MPLS Traffic Engineering (TE): Fast Reroute (FRR) Link and Node Protection

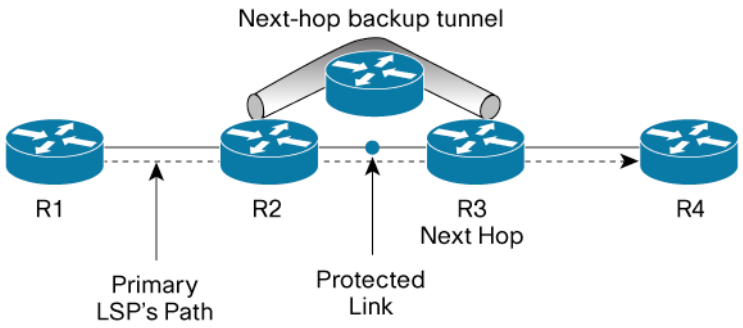
The MPLS Traffic Engineering (TE): Fast Reroute (FRR) Link and Node Protection feature provides link protection (backup tunnels that bypass only a single link of the Label-Switched Path (LSP), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following FRR capabilities:

- Backup tunnel support
- Backup bandwidth protection
- Resource Reservation Protocol (RSVP) Hellos

Fast Reroute (FRR) is a mechanism for protecting MPLS Traffic Engineering (TE) Label-Switched Paths (LSPs) from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

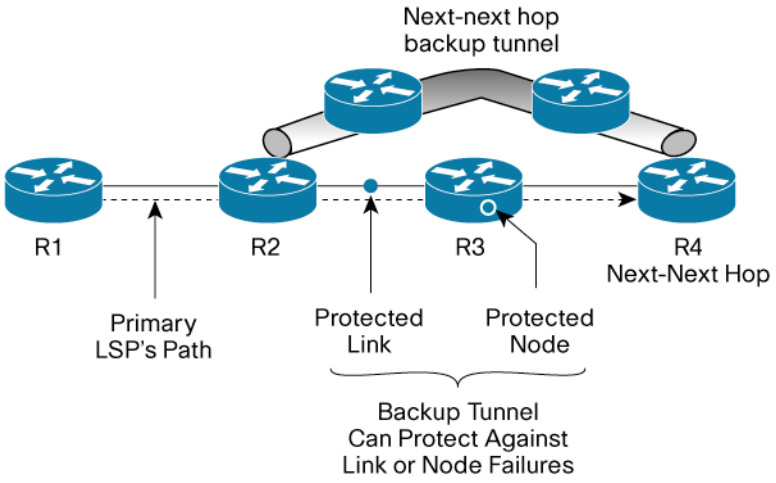
Backup tunnels that bypass only a single link of the LSP's path provide Link Protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as Next-Hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. Figure 16 illustrates a next-hop backup tunnel.

Figure 16. Next-Hop Backup Tunnel



FRR provides Node Protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called Next-Next-Hop (NNH) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. Next-Next Hop (NNHOP) backup tunnels also provide protection from link failures, because they bypass the failed link as well as the node. Figure 17 illustrates a next-next hop backup tunnel.

Figure 17. Next-Next Hop Backup Tunnel



If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes include the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.
- Primary LSP is modified so that Fast ReRoute is disabled. (The no mpls traffic-eng fast-reroute command is entered)

The Fast Reroute enhancements include the following:

- **Backup tunnel support:** Backup tunnels can terminate at the next-next hop to support FRR.
- **Multiple backup tunnels:** There no longer is a limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for Node Protection requires supporting multiple backup tunnels per protected interface. These backup tunnels can terminate at the same destination or at different destinations. That is, for a given protected interface, you can configure multiple NHOP or NNHOP backup tunnels. This allows for redundancy and load balancing.
- **Bandwidth protection on backup tunnels:** NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup-bandwidth. You can associate backup-bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup-bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup-bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected.
- **Bandwidth pool restrictions for backup tunnels:** You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using sub-pool bandwidth can use them or only LSPs that use global-pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could (optionally) not provide bandwidth protection.

- **Semi-dynamic backup tunnel paths:** The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature (this feature was introduced in Release 12.0(14)ST). Using this feature, semi-dynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semi-dynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.
- **RSVP Hello:** RSVP Hello enables RSVP nodes to detect when a neighboring node is not reachable. This feature is useful when next-hop node failure is not detectable by link layer mechanisms, or when notification of link-layer failures is not available (for example, Gigabit Ethernet).

Benefits

- **Node Protection:** Backup tunnels that terminate at the next-next hop protect both the downstream link and node. This provides protection for link and node failures.
- **Multiple Backup Tunnels Can Protect the Same Interface:** In addition to being required for Node Protection, this enhancement provides the following benefits:
  - **Redundancy:** If one backup tunnel is down, other backup tunnels protect LSPs.
  - **Increased backup capacity:** If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels).
- **Bandwidth Protection:** Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.
- **Scalability:** A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection. N:1 protection is not new with Node Protection; it existed with Link Protection.
  - **Example of 1:1 protection:** When 5,000 backup tunnels protect 5,000 LSPs, each router along the backup path must maintain state for an additional 5,000 tunnels.
  - **Example of N:1 protection:** When one backup tunnel protects 5,000 LSPs, each router along the backup path maintains one additional tunnel.
- **RSVP Hello:** RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, Hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

5. **Fast Reroute (FRR) Prefix Independence:** The MPLS Fast Reroute Prefix Independence feature is a mechanism which makes Fast Reroute failover time independent of the number of prefixes/routes, and Layer 2 VPN and VPLS Virtual Circuits with Fast Reroute protection.

6. **MPLS Traffic Engineering: Label Switched Path (LSP) Attributes:** The MPLS Traffic Engineering LSP Attributes feature is an extension to Multiprotocol Label switching (MPLS) Traffic Engineering (TE) that allows for a flexible configuration of attributes for path options associated with MPLS TE tunnels. LSP Attributes provide an LSP Attribute List feature and a Path Option for Bandwidth Override feature. Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a path option for bandwidth override.

Benefits

- LSP Attribute Lists provide an ability to configure values for several LSP-specific path options for TE tunnels.
- One or more TE tunnels can specify specific path options by referencing an LSP attribute list.
- LSP Attribute Lists make the MPLS TE user interface more flexible, easier to use, and easier to extend and maintain.
- Path Option for Bandwidth Override provides a single command that allows a TE tunnel to fall back temporarily to path options that can reduce bandwidth constraints.

7. **MPLS Traffic Engineering Verbatim Path Support:** This feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for Traffic Engineering (TE), thereby bypassing the topology database verification process.

   MPLS TE LSPs usually require that all the nodes in the network are TE aware, meaning they have IGP extensions to TE in place. However, some network administrators want the ability to build TE LSPs to traverse nodes that do not support IGP extensions to TE, but that do support RSVP extensions to TE.

   Verbatim LSPs are helpful when all or some of the intermediate nodes in a network do not support IGP extensions for TE.

   When this feature is enabled, the IP explicit path is not checked against the TE topology database. Since the TE topology database is not verified, a Path message with IP explicit path information is routed using the Shortest Path First (SPF) algorithm for IP routing.

8. **MPLS Traffic Engineering Autotunnel Mesh Groups:** MPLS Traffic Engineering AutoTunnel Mesh Groups (referred to as mesh groups) allow a network administrator to configure Traffic Engineering (TE) Label-Switched Paths (LSPs) by using a few Command-Line Interface (CLI) commands.

   In a network topology where edge TE Label Switch Routers (LSRs) are connected by core LSRs, the Mesh Group feature automatically constructs a mesh of TE LSPs among the Provider Edge (PE) routers.

   Initially, you must configure each existing TE LSR to be a member of the mesh by using a minimal set of configuration commands. When the network grows (that is, when one or more TE LSRs are added to the network as PE routers), you do not need to reconfigure the existing TE LSR members of that mesh.

   Mesh groups have the following benefits:

   - Minimize the initial configuration of the network. You configure one template interface per mesh, and it propagates to all mesh tunnel interfaces, as needed.

- Minimize future configurations resulting from network growth. The feature eliminates the need to reconfigure each existing TE LSR to establish a full mesh of TE LSPs whenever a new PE router is added to the network.
- Enable existing routers to set up TE LSPs to new PE routers.
- Enable the construction of a mesh of TE LSPs among the PE routers automatically.

9. **MPLS Traffic Engineering Shared Risk Link Groups (SRLG):** Shared Risk Link Groups (SRLGs) refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

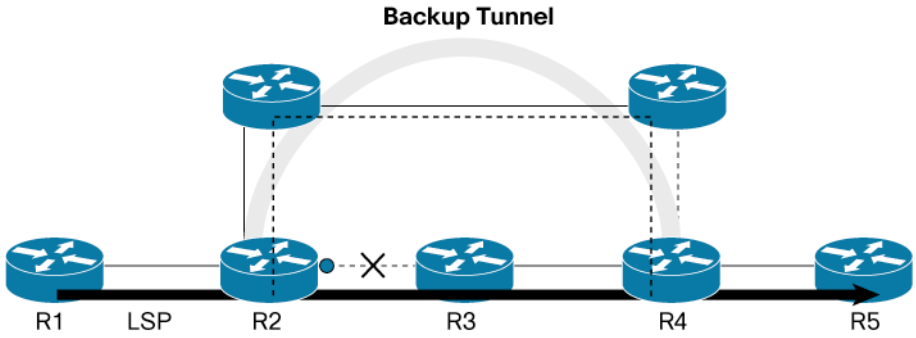
   The MPLS Traffic Engineering Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same SRLG as interfaces the backup tunnel is protecting.

Benefits

Backup tunnels should avoid using links in the same SRLG as interfaces they are protecting. Otherwise, when the protected link fails, the backup tunnel fails too.

Figure 18 shows a primary Label-Switched Path (LSP) from router R1 to router R5. The LSP protects against the failure of the R2-R3 link at R2 via a backup tunnel to R4. If the R2-R3 link fails, Link Protection reroutes the LSP along the backup tunnel. However, the R2-R3 link and one of the backup tunnel links are in the same SRLG. So if the R2-R3 link fails, the backup tunnel may fail too.

Figure 18. Backup Tunnel in the Same SRLG as the Interface it is Protecting



The MPLS TE SRLG feature enhances backup tunnel path selection so a backup tunnel can avoid using links that are in the same SRLG as the interfaces it is protecting.

There are two ways for a backup tunnel to avoid the SRLGs of its protected interface:

1. The router does not create the backup tunnel unless it avoids SRLGs of the protected interface.
2. The router tries to avoid SRLGs of the protected interface, but if that is not possible the router creates the backup tunnel anyway. In this case there are two explicit paths. The first explicit path tries to avoid the SRLGs of the protected interface. If that does not work, the backup tunnel uses the second path (which ignores SRLGs).

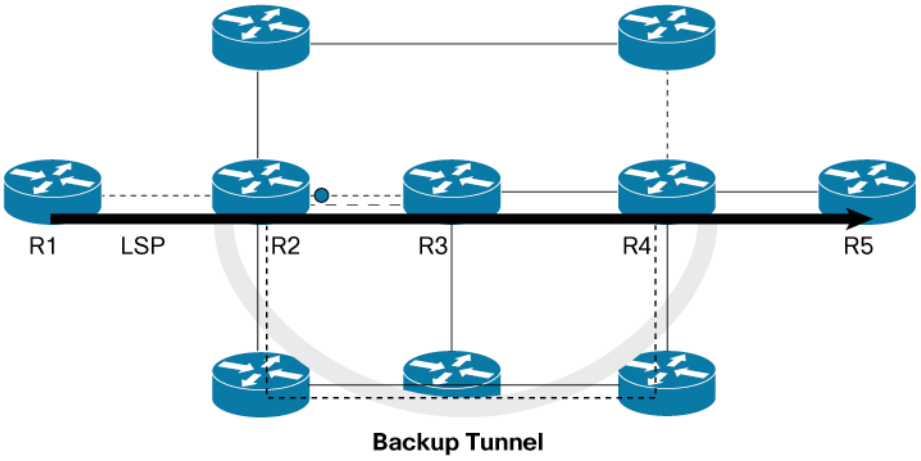
To activate the MPLS TE SRLG feature, you must do the following:

- Configure the SRLG membership of each link that has a shared risk with another link.

- Configure the routers to automatically create backup tunnels that avoid SRLGs of the protected interfaces.

OSPF and Intermediate System-to-Intermediate System (IS-IS) flood the SRLG membership information (including other TE link attributes such as bandwidth availability, affinity, and so forth) so that all routers in the network have the SRLG information for each link. With this topology information, routers can compute backup tunnel paths that exclude links having SRLGs in common with their protected interfaces. As shown in Figure 19, the backup tunnel avoids the link between R2 and R3, which shares an SRLG with the protected interface.

Figure 19. Backup Tunnel that Avoids SRLG of Protected Interface



10. **NSF/SSO: MPLS TE and RSVP Graceful Restart:** This feature allows a Route Processor (RP) to recover from disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

    Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO) provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

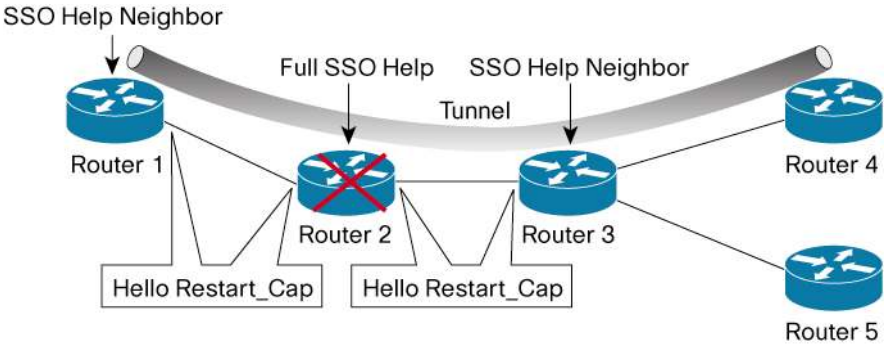
    RSVP graceful restart allows RSVP TE-enabled nodes to recover gracefully following a node failure in the network such that the RSVP state after the failure is restored as quickly as possible. The node failure may be completely transparent to other nodes in the network as far as the RSVP state is concerned.

    RSVP graceful restart preserves the label values and forwarding information and works with third-party or Cisco routers seamlessly.

    RSVP graceful restart depends on RSVP hello messages to detect that a neighbor went down. Hello messages include Hello Request or Hello Acknowledgment (ACK) objects between two neighbors.

    As shown in Figure 20, the RSVP graceful restart extension to these messages adds an object called Hello Restart_Cap, which tells neighbors that a node may be capable of recovering if a failure occurs.

Figure 20. How RSVP Graceful Restart Works



The Hello Restart_Cap object has two values: the restart time, which is the sender's time to restart the RSVP_TE component and exchange hello messages after a failure; and the recovery time, which is the desired time that the sender wants the receiver to synchronize the RSVP and MPLS databases.

As illustrated in Figure 20 above, RSVP graceful restart help neighbor support is enabled on Routers 1 and 3, so that they can help a neighbor recover after a failure, but they cannot perform self recovery. Router 2 has full SSO help support enabled, meaning it can perform self recovery after a failure or help its neighbor to recover. Router 2 has two RPs, one that is active and one that is standby (backup). A TE Label-Switched Path (LSP) is signaled from Router 1 to Router 4.

Router 2 performs checkpointing; that is, it copies state information from the active RP to the standby RP, thereby ensuring that the standby RP has the latest information. If an active RP fails, the standby RP can take over.

Routers 2 and 3 exchange periodic graceful restart hello messages every 10,000 milliseconds (ms) (10 seconds), and so do Routers 2 and 1 and Routers 3 and 4. Assume that Router 2 advertises its restart time = 60,000 ms (60 seconds) and its recovery time = 60,000 ms (60 seconds) as shown in the following example:

```
23:33:36: Outgoing Hello:
23:33:36: version:1 flags:0000 cksum:883C ttl:255 reserved:0 length:32
23:33:36: HELLO type HELLO REQUEST length 12:
23:33:36: Src_Instance: 0x6EDA8BD7, Dst_Instance: 0x00000000
23:33:36: RESTART_CAP type 1 length 12:
23:33:36: Restart_Time: 0x0000EA60, Recovery_Time: 0x0000EA60
```

Router 3 records this into its database. Also, both neighbors maintain the neighbor status as UP. However, Router 3's control plane fails at some point (for example, a primary RP failure). As a result, RSVP and TE lose their signaling information and states although data packets continue to be forwarded by the line cards.

When Router 3 declares communication with Router 2 lost, Router 3 starts the restart time to wait for the duration advertised in Router 2's restart time previously recorded (60 seconds). Routers 1 and 2 suppress all RSVP messages to Router 3 except hellos. Router 3 keeps sending the RSVP PATH and RESV refresh messages to Routers 4 and 5 so that they do not expire the state for the LSP; however, Routers 1 and 3 suppress these messages for Router 2.

When Routers 1 and 3 receive the hello message from Router 2, Routers 1 and 3 check the recovery time value in the message. If the recovery time is 0, Router 3 knows that Router 2 was not able to preserve its forwarding information, and Routers 1 and 3 delete all RSVP states that they had with Router 2.

If the recovery time is greater than 0, Router 1 sends Router 2 PATH messages for each LSP that it had previously sent through Router 2. If these messages were previously refreshed in summary messages, they are sent individually during the recovery time. Each of these PATH messages includes a Recovery_Label object containing the label value received from Router 2 before the failure.

When Router 3 receives a PATH message from Router 2, Router 3 sends a RESV message upstream. However, Router 3 suppresses the RESV message until it receives a PATH message. When Router 2 receives the RESV message, it installs the RSVP state and reprograms the forwarding entry for the LSP.

Benefits

- **State Information Recovery:** RSVP graceful restart allows a node to perform self recovery or to help its neighbor recover state information when there is an RP failure or the device has undergone an SSO.
- **Session Information Recovery:** RSVP graceful restart allows session information recovery with minimal disruption to the network.
- **Increased Availability of Network Services:** A node can perform a graceful restart to help itself or a neighbor recover its state by keeping the label bindings and state information, thereby providing a faster recovery of the failed node and not affecting currently forwarded traffic.

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Harman Van Der Linde, havander@cisco.com

Cisco IOS MPLS LDP Support

Cisco IOS MPLS LDP offers standards-based feature capabilities for MPLS label information signaling between MPLS-enabled routers. In addition to RFC3036-compliant MPLS signaling, Cisco's MPLS LDP also offers a number of value-added feature capabilities, which enable improved configuration and usability of MPLS LDP functionality. MPLS LDP feature capabilities are focused on MPLS LDP CLI configuration enhancements, enhanced security, and coexistence support with the Cisco High Availability (HA) feature set, including NSF/SSO and ISSU.

In Release 12.2(33)SXH, various new LDP feature enhancements are introduced, which include:

MPLS LDP Session Management, Label Signaling and Assignment:

- MPLS LDP: Static Label Support
- MPLS LDP: VRF-aware Static Label Support

MPLS LDP High Availability:

- MPLS LDP: Graceful Restart (GR) Support
- MPLS LDP: Session Protection
- MPLS LDP: HA (SSO, NSF, and ISSU) Support

Benefits

Key benefits of the Cisco MPLS LDP feature portfolio are:

- **MPLS LDP Support for Static Labels:** Enables configuration of static bindings between MPLS labels and IPv4 prefixes to support MPLS hop-by-hop forwarding through neighbor router nodes, which don't support LDP label distribution. With this feature static MPLS cross-connects can be configured to support MPLS Label Switched Path (LSP) midpoints in an MPLS network where neighbor router nodes do not support LDP or RSVP label distribution, but do support MPLS forwarding.
- **MPLS LDP Support for MPLS High Availability (HA):** MPLS LDP support for MPLS HA enables LDP sessions to stay operational during a Route Processor (RP) switch-over event and this way LDP-established MPLS forwarding entries will not be removed and will stay operational until LDP has re-initialized itself with it's remote neighbor (helper) nodes.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- MPLS Label Distribution Protocol (LDP): http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a00800a8698.html
- MPLS Static Labels: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008010dd41.html
- VRF Aware MPLS Static Labels: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_white_paper09186a00801b23af.shtml
- MPLS LDP Graceful Restart: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a008029b285.html
- MPLS LDP Session Protection: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a00802d95d9.html
- NSF/SSO-MPLS LDP: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a008029b285.html

Product Management Contact: Harmen van der Linde, havander@cisco.com

VRF Aware Syslog

The VRF Aware System Message Logging (Syslog) feature allows a customer to send system logging (syslog) messages to a syslog server host connected through a Virtual Private Network (VPN) Routing and Forwarding (VRF) interface. Logging information can be used for network monitoring and troubleshooting. This feature extends this capability to network traffic connected through VRFs.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

Any Transport over MPLS: ATM Adaptation Layer 5 (AAL5) over MPLS

Any Transport over MPLS: ATM AAL5 over MPLS enables a network provider to transport ATM AAL5 frames across an MPLS backbone. This extends the reachability of ATM and allows Service Providers to aggregate ATM transport and IP transport across a common packet backbone. The Service Provider can integrate an existing ATM environment with the packet backbone to improve operational efficiency and make use of the high-speed packet interfaces to scale the ATM implementations.

Transporting ATM AAL5 across MPLS networks provides a number of benefits, including:

- ATM PVC extended service.
- Aggregation to a higher speed backbone, such as OC-192, in order to scale ATM implementations.
- Improved operational efficiency. The MPLS backbone becomes the single network that integrates the various existing networks and services.

ATM AAL5 over MPLS transports ATM AAL5 frames across the MPLS backbone instead of cells, creating an efficient transport mechanism of ATM PVCs.

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Tim McSweeney, timcswee@cisco.com

ATM OAM Cell Emulation

In Release 12.2(33)SXH, the Catalyst 6500 Series Switch supports ATM Operation, Administrative, and Maintenance (OAM) cell emulation with AAL5 over MPLS. You configure OAM cell emulation on both PE routers, which emulates a VC by forming two unidirectional LSPs. After OAM cell emulation is enabled on a router, you can configure and manage the ATM VC in the same manner as you would a terminated VC. A VC that has been configured with OAM cell emulation can send loopback cells at configured intervals toward the local CE router. The endpoint can be either of the following:

- End-to-end loopback, which sends OAM cells to the local CE router.
- Segment loopback, which responds to OAM cells to a device along the path between the PE and CE routers.

The OAM cells include the following:

- Alarm Indication Signal (AIS)
- Remote Defect Indication (RDI)

These cells identify and report defects along a VC. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream devices affected by the failure. When a router receives an AIS cell, it marks the logical interface down and sends an RDI cell to let the remote end know about the failure.

Hardware
Cisco Catalyst 6500 Series Switches

Product Management Contact: Tim McSweeney, timcswee@cisco.com

Any Transport over MPLS: ATM Cell Relay over MPLS

Any Transport over MPLS: ATM Cell Relay over MPLS enables a Service Provider to carry ATM cells transparently across the MPLS backbone. This functionality is supported for single ATM cells in PVC mode only. ATM cell relay treats each ATM cell as a data packet and transports it across the MPLS network. This allows cells to be carried, regardless of which adaptation layer is used underneath. ATM Cell Relay over MPLS is more versatile than ATM AAL5 over MPLS, which carries only AAL5 frames. Other AAL types, such as AAL2 and AAL1, cannot be carried across the packet backbone, even if Quality of Service (QoS) is not an issue.

ATM Cell Relay over MPLS also allows the signaling of Operation, Administration, and Maintenance (OAM) cells to pass transparently across the packet network.

Hardware
Cisco Catalyst 6500 Series Switches

Product Management Contact: Tim McSweeney, timcswee@cisco.com

Any Transport over MPLS: Ethernet over MPLS

Any Transport over MPLS: Ethernet over MPLS enables a Service Provider to transport Ethernet VLAN packets across an MPLS backbone. This extends the reachability of Ethernet and allows Service Providers to offer Ethernet as a service to end customers.

A number of applications involve transporting raw Ethernet packets across MPLS networks, including:

- Metro Ethernet service
- Point-to-point Ethernet service
- LAN or broadcast domain extensions
- Remote peering and distributed Network Access Points (NAPs)

The Provider Edge (PE) router does not need to peer with the customer device. The Service Provider does not carry any customer IP routing information but instead transports the Layer 2 frames across the network. This is analogous to providing a Layer 2 circuit point-to-point.

Other MPLS features can be enabled on the PE router with AToM support, such as MPLS Virtual Private Networks (VPNs). For end users, the connectivity to remote sites is the same as if they were on the same LAN, and they do not have to modify their applications.

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Tim McSweeney, timcswee@cisco.com

Any Transport over MPLS Graceful Restart

The AToM Graceful Restart feature assists neighboring routers that have nonstop forwarding (NSF), Stateful Switchover (SSO) and Graceful Restart (GR) for Any Transport over MPLS (AToM) to recover gracefully from an interruption in service. AToM GR functions strictly in helper mode, which means it helps other routers that are enabled with the NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature to recover. If the router with AToM GR fails, its peers cannot help it recover. AToM GR is based on the MPLS Label Distribution Protocol (LDP) Graceful Restart feature.

AToM GR works in strict helper mode, which means it helps a neighboring route processor that has AToM NSF/SSO to recover from a disruption in service without losing its MPLS forwarding state. The disruption in service could result from a TCP or User Datagram Protocol (UDP) event or the stateful switchover of a route processor. AToM GR is based on the MPLS LDP Graceful Restart feature, which preserves forwarding information for AToM circuits during an LDP session interruption. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding state are recovered.

Additional Information

For more information related to how the LDP Graceful Restart feature works, see the MPLS LDP Graceful Restart feature module:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00806994d4.html

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Tim McSweeney, timcswee@cisco.com

Multiplexed UNI

This feature enables Layer 2 Switching and L2 VPN services on a single physical interface.

Benefits

There is no need to configure separate physical interfaces to offer multiple VLAN and VPN services

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Chiara Regale, chiarar@cisco.com

MPLS Management

CISCO IOS MPLS Embedded Management

Cisco IOS MPLS embedded management offers standards-based management capabilities for IP/MPLS networks. The Cisco industry leading MPLS management feature portfolio offers network operators detailed MPLS resource monitoring and connectivity troubleshooting capabilities, which include MPLS-specific SNMP MIBs, MPLS OAM, and MPLS-enabled NetFlow features.

In Release 12.2(33)SXH, various new enhancements are introduced to the MPLS embedded management feature portfolio, including enhanced MPLS MIB and MPLS OAM support. The MPLS embedded management feature portfolio can be summarized as follows:

MPLS MIBs:

- MPLS LSR MIB: IETF draft version 05
- MPLS LDP MIB: IETF draft version 08
- MPLS TE MIB: IETF draft version 05
- MPLS TE FRR MIB: IETF draft version 01 **New**
- MPLS VPN MIB: IETF draft version 05

MPLS OAM:

- MPLS LSP Ping/Trace for MPLS core (LDP IPv4 and RSVP IPv4 FEC support): IETF draft version 03 **New**
- IP SLA automation for MPLS LSP Ping/Trace for MPLS core **New**
- MPLS LSP Ping for Layer-2 VPNs (via VCCV): IETF draft version 03 **New**

MPLS NetFlow:

- MPLS-aware NetFlow
- MPLS Prefix Application Label (PAL)

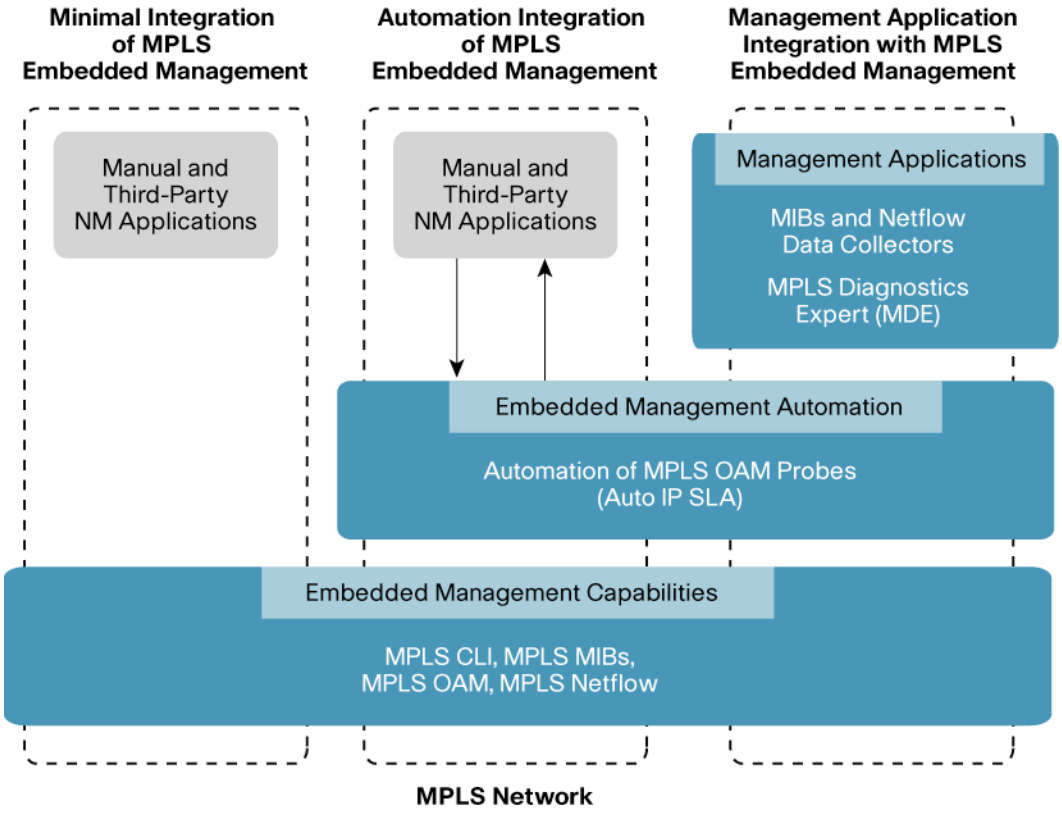
The embedded management capabilities for MPLS can be used in various usage scenarios ranging from manual CLI-based trouble shooting to a fully automated trouble shooting solution. In

addition to MPLS MIB, OAM, and NetFlow features, Cisco also offers complementary management tools, which can be integrated with embedded MPLS management capabilities:

- **Auto IP SLA:** Automatic execution of MPLS OAM probes.
- **Cisco MPLS Diagnostics Expert (MDE):** Unique Cisco management application for automated MPLS troubleshooting, which leverages embedded MPLS management capabilities.

Depending on the level of automation and integration needed, an operator may choose to use MPLS OAM capabilities manually via CLI access or to leverage the Cisco Auto IP SLA and MDE application to deploy a fully automated MPLS failure detection, isolation, and diagnosis solution.

Figure 21. Cisco IOS Embedded MPLS Management Framework



Benefits

Key benefits of the Cisco MPLS embedded management solution are:

- **Enables enhanced MPLS resource monitoring:** MPLS MIB modules provide standard SNMP access to a wide variety of MPLS-specific resources supported on Label Switched Routers (LSR), including MPLS label forwarding and LDP session information. Existing SNMP-based management applications can be configured to retrieve and collect MPLS-specific management information via the new MPLS MIB modules.
- **Increases operational efficiency:** MPLS OAM tools, such as LSP Ping and LSP Trace, enable fast detection and isolation of complex MPLS connectivity problems, which improves trouble resolution time and will help with reducing network downtime.
- **Provides a comprehensive solution for addressing MPLS network and service availability:** The Cisco MPLS embedded management capabilities, together with Cisco Auto IP SLA automation and automated trouble resolution capabilities via the Cisco MPLS

Diagnostics Expert (MDE), provide a comprehensive end-to-end solution for MPLS network monitoring and trouble resolution.

Additional Information

- MPLS Label Switching Router MIB: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a00804b66b8.html
- MPLS Label Distribution Protocol MIB: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a00801149ff.html
- MPLS Traffic Engineering (TE) MIB: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008008705e.html
- MPLS VPN: MIB Support: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008016108a.html#wp1037190
- MPLS Embedded Management: LSP Ping/Traceroute and AToM VCCV: http://www.cisco.com/en/US/partner/products/ps6566/products_feature_guide09186a008063d009.html
- Cisco Auto IP SLA: http://www.cisco.com/en/US/partner/products/ps6566/products_feature_guide09186a008052845 0.html
- Cisco MPLS Diagnostics Expert: http://www.cisco.com/en/US/products/ps6755/index.html

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contacts:

- **MPLS Embedded Management:** Harmen van der Linde, havander@cisco.com
- **Cisco Auto IP SLA:** Ernie Mikulic, emikulic@cisco.com
- **Cisco MPLS Diagnostics Expert (MDE):** Stephen Speirs, sspeirs@cisco.com

Pseudo Wire Emulation Edge to Edge (PW-E3) MIB Support

This feature provides the infrastructure for PW-E3 (Pseudo Wire Emulation Edge to Edge) to manage Ethernet attachment circuits in L2 VPN deployments.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

IP Services (Including QoS Features)

Enhanced Object Tracking

The Enhanced Object Tracking feature provides complete separation between the objects to be tracked and the action to be taken by a client when a tracked object changes. Thus, several clients such as HSRP, VRRP, or GLPB can register their interest with the tracking process, track the same object, and each take different action when the object changes.

Each tracked object is identified by a unique number that is specified on the tracking Command-Line Interface (CLI). Client processes use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

The tracking capabilities have been enhanced to enable the configuration of a combination of tracked objects in a list, and a flexible method of combining objects using Boolean logic. The enhancements introduced the following capabilities:

- **Threshold:** The tracked list can be configured to use a weight or percentage threshold to measure the state of the list. Each object in a tracked list can be assigned a threshold weight. The state of the tracked list is determined by whether or not the threshold has been met.
- **Boolean “and” function:** When a tracked list has been assigned a Boolean “and” function, it means that each object defined within a subset must be in an up state so that the tracked object can become up.
- **Boolean “or” function:** When the tracked list has been assigned a Boolean “or” function, it means that at least one object defined within a subset must be in an up state so that the tracked object can become up.

Object tracking of IP SLAs operations allows tracking clients to track the output from IP SLAs objects and use the provided information to trigger an action.

Cisco IOS IP SLAs is a network performance measurement and diagnostics tool that uses active monitoring. Active monitoring is the generation of traffic in a reliable and predictable manner to measure network performance. Cisco IOS Software uses IP SLAs to collect real-time metrics such as response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss.

These metrics can be used for troubleshooting, for proactive analysis before problems occur, and for designing network topologies.

Benefits

- Increases the availability and speed of recovery of a router system.
- Decreases outages and their duration.
- Provides a scalable solution that allows processes such as HSRP, GLBP or VRRP to track objects individually or a list of objects.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbeb.html

Product Management Contact: Benoit Lourdelet, blourdel@cisco.com

Stateful SwitchOver (SSO) for HSRP and GLBP

The SSO Aware FHRP (respectively GLBP) feature enables the Cisco IOS HSRP (respectively GLBP) subsystem software to detect that a standby RP (Route Processor) is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP (respectively GLBP) group itself and traffic continues to be forwarded through the current active gateway router.

Prior to this feature, when the active HSRP (respectively GLBP) router primary RP failed, it would stop participating in the HSRP (respectively GLBP) group and trigger another router in the group to take over as the active HSRP (respectively GLBP) router.

The SSO-Aware HSRP feature is required to preserve the forwarding path for traffic destined to the HSRP (respectively GLBP) virtual IP through a RP switchover.

Configuring SSO on the edge router enables the traffic on the Ethernet links to continue during an RP failover without the Ethernet traffic switching over to an HSRP (respectively GLBP) standby router (and then back, if preemption is enabled).

With this feature, HSRP (respectively GLBP) SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP (respectively GLBP) virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP router, then the standby HSRP (respectively GLBP) router takes over as the active HSRP (respectively GLBP) router.

Benefits

The addition of SSO to the HSRP and GLBP redundancy scheme unparallel gateway high availability scheme.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080245c05.html

Product Management Contact: Benoit Lourdelet, blourdel@cisco.com

Message Digest 5 (MD5) Authentication for HSRP and GLBP

Before the introduction of MD5 authentication, HSRP and GLBP authenticated protocol packets with a simple plain text string. HSRP and GLBP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP and GLBP portion of the multicast HSRP and GLBP protocol packet. This functionality provides added security and protects against the threat from HSRP and GLBP spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP and GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash, the packet is ignored.

Benefits

Protects against HSRP and GLBP spoofing software

Uses the industry-standard MD5 algorithm for improved reliability and security

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html#wp1077140
- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fb97.html#wp1056945

Product Management Contact: Benoit Lourdelet, blourdel@cisco.com

TCP Maximum Segment Size (MSS) Adjustment

The TCP MSS Adjustment feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments in the SYN bit set, when PPP over Ethernet (PPPoE) is being used in the network. PPPoE truncates the Ethernet Maximum Transmission Unit (MTU) 1492, and if the effective MTU on the hosts (PCs) is not changed, the router in between the host and the server can terminate the TCP sessions. The ip tcp adjust-mss command specifies the MSS value on the intermediate router of the SYN packets to avoid truncation.

Usage Guidelines

When a host initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the Maximum Transmission Unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes.

The PPP over Ethernet (PPPoE) standard supports a MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the ICMP error messages that must be relayed from the host in order for path MTU to work.

The ip tcp adjust-mss command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

Considerations

The ip tcp adjust-mss command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the max-segment-size argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the ip mtu command on the same interface as the ip tcp adjust-mss command, it is recommended that you use the following commands and values:

```
ip tcp adjust-mss 1452
ip mtu 1492
```

Example

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1.255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
 pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
 ip address negotiated
```

```
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list permit ip 192.168.100.0.0.0.0.255 any
```

Hardware
Cisco Catalyst 6500 Series Switches

Product Management Contact: Rick Williams, rwill@cisco.com

AutoQoS

Cisco IOS AutoQoS represents innovative technology that simplifies a network administrator's challenges by reducing Quality-of-Service (QoS) complexity and deployment time and cost in Enterprise networks. Cisco AutoQoS incorporates value-added intelligence in Cisco IOS® Software and Cisco Catalyst® OS software to provision and manage large-scale QoS deployments.

AutoQoS offers straightforward capabilities to automate Voice-over-IP (VoIP) deployments for customers who want to deploy IP telephony, but who lack the expertise and/or staffing to plan and deploy IP QoS and IP services.

Customers can more easily provision and manage successful QoS deployments using Cisco AutoQoS together with CiscoWorks QoS Policy Manager (Cisco QPM). Cisco AutoQoS provides QoS provisioning for individual routers and switches, simplifying deployment and reducing human error. Cisco QPM provides centralized QoS design, administration, and traffic monitoring that scales to large QoS deployments.

Quality-of-Service Deployment Overview
Cisco AutoQoS simplifies and shortens the QoS deployment cycle. The five major aspects of successful QoS deployments are:

1. Application classification
2. Policy generation
3. Configuration
4. Monitoring and reporting
5. Consistency

Each aspect presents challenges to the network manager.

Application Classification

The first step in deploying QoS is identifying and categorizing the network traffic generated by each application. Access Control Lists (ACLs) are the most commonly used tools for identifying traffic. ACLs use information from Layer 3 (IP addresses) and Layer 4 (TCP/User Datagram Protocol [UDP] port numbers) to identify traffic. However, using ACLs alone to deploy QoS rapidly increases the size and number of ACLs required in a network. Furthermore, they cannot easily identify all applications (that is, various kinds of HTTP traffic).

Policy Generation

Developing the initial QoS policy often challenges customers, who must balance QoS policy variables (bandwidth, delay, jitter, and packet loss) to achieve the desired application performance. Cisco QoS empowers the network manager to set policies for delivering the desired application performance for the business; however, many customers lack the required expertise to arrive at a starting point for their QoS policies.

Configuration

Network devices need to be programmed with the right set of features and parameters to implement the policy. Although QoS is rich in features, the process of effective implementation is time-consuming. Without automation, the QoS configuration challenge can be very complex.

Monitoring and Reporting

Customers are often deluged with large quantities of data, but very little relevant information that helps them to identify the cause of a problem or any important trends (for example, traffic patterns and exceptions). Obtaining the right information can be quite expensive, and it often arrives too late to be useful. A typical example is finding out “who” (that is, which user or IP address) is causing congestion or creating abnormal loads on a link. Without automation, establishing an efficient monitoring process can take many months.

Consistency

Customers are faced with managing QoS policies consistently across multiple kinds of devices in the network, including IP phones, switches, and routers. Different devices and vendors often implement QoS functionality differently, creating a challenge for the network manager.

Cisco AutoQoS: A New Paradigm For Simplifying Quality of Service

Cisco AutoQoS provides a new paradigm for automating the delivery of network QoS. It simplifies the provisioning of network QoS with intelligence and shortens the QoS deployment cycle.

Customers can use Cisco AutoQoS to:

- Get a quick start on QoS deployment
- Automate the most common deployment scenarios
- Identify and classify applications
- Establish alert conditions

Cisco AutoQoS addresses the major elements of end-to-end QoS deployments, using decades of networking experience, extensive lab performance testing, and input from a broad base of customer AVVID (Architecture for Voice, Video and Integrated Data) installations to determine the optimal QoS configuration for typical VoIP deployments. (See Figure 22).

Figure 22. Cisco AutoQoS: Simplifying QoS Deployment

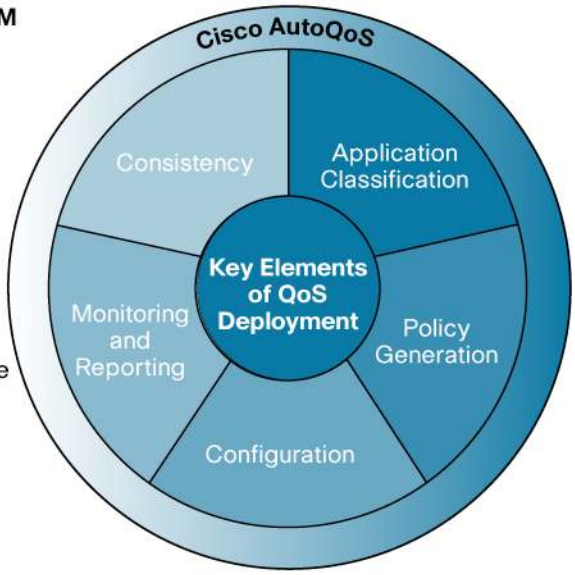
Agile QoS Deployment for VoIP Using Cisco AutoQoS-VoIP and CiscoWorks QPM

- **Application Classification**
  - AutoQoS identifies VoIP bearer and control traffic
- **Policy Generation**
  - AutoQoS evaluates the network environment and generates initial policy on a given Port, Interface, or PVC

Configuration
- AutoQoS provides a single command to enable QoS on each interface/PVC
- QPM provides centralized network-wide configuration, management, and monitoring

Monitoring and Reporting
- Traps issued on VoIP packet drops
- QPM uses data received from network devices to generate QoS reports

Consistency
- AutoQoS is fully inter-operable between LAN and WAN devices



Cisco AutoQoS-Simplifying QoS Deployment

Cisco AutoQoS addresses the five key elements of QoS deployment.

Application Classification

Cisco AutoQoS uses intelligent classification on routers, utilizing Cisco Network-Based Application Recognition (NBAR) to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol for voice packets, helping ensure that the device attached to the LAN is really an IP phone.

Policy Generation

Cisco AutoQoS evaluates the network environment and generates an initial policy. It automatically determines WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM interworking, eliminating the need to understand QoS theory and design practices in various scenarios. Customers can meet additional or special requirements by modifying the initial policy as they normally would.

The first release of Cisco AutoQoS provides the necessary AutoQoS-VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. AutoQoS-VoIP will automatically employ Cisco NBAR to classify voice traffic and mark it with the appropriate Differentiated Services Code Point (DSCP) value. AutoQoS-VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.

Configuration

With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network requirements.

Not only will Cisco AutoQoS automatically detect Cisco IP phones and enable QoS settings; it also will disable the QoS settings when a Cisco IP Phone is relocated or moved to prevent malicious activity.

Monitoring and Reporting

Cisco AutoQoS provides visibility into the classes of service deployed using system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (for example, VoIP packet drops).

Cisco QPM uses the Cisco Systems® intelligent IP network to provide visibility into network operations. Users can measure traffic throughput for top applications and service classes; they can also troubleshoot problems with real-time and historical QoS feedback. Traffic and QoS statistics can be displayed as line or bar charts in bits or packets per second, per interface or policy. Cisco QPM enables a user to view graphs before and after QoS deployment, tied to traffic filters and policies, as well as results from QoS policy actions.

Consistency

Cisco AutoQoS policies are designed to work together across Cisco devices, helping ensure consistent end-to-end QoS.

Features and Benefits

Cisco AutoQoS simplifies deployment and speeds provisioning of QoS technology over a Cisco network infrastructure. It reduces human error and lowers training costs. With AutoQoS-VoIP, you use just one command to enable QoS for VoIP across every Cisco router and switch. You can also modify an AutoQoS-generated policy to meet your specific requirements.

Tables 12 and 13 detail the initial Cisco AutoQoS features for Cisco IOS Software and Cisco Catalyst OS software.

Table 12. Cisco AutoQoS for VoIP in the WAN

Feature	Benefit
Autodetermination of WAN Settings	Automatic determination of WAN settings for fragmentation and interleaving, compression, encapsulation, and Frame Relay-ATM interworking. Eliminates the need to understand QoS theory and design practices in common deployment scenarios.
Initial Policy Generation	Initial policy generation provides users an advanced starting point for VoIP deployments. This reduces the time needed to establish an initial, feasible QoS policy solution that includes providing QoS to VoIP bearer traffic, signaling traffic, and best-effort data. The initial policy can be modified to meet additional or special requirements.
Traps and Reporting	Syslog and SNMP traps provide visibility into the classes of service deployed and notification of abnormal events such as VoIP packet drops.
Intelligent Classification of Network Traffic	Using Cisco NBAR for deep and stateful packet inspection, this feature can identify VoIP bearer and control traffic. Simplifies QoS configurations by reducing, and in some cases eliminating, the need for ACLs.

Table 13. Cisco AutoQoS for VoIP in the LAN

Feature	Benefit
Simplified Configuration	• In one command, AutoQoS configures the port to prioritize voice traffic without affecting other network traffic. • Includes the flexibility to tune AutoQoS settings for unique network requirements.
Automated and Secure	Automatically detects Cisco IP phones and enables AutoQoS settings. Prevents malicious activity by disabling QoS settings when a Cisco IP Phone is relocated/moved.
Optimal VoIP Performance	• Uses decades of networking experience, extensive lab performance testing, and input from a broad base of customer AVVID installations to determine the optimal QoS configuration for typical VoIP deployments. • Uses all advanced QoS capabilities of the Cisco Catalyst switches.
End-to-End Interoperability	Designed to work well with the AutoQoS settings on all other Cisco switches and routers, helping ensure consistent end-to-end QoS.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/tech/tk543/tk759/tk879/tsd_technology_support_protocol_home.html

Product Management Contact: Michael Lin, mhelin@cisco.com

CBQOSMIB Index Persistency

The Class-based QoS MIB Index Persistency feature in Cisco IOS Software Release 12.2(33)SXH solves the following Class-based QoS MIB indexing problem: previously, Class-based QoS MIB indexes that pointed to CBQoSMIB variables changed each time the system rebooted. This required that network management applications frequently reread the CBQoSMIB to obtain accurate statistical and configuration information. The following three Class-based QoS MIB indexes changed each time the system rebooted:

- cbQosConfigIndex
- cbQosObjectstIndex
- cbQosPolicyIndex

Prior to Cisco IOS Software Release 12.2(33)SXH, each Modular QoS Configuration (MQC) and policy map was indexed by its own separate cbQosObjectstIndex instance, which resulted in degraded CPU performance when extensive policy maps were in use. The Class-based QoS MIB Index Persistency feature solves this problem with the following, new Class-based QoS MIB index scheme:

- Does not use cbQosObjectstIndex instances to index policy maps or Modular QoS Configurations (MQCs). Policy maps are indexed directly by the cbQosPolicyIndex. Modular QoS Configurations (MQCs) are indexed by instances of cbQosConfigIndex.
- Maintains two separate indexes:
  - Service Policy Index
  - QoS Configuration Index

Benefits

- Significantly reduces to the number of cbQosObjectsIndex instances
- Reduces the complexity of configuring and correlating statistics objects, making it easy for network management application to gather accurate information

Additional Information

- http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html
- http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Hardware

Cisco Catalyst 6500 Series Switches

Product Management Contact: Michael Lin, mhelin@cisco.com

Embedded Management

IOS Configuration Rollback

IOS Configuration Rollback/Replace allows network administrators the ability to automatically "undo" changes to the currently running configuration with an archived configuration file.

Currently, rolling back changes to the running configuration requires one of two tasks:

- Manually undoing the original config changes
- Reboot to the start-up config

IOS Configuration Rollback/Replace provides a new third option allowing efficiency improvements through automation, increased accuracy and reduced downtime.

Combined with periodic off-site storage of config files (configuration archive) over File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), IOS Config Rollback/Replace allows network operations to rollback to any saved IOS configuration state without rebooting or manual reconfiguration.

IOS Configuration Rollback/Replace detects and adjusts to situations where an IOS command in the configuration file is not applicable to the current hardware or software configuration. In these cases, IOS Config Rollback/Replace will provide a list of commands which could not be applied.

IOS Configuration Rollback/Replace only makes changes to the IOS commands which are different between the current running config and the saved config state. This shortens the time to Rollback as the configuration changes only happen for a subset of commands. The Rollback will add lines which do not appear in the running config and will remove command lines which do not appear in the saved configuration file.

IOS Configuration Rollback/Replace handles order-sensitive commands (such as Access Control Lists) and adjusts appropriately. If needed, IOS Config Rollback/Replace will perform multiple passes over the running configuration to leave the system in a functional state during rollback.

Benefits

- **Increased Accuracy:** The network administrator has the ability to quickly undo configuration changes back to any well-known state without manual configuration.
- **Reduced Downtime:** Using IOS Configuration Rollback/Replace to restore the running config to a well-known state avoids rebooting to the startup config and applying changes manually.
- **Improved Efficiency:** Allows quick restoration to the last configuration to quickly undo configuration changes without manually configuring through CLI.

- **Improved Configuration Speed:** IOS Configuration Rollback/Replace only applies the changes between the configurations improving the speed of applying configuration changes.

Hardware

Routers	Cisco 7304 and 10000 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080356ea5.html

Product Management Contact: Steve Giles, stgiles@cisco.com

Contextual Diff Utility

The Contextual Configuration Diff Utility allows users to view the differences between any two Cisco IOS configuration files, located locally or remotely, including the startup or running configs. The output includes the submode information to provide the context for the command differences.

The Contextual Configuration Diff Utility feature provides the ability to perform a line-by-line comparison of any two configuration files (accessible through the Cisco IOS File System) and generate a list of the differences between them. The generated output includes information regarding configuration lines that have been added, modified, or deleted, and the configuration modes within which a changed configuration line exists.

Benefits

- **Auditability:** The ability to audit the changes to configuration using the Contextual Diff Utility improves the change management and provisioning tracking capabilities.
- **Contextual:** The Contextual Diff Utility knows where the submodes exist and performs improved display of configuration changes which would not be properly rendered using non-contextual diff utilities.
- **Improved Change Tracking and Rollback:** Knowing what changes have occurred in a configuration allows rollback capabilities without reloading a complete config.
- **Improved Automation Environment:** Contextual Diff Utility enables automated comparisons of configurations on-the-box saving manual effort needed to download the configurations to an external system and using diff utilities.

Hardware

Routers	Cisco 10000, UBR 10000, UBR 7200, 7300 Series Routers

Additional Information

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1dc2.html

Product Management Contact: Steve Giles, stgiles@cisco.com

Config Logger Persistency

Cisco IOS Software uses the startup-config file to save router configuration commands across reloads. This single file contains all the commands that need to be applied when the router reboots. The startup-config file gets updated every time a write memory command or copy url startup-config command is entered. As the size of the running-config file grows, the time to save the startup-config file to the NVRAM file system increases as well. Startup-config files can be 1 MB and larger. For files of this size, making a single-line change to the startup-config file requires that the entire startup-config file is saved again even though most of the configuration has not changed.

The Configuration Logger Persistency feature implements a “quick-save” functionality. The aim is to provide a “configuration save” mechanism where the time to save changes from the startup-config file is proportional to the size of the incremental changes (with respect to the startup-config file) that need to be saved.

The Cisco IOS configuration logger logs all changes that are manually entered at the command-line prompt. This feature also notifies the registered clients when changes to the log occur. The contents of the configuration log are stored in the run-time memory—the contents of the log are not persisted after reboots.

The Configuration Logger Persistency feature provides a mechanism to persist the configuration commands entered by users across reloads. Only the commands entered at the Command-Line Interface (CLI) (that is, the commands entered in configuration mode) are persisted across reload. This feature uses the Cisco IOS secure file system to persist the configuration commands that are generated.

Benefits

- **Improved Speed:** Only the changed configuration lines are applied at reload time.
- **Reduced Config File Across Reloads:** Since only the persistent configuration commands are stored across reloads, the size of the startup config file is significantly reduced.

Hardware

Routers	Cisco 10000, UBR 10000, UBR 7200, 7304 Series Routers

Additional Information

http://www.cisco.com/en/US/partner/products/ps6922/products_feature_guide09186a0080667752.html

Product Management Contact: Steve Giles, stgiles@cisco.com

Configuration Change Logging

The Configuration Change logging feature provides a way to track configuration changes made by users, on a per-session and per-user basis. System logging notifications can be enabled for when changes are made, and the log files (record of changes) can be sent to a remote syslog server.

Benefits

- **Increased Configuration Auditing:** As changes to the configuration occurs, audit records are generated indicating when the change occurred, who made the change and what the change was.
- **Configuration Security Monitoring:** Detect and monitor who is changing the configurations to verify that only authorized people are impacting the network.
- **Increased Automation:** Provides increased automation capabilities to synchronize offline configurations as changes occur.

Hardware

Routers	Cisco 10000, UBR 10000, UBR 7200, 7300 Series Routers

Additional Information

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1e81.html

Product Management Contact: Steve Giles, stgiles@cisco.com

Exclusive Configuration Change Access and Session Locking

The configuration lock (exclusive configuration change access) feature enables single-user access to the running configuration. The Access Session Locking feature adds functionality that prevents another user's attempted execution of User Mode commands until the system finishes processing the commands executed by the user with Excluding Configuration Change Access.

The Exclusive Configuration Change Access feature ("exposed lock") is complementary with the locking mechanism in the Configuration Replace and Configuration Rollback feature ("rollback lock").

Benefits

- **Improved Control:** The integrity of the device being configured is significantly improved when only one person can configure it at a time.
- **Improved Uptime:** Operational uptime is improved by eliminating configuration conflicts between different users which may adversely impact operation.
- **Increased Automation Capabilities:** By allowing applications to exclusively change configurations without being impacted by other configuration operations, programs can be developed which automate configuration and provisioning of the device.

Hardware

Routers	Cisco 10000, 7304, UBR 10000, UBR 7200 Series Routers

Additional Information

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a008036a23c.html

Product Management Contact: Steve Giles, stgiles@cisco.com

IPv6 Default Router Selection

The Router Advertisement (RA) mechanism (RFC2461), amongst other things, informs hosts about the default routers on a link. Hosts maintain a default router list from which one is selected for traffic to remote destinations. The selection for a destination is then cached. RA allows round-robin, or “always the same: selection mechanisms.”

This is simple and works well in most cases. But there are times where it is suboptimal when some form of traffic engineering is desired. For instance, when two routers on a link provide equivalent, but not equal-cost routing, policy may dictate that one is preferred. In current implementation, there is no mechanism to inform the hosts to prefer one default router over the others.

IPv6 Default Router Preference (DRP) can provide preference metric for default routers. IPv6 DRP is the Cisco IOS implementation of the RFC 4191, enabling a network manager to assign a priority to a router. This new feature introduces a new command under the interface configuration:

```
ipv6 nd router-preference {High|Medium|Low}
```

The “low” keyword indicates the least preferred, while the “High” keyword indicates the most preferred default router. If this command is not applied, RAs are sent with the default preference of “Medium”.

Benefits

- Allow end devices to select a more optimal default router to remote destinations.
- Reduces the number of redirect messages sent from the non-optimal default routers.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information

- http://www.ietf.org/rfc/rfc4191.txt
- http://www.faqs.org/rfcs/rfc2461.html

Product Management Contact: Patrick Grossetete, pgrosset@cisco.com

NetFlow Egress Multicast Enhancement

The NetFlow Multicast support feature was introduced on Catalyst 6500 Series Switches with Release 12.2(18)SXF. It lets you capture multicast-specific data (both packets and bytes) for multicast flows. The NetFlow Multicast Support feature can identify and count multicast packets on the ingress side or the egress side (or both sides) of a router. Multicast ingress accounting provides information about the source and the number of times the traffic was replicated, and multicast egress accounting monitors the destination of the traffic flow.

NetFlow Egress Multicast has been enhanced to support RFP-Check Failure. The NetFlow Multicast Support feature lets you enable NetFlow statistics to account for all packets that fail the Reverse Path Forwarding (RPF) check that are dropped in the core of the Service Provider network. Accounting for RPF-failed packets provides more accurate traffic statistics and patterns.

Hardware

Routers	Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

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

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

NetFlow for IPv6 Unicast Traffic

NetFlow for IPv6 is based on NetFlow Version 9 and functions by identifying packet flows for ingress IP and IPv6 packets. NetFlow enables you to collect traffic flow statistics on your routing devices and analyze traffic patterns, which are used to detect DoS attacks. It does not involve any connection-setup protocol between routers or to any other networking device or end station and does not require any change externally, either to the traffic or packets themselves or to any other networking device.

NetFlow is completely transparent to the existing network, including end stations and application software and network devices such as LAN switches. Also, NetFlow is performed independently on each internetworking device; it need not be operational on each router in the network. You can use NetFlow Data Export (NDE) to export data to a remote workstation for data collection and further processing. Network planners can selectively invoke NDE on a router or on a per-sub interface basis to gain traffic performance, control, or accounting benefits in specific network locations. NetFlow collects accounting information for IPv6 encapsulation and tunnels. If NetFlow capture is configured on a logical interface, IPv6 flows will be reported with that interface as the input or output interface, depending on whether the feature has been activated on the ingress or egress port.

Hardware

Routers	Cisco 800, 1800, 2800, 3800, 7200, and 7300 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

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

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

NetFlow MIB and TopNTalkers

Understanding who is using the network and for how long, what protocols and applications are being utilized and where the network data is flowing is a necessity for today's IP network managers. NetFlow data can be used for a variety of purposes, including network management and planning, user and security monitoring, protocol and application monitoring, Enterprise accounting, and departmental charge backs, Internet Service Provider (ISP) billing, data warehousing, and data mining for marketing purposes.

Traditionally NetFlow information is exported from the router and persistently stored and analyzed by network management applications. An additional method to retrieve NetFlow data is now available: The NetFlow MIB (CISCO-NETFLOW-MIB) allows access to NetFlow data. The MIB will provide the ability to configure and modify NetFlow using an SNMP interface. The user can retrieve a snapshot of IP flow, protocol and packet size distribution information easily with SNMP. The NetFlow MIB will be very useful for security monitoring and detection of attacks by monitoring flow information. One of the key features of the NetFlow MIB will be Top N Talkers and the top conversations (NetFlow cache) information is now available. Also, included as part of the Top N Talkers feature is a new show command, so the user can monitor top conversations in the network using CLI.

Benefits

- A new additional method to retrieve NetFlow information
- Top N Talker NetFlow information using the CLI and MIB
- MIB access to IP flow, protocol and packet size distribution information
- Retrieval of NetFlow information when the traditional export may not be practical
- Useful security information directly from an SNMP MIB
- Remote configuration of NetFlow features without using CLI

Hardware

Routers	Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, and 7300 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

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

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

NetFlow: Per-interface/sub-interface NetFlow

NetFlow Data Export (NDE) is an important feature used in network accounting and traffic engineering. Today NDE on the Catalyst 6500 is global and enabled on all layer3 interfaces. To better utilize NetFlow table and control export, Interface-NDE selectively enables NetFlow entry creation and export per layer 3 interfaces.

Hardware

Routers	Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, 7300, and 7600 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

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

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

Cisco IOS TCL

Cisco IOS Scripting with Tool Command Language (Tcl) provides the ability to run Tcl version 8.3.4 commands from the Cisco IOS Software Command-Line Interface (CLI).

Tcl is a standard scripting language, and a partial implementation of Tcl has been in Cisco IOS Software in support of internal applications, such as Cisco IOS Software Interactive Voice Response (IVR).

Tcl version 8.3.4 provides support for the Embedded Syslog Manager (ESM) feature as well as exposing a Tcl Shell (tclsh) for use in the Cisco IOS Software CLI.

SNMP MIB Object Access

Designed to make access to Simple Network Management Protocol (SNMP) MIB objects easier, a set of UNIX-like SNMP commands has been created. The Tcl shell is enabled either manually or by using a Tcl script, and the new commands can be entered to allow you to perform specified get and set actions on MIB objects. To increase usability, the new commands have names similar to those used for UNIX SNMP access.

Benefits

- **Powerful Scripting Capability:** Powerful method of custom-processing the events or states within a router, and taking a variety of actions based on them.
- **Easy to Learn:** Industry standard language.
- **Complete Coverage of Cisco IOS Software Commands:** All Cisco IOS Software CLI commands may be references by Tcl scripts, in both EXEC and CONFIG mode.
- **Customization of Cisco IOS Software Commands:** Tcl scripts can be used to create customized commands, grouping multiple IOS commands, processing and customizing output, even creating auto-refreshing commands for real-time refresh at the CLI level.

Hardware

Routers	Cisco 7200 Series, Cisco 7301, Cisco 7500 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/index.htm

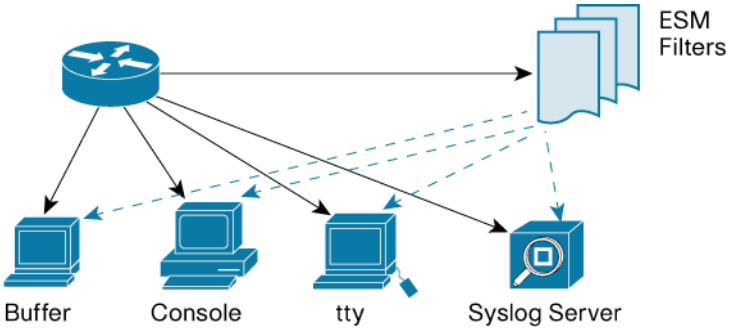
Product Management Contact: Madhu Vulpala, mvulpala@cisco.com

Embedded Syslog Manager

Embedded Syslog Manger (ESM) is a customizable framework integrated in Cisco IOS Software for correlating, augmenting, filtering, and routing syslog messages generated by the IOS logger. ESM allows complete control over system message logging at the source. ESM provides a programmatic interface to allow you to write custom filters that meet your specific needs in dealing with system logging.

ESM allows the user to configure post-processing of syslog messages with selected ESM filters, via new message queue in parallel with standard IOS syslog message stream. Either filtered or non-filtered syslog streams may be configured for individual syslog destinations. ESM leverages the Cisco IOS Scripting (Tcl 8.3.4).

Figure 23. Embedded Syslog Manager Version 1.0



Benefits

- **Customization:** Fully customizable processing of system logging messages, with support for multiple, interfacing syslog collectors.
- **Severity Escalation for Key Messages:** Ability to configure unique severity levels for syslog messages instead of using the system-defined severity levels.
- **Specific Message Targeting:** Ability to route specific messages or message types, based on type of facility or type of severity, to different syslog collectors.
- **SMTP-Base Email Alerts:** Capability for notifications using TCP to external servers, such as TCP-based syslog collectors or Simple Mail Transfer Protocol (SMTP) servers.
- **Message Limiting:** Ability to limit and manage syslog “message storms” by correlating device-level events.

Hardware

Routers	Cisco 7200 Series, Cisco 7301, Cisco 7500 Series Routers
Switches	Cisco Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/index.htm

Product Management Contact: Rick Williams, rwill@cisco.com

IP Service Level Agreements (SLAs)

Network services have changed dramatically in recent years, most notably due to the addition of Voice, Video, and other mission-critical delay and performance sensitive applications. The network has been embraced as a productivity tool. Customers have come to demand guaranteed, reliable network services as more business-critical applications are deployed across the network. Cisco IOS® IP Service Level Agreements (SLAs) is a capability embedded within nearly all Cisco IOS® and IOS-XR® devices, which allows Cisco customers to understand TCP/IP, VoIP, MPLS, and Metro-Ethernet service levels for Data, Voice, and Video, LAN and WAN network services. This results in increased productivity, lower operational costs, and reduces the frequency of unplanned network outages.

IP SLAs has become the standard for acquiring VoIP, MPLS, Metro-Ethernet and TCP/IPIP operational data for many customers. Visibility into the network is an indispensable tool. In response to new requirements and pressures, network operators are finding it critical to understand how the network is behaving.

The Challenge

IP Network services enhance the efficiency of the network, and help businesses achieve key objectives and gain a competitive advantage. Service levels and network performance are crucial because they test, monitor, and measure how well the IP services and business-critical applications are running. SLAs between Service Providers and customers or between corporate Enterprise IT departments and their end-users are intended to be the basis for service guarantees and validation.

In many cases it may be difficult to deliver differentiated services and monitor service levels. The chosen metrics are often not strict enough to allow for service differentiation. Many network administrators today have not implemented best practices for measuring IP services and service levels. When network performance is poorly understood, there is naturally a greater risk of network downtime and real potential for decreased network availability. When network administrators implement technology that can measure how well the network is performing for each service, they can then use that information to continually improve and adjust network performance in a baseline-monitor-test-modify-baseline loop.

Making modifications to any operational parameters in the network operation without a well defined plan to measure and monitor the effects of the changes, usually leads to poor end user satisfaction and network or service outages. Effectively measuring and monitoring IP services in real time should be a critical baseline component of network management toolkit that can contribute to increased profits, effective troubleshooting, and faster deployment of network applications in order to further business or organizational goals.

The Solution: Cisco IP SLAs

Cisco IP SLAs is embedded within Cisco IOS and Cisco IOS-XR Software and there is no additional device to deploy, learn, or manage. A dependable set of tools used to verify VoIP, MPLS, Metro-Ethernet and IP service levels, Cisco IP SLAs provides a scalable, cost-effective solution for network performance measurement.

Cisco IP SLAs is designed to generate measurement traffic samples in reliable, predictable, continuous or on-demand manner to test the network or service in question end to end. IP SLAs then collects and alerts on the resulting network performance information in real time such as server and network response times, one-way and round-trip latency, jitter, packet loss, voice quality measurement, and other network statistics. This enables user or network operators to continuously, reliably, and predictably measure network performance and proactively monitor network health. With Cisco IP SLAs, service level monitoring can be easily automated, service levels can be assured, network operation can be actively and continuously verified, and network performance can be measured.

Network administrators can additionally use Cisco IOS IP SLAs as a troubleshooting tool. They can obtain hop-by-hop performance statistics between any two Cisco devices or between a Cisco device and a host system or server. If the network performance level drops during any IP SLAs operation (ie: due to congestion), the network administrator can automatically and promptly identify the location of the bottleneck and resolve the problem. Cisco IOS IP SLAs can also be used to perform a network assessment for a new IP service or verify Quality of Service (QoS) levels. For example, Cisco IP SLAs can determine whether the network is ready for Voice over IP (VoIP) by simulating VoIP codec's and measuring network performance and VoIP quality across the IP network.

Key Cisco IOS IP SLAs Benefits

- Embedded in Cisco IOS and IOS-XR Software
- Automated real-time network performance and health monitoring and alerting
- Capable of verifying and measuring IP service levels and parameters needed for service level agreements
- Per-class QoS traffic monitoring
- Multiple Scheduling Algorithms
- Real-time notifications of Threshold Alerts with Simple Network Management Protocol (SNMP)
- Hop-by-hop, end-to-end, and any-to-any performance measurement capable
- Fully controlled through either SNMP MIB, Cisco IOS, or IOS-XR Software Command-Line Interface (CLI)
- VoIP codec simulation and VoIP quality measurement; Mean Opinion Score (MOS) and Calculated Planning Impairment Factor (ICPIF)
- Multiprotocol Label Switching (MPLS) network monitoring
- Integrated into several Cisco Network Management Solutions
- Integrated into several third-party Cisco Partner Network Management products

Cisco IP SLAs can measure and report on items such as:

- End to End One-Way and Round-Trip Network Latency, Packet Loss and Jitter
- Voice Quality
- Network Availability
- Service Availability
- Network Change Impact
- QoS Class of Service Testing
- Troubleshooting

Cisco IP SLAs features at a glance:

- VoIP, TCP/IP, MPLS, and Metro-Ethernet Operation Types
- Microsecond Resolution
- Real-Time Threshold Alerts through SNMP Trap
- Hourly Aggregates Storage and Retrieval up to 24 Hours Per/Operation
- VRF Routable Operations
- QoS Verification
- 3 Different Scheduling Algorithms
- SNMP MIB and IOS CLI Support for both Provisioning and Collecting
- Cisco IOS Optimized Edge Routing (OER) Integration
- Cisco IOS Enhanced Object Tracking (EoT) Integration
- Cisco IOS Embedded Event Manager (EEM) Support
- Cisco Network Management Solution Support

- Cisco Technology Partner 3rd Party Network Management Solution Support

The following IP SLAs operation types are supported Release 12.2(33)SXH for the Catalyst 6500 Series Switch:

- **VoIP Networks**
  - IP SLAs UDP Jitter (+VoIP)
- **UDP and ICMP Operations**
  - IP SLAs UDP Jitter
  - IP SLAs UDP Echo
  - IP SLAs UDP Path Echo
  - IP SLAs ICMP Echo
  - IP SLAs ICMP Path Echo
- **Network Services**
  - IP SLAs HTTP
  - IP SLAs DNS
  - IP SLAs FTP
  - IP SLAs TCP Connect
- **MPLS Networks**
  - IP SLAs LSP Health Monitor

Table 14. Cisco IOS IP SLAs Operations and Applications

Operation Type	Measurement Capability	Key Applications
UDP Jitter	• Round-trip delay, one-way delay, one-way jitter, one-way packet loss • One-way delay requires time synchronization between the Cisco IOS IP SLAs source and target routers	Most common operations for networks that carry voice or video traffic, such as IP backbones
UDP Echo	Round-trip delay	Accurate measurement of response time of UDP traffic
UDP Jitter (VoIP Option)	• Round-trip delay, one-way delay, one-way jitter, one-way packet loss • VoIP codec simulation G.711 ulaw, G.711 alaw, and G.729a • MOS and ICPIF voice quality scoring capability • One-way delay requires time synchronization between the Cisco IOS IP SLAs source and target routers	Useful for VoIP network monitoring
TCP Connect	Connection time	Server and application performance monitoring
Domain Name System (DNS)	DNS lookup time	DNS performance monitoring, troubleshooting
Dynamic Host Configuration Protocol (DHCP)	Round-trip time to get an IP address	Response time to a DHCP server
FTP	Round-trip time to transfer a file	FTP get performance monitoring
HTTP	Round-trip time to get a Web page	Web site performance monitoring
Internet Control Message Protocol (ICMP) Echo	Round-trip delay	Troubleshooting and availability measurement using ICMP ping
ICMP Path Echo	Round-trip delay for the full path	Troubleshooting

LSP Health Monitor	Round-trip response time, Path Trace, and Discovery	Monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

Network Management Solutions

Cisco IOS IP SLAs is widely supported and integrated with many industry-leading performance management applications, which can provide a user friendly graphical interface for configuration, analyzing performance data metrics, and detailed reports over time.

Multiple applications rely on Cisco IOS IP SLAs today for network performance measurements including:

Cisco Integrated Network Management Solutions

- Cisco Works LMS: Internetwork Performance Monitor (IPM)
- IP Solution Center (ISC)
- MPLS Diagnostics Engine (MDE)
- Performance Visibility Manager (PVM)
- Unified Service Monitor (USM)
- Unified Operations Manager (UOM)

Cisco Technology Partner Integrated Network Management Solutions

- NetQoS
- Fluke Networks
- Computer Associates
- InfoVista
- IBM
- Wired City
- SolarWinds

Open Source or Freeware Products

Multi Router Traffic Grapher (MRTG)

Hardware

Routers	Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, CRS-1, 12000, 10000, and 7600 Series Routers
Switches	Cisco 3750-E, 3750, 3560-E, 3560, 3550, 2960, 3750 Metro, ME3400, ME2400, and 6500 Series Switches

Additional Information

http://www.cisco.com/en/US/products/ps6602/products_ios_protocol_group_home.html

Product Management Contact: Ernest Mikulic, ask-ipsla@cisco.com

Please direct any inquiries through your Cisco Account Team or Cisco Solutions Partner.

Service Layer OAM (IEEE 802.1ag Ethernet Connectivity Fault Management)

Ethernet Connectivity Fault Management (CFM) is comprised of the following four categories of messages that work together to help administrators debug Ethernet networks:

- **Continuity check messages:** These are “heartbeat” messages issued periodically by maintenance endpoints. They allow maintenance endpoints to detect loss of service connectivity among themselves. They also allow maintenance endpoints to discover other maintenance endpoints within a domain, and allow maintenance intermediate points to discover maintenance endpoints.
- **Link trace messages:** These are transmitted by a maintenance endpoint on the request of the administrator to track the path (hop-by-hop) to a destination maintenance endpoint. They allow the transmitting node to discover vital connectivity data about the path. Link trace is similar in concept to UDP Traceroute.
- **Loopback messages:** These are transmitted by a maintenance endpoint on the request of the administrator to verify connectivity to a particular maintenance point. Loopback indicates whether the destination is reachable or not; it does not allow hop-by-hop discovery of the path. It is similar in concept to ICMP Echo (Ping).
- **Alarm Indication Signal (AIS) messages:** A part of Y.1731, in general, provide notification to other elements in the network that there is a fault in the Metro Ethernet network. Support AIS messages are planned for a future release of Release 12.2SX.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

Link Layer OAM (IEEE 802.3ah Ethernet Operations, Administration, and Maintenance (OAM)

Link Layer OAM (as specified in IEEE Standard 802.3ah-2004 Clause 57) can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. The frames (OAM Protocol Data Units or OAMPDUs) cannot propagate beyond a single hop within an Ethernet network and have modest bandwidth requirements (frame transmission rate is limited to a maximum of 10 frames per second).

Release 12.2SX includes support for the following functionality:

- **OAM Discovery:** Discovery is the first phase of Link Layer OAM. It identifies the devices at each end of the link along with their OAM capabilities.
- **Link Monitoring:** Link monitoring OAM serves for detecting and indicating link faults under a variety of conditions. Faults in link connectivity that are caused by slowly deteriorating quality are difficult to detect. Link OAM provides a mechanism for an OAM entity to convey these types of failure conditions to its peer via specific flags in the OAMPDUs. It provides statistics on the number of frame errors (or percent of frames that have errors) as well as the number of coding symbol errors.
- **Remote Loopback:** An OAM entity can put its remote peer into loopback mode using the loopback control OAMPDU. In loopback mode, every frame received is transmitted back on the same port (except for OAMPDUs, which are needed to maintain the OAM session). This

helps the administrator ensure the quality of links during installation or when troubleshooting, and can also be used to test SLA requirements such as delay, jitter, and throughput. This feature is asymmetric in that the Service Provider device can put the customer device into loopback mode, but not conversely.

- **Remote Fault Indication (RFI), Dying Gasp:** The failure conditions that can be communicated are a loss of signal in one direction on the link, an unrecoverable error (such as a power failure), or some critical event. Currently, Cisco supports the Dying Gasp generation and can receive the Critical Event and Link Fault.

Release 12.2SX includes support for the following proprietary reason codes:

- Administratively Down
- Error Disabled
- Reload

Reason codes are sent through organization specific OAMPDU frame structure.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

Smart Call Home

Smart Call Home represents a new value proposition for Cisco customers in having the Catalyst 6500 Series Switches send diagnostic information directly to Cisco TAC, this significantly reduces the time to solve minor hardware problems and the RMA cycle. This feature is available to all Cisco Catalyst 6500 Series Switch customers that have a current standard Cisco SMARTNet support contract.

Smart Call Home works by utilizing Generic On-Line Diagnostics (GOLD) and Embedded Event Manager (EEM). GOLD is an online health test that essentially allows the device to check the health of all components in the system. Upon a failure detected by GOLD, an EEM script will collect all required data and a call home message will be sent to a server specified by the network operator.

Smart Call Home provides the capability for a customer to configure call home profiles that define:

- Destination where the Smart Call Home server is, whether it is a server within the customer's network, or a Cisco TAC server
- Transport mechanism such as email or HTTPS
- Events of interest

For example, a customer might configure a profile to allow an individual to be paged at home via short text email when a major diagnostic failure occurs, or syslog events might be sent via HTTPS to a network management station. Another option is to send interested events messages via HTTPS or email to Cisco TAC, and the TAC engineer will be able to access all messages along with the Cisco analysis on the Smart Call Home web application.

Also available on the Smart Call Home web application are reports on the device hardware, software and configuration cross-referenced against any field notices, security alerts, and or end of life notifications specific to the hardware and software on the device.

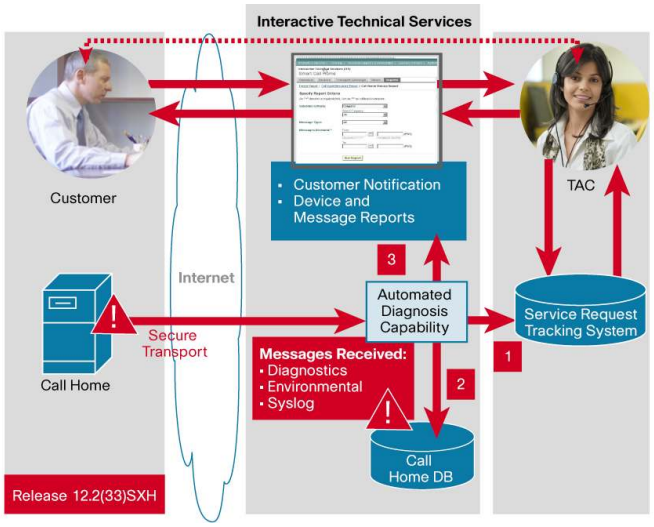
One example of the Call Home is illustrated in the picture below. Any of the diagnostic failure, environmental alarm, or high severity syslog messages can trigger a Call Home message. A default call home profile is then triggered, and appropriate information is gathered. The type of messages that are sent to Cisco TAC is configurable, meaning customers can choose to send only certain portion of the messages to Cisco. If customers choose to send configuration files, then all sensitive information such as passwords will be removed from the configuration file.

The next step is passing these messages into the rules processor that will inspect the message and determine what next steps to take. If the situation is serious enough (module failure or fan failure for example) a service request will be raised direct with the Cisco TAC and routed to the correct team to handle the problem.

If a service request is not raised then the message is stored along with the associated analysis of the problem for a customer or TAC engineer to use as part of their troubleshooting.

Smart Call Home then has the option of proactively notifying the customer of problems which are likely to be emerging issues rather than issues the TAC can deal with (for example high temperature alarms independent of any fan failures or accumulating single bit memory errors).

Figure 24. Smart Call Home Process



Benefits

Significantly reduces the time to solve minor hardware problems and RMA cycle by utilizing GOLD and EEM, sending diagnostic information to Cisco TAC and proactively take care of minor issues before they become disruptive.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Sairaj Pakkam, spakkam@cisco.com

Integrated Security

Identity-Based Network Services (IBNS) Enhancements

Identity-Based Networking Services (IBNS) authenticates and authorizes users and devices to protect against unauthorized access. Using IBNS, the network can determine whether a user is authorized to gain access to the network, and what they have access to. This provides comprehensive identity-based controls for deciding who and what can gain entry to the network.

Release 12.2(33)SXH delivers significant IBNS enhancements. These include:

- 802.1x with VLAN assignment
- 802.1X with Guest VLAN
- 802.1X with Auth Fail VLAN
- 802.1x with Wake-on-LAN
- 802.1x with Voice VLAN
- 802.1x with port security
- 802.1X with PVLAN
- 802.1X with DHCP Snooping
- 802.1X with HA
- 802.1x and Accounting
- 802.1x with Radius-supplied timeout
- 802.1x with Inaccessible Authentication Bypass
- Web Auth
- Web Auth with downloadable ACLs
- MAC authentication Bypass

Benefits

- Flexible authentication methods to support both 802.1x capable and non-capable endpoints
- Flexible policy enforcement options: Provide network administrators the flexibility to apply different types of access controls that fit their deployment scenarios

Hardware

Switches	Catalyst 6500 Series Switches

Product Management Contact: Qiang Huang, qhuang@cisco.com

Wake-on-LAN (WoL)

Wake-on-LAN is an industry initiative that provides a network administrator the ability to “wake up” a powered off PC/host/workstation to boot from the network. It can also be used for such activities as performing unattended system backups and software upgrades on those hosts which are attached to the switch.

With regards the 802.1x configured port, enabling the WoL feature opens up the unidirectional controlled port on the outbound direction prior to 802.1x authentication having occurred. Opening up the port in this unidirectional outbound direction enables a management station to send Wake-on-LAN frames to selected hosts and trigger them to wake/boot, authenticate, and then perform the unattended operation.

Benefits

Flexibility and Security: This feature allows network administrator to offer the flexibility of WoL to remotely activate PC’s without sacrificing the security aspect of 802.1x.

Hardware

Cisco Catalyst 6500 Series Switches

Additional Information:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns75/networking_solutions_sub_solution_home.html

Product Management Contact: Michael Lin, mhelin@cisco.com

AutoSecure

By using a single Command-Line Interface (CLI), the AutoSecure feature allows a user to perform the following functions:

- Disable common IP services that can be exploited for network attacks
- Enable secure access to the switch
- Secure forwarding plane by enabling hardware rate limiters

This feature also simplifies the security configuration of a router and hardens the router configuration.

Benefits

AutoSecure saves security managers considerable times by automatically setting a standard security policy on the switch, thereby quickly bringing the entire network to a security baseline.

Hardware

Switches	Catalyst 6500 Series Switches

Product Management Contact: Qiang Huang, qhuang@cisco.com

Network Admission Control (NAC) Enhancements

The Cisco Self-Defending Network includes the Network Admission Control (NAC) Framework to systematically enforce endpoint policy compliance. The NAC Framework encompasses Cisco switches, routers, access points, VPN appliances, and NAC appliances, enabling flexibility and consistency throughout the network. Cisco switches and wireless access points-typical network entry points for campus employees-become enforcement points by enforcing rights based on the state of the attaching device.

In Release 12.2(33)SXH, two NAC deployment methods are introduced:

- Layer 3 NAC
- IEEE 802.1x based layer 2 NAC

Benefits

Support more NAC framework deployment scenarios

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

To learn more about NAC, visit http://www.cisco.com/go/nac

Product Management Contact: Qiang Huang, qhuang@cisco.com

IP Source Guard

IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, a Port Access Control List (PACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server; any IP traffic with a source IP address other than that in the PACLs permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.

Benefits

IP Source Guard allows the switch to mitigate the IP spoofing attacks at the wiring closet access.

Hardware

Switches	Catalyst 6500 Series Switches

Product Management Contact: Qiang Huang, qhuang@cisco.com

Policy Based Access Control List (PBACL)

This feature eases the management of access-control lists with the use of object-grouping by ensuring that the same object-groups can be used as part of multiple access control lists. Any change in the object group is automatically updated in the access-control lists as well. It allows customers to enable security-policy management by introducing level of abstraction in security policies. It allows the use of group names in ACE instead of IP addresses and protocol port numbers making it easier to manage and be used across multiple access-lists. It does not provide any improvement in the hardware implementation of access-control lists as such.

Benefits

This feature is useful when the customer has typically large access-lists (Internet edge, core and distribution layer) where different networks (or hosts) with similar policies can be grouped together thus allowing easier management and access control.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Muninder Singh Sambi, msambi@cisco.com

Private Hosts

This feature allows the ability to leverage the same VLAN identifier to segment traffic coming from different users on different physical interfaces (configured as 802.1Q Trunks). The Private Hosts feature complements Private VLAN functionality on 802.1Q trunks.

Besides providing traffic segmentation, the ACL-based implementation of the feature protects also from MAC address spoofing threats.

Hardware

Switches	Catalyst 6500 Series Switches

Additional Information

http://www.cisco.com/go/6500

Product Management Contact: Chiara Regale, chiarar@cisco.com

4) RELEASE 12.2SX ADDITIONAL INFORMATION

Cisco IOS Software Information

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

Release 12.2SX Information

- http://www.cisco.com/en/US/products/ps6017/tsd_products_support_series_home.html
- http://www/en/US/products/hw/switches/ps708/prod_bulletin0900aecd804f0694.html

Cisco IOS Software Product Lifecycle Dates & Milestone

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd801eda8a.html

Cisco IOS Software Center

Download Cisco IOS Software releases and access software upgrade planners.

http://www.cisco.com/public/sw-center/

Cisco Software Advisor (Requires Cisco.com Account)

Determine the minimum supported software for platforms.

http://tools.cisco.com/Support/Fusion/FusionHome.do

Cisco Feature Navigator (Requires Cisco.com Account)

A Web-based application that allows you to quickly match Cisco IOS Software releases, features, and hardware.

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS Planner (Requires Cisco.com Account)

View all major releases, all platforms, and all software features from a single interface.

http://www.cisco.com/pcgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

Cisco MIB Locator

MIB Locator finds MIBs in Cisco IOS Software releases.

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Cisco Bug Toolkit (Requires Cisco.com Account)

Search for known bugs based on software version, feature set and keywords.

http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C25-424302-00 8/07

