Product Bulletin No. 3057

Cisco IOS Software Release 12.2(18)SXF New Features and Hardware Support

Last Updated: July 2006

1. CISCO IOS SOFTWARE RELEASE 12.2S 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. The Cisco Catalyst® Switches and high-end routers in Release 12.2S provide secure, converged network services in the most demanding Enterprise and Service Provider environments, from the wiring closet and data center to the WAN aggregation edge.

The infrastructure innovation and technology leadership in Release 12.2S enable advanced Ethernet LAN switching, Metro Ethernet, and Broadband Aggregation services through enhancements in High Availability, Security, MPLS, VPNs, and IP Routing and Services.

Releases 12.2(22)S, 12.2(20)S, 12.2(18)S, and 12.2(14)S are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, refer to Release 12.2S New Features and Hardware Support, Product Bulletin No. 2216.

Derived from Release 12.2(14)S, Release 12.2SX provides Release 12.2S functionality and new features and hardware support for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

In addition to Release 12.2(18)SXD and 12.2(18)SXE, Releases 12.2(17d)SXB, 12.2(17b)SXA, 12.2(17a)SX, and 12.2(14)SX are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, please visit:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletins_list.html

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

1.1 Release 12.2SX Ordering Information, Feature Sets, and Image Names

Refer to the “Feature Sets” section of the Release 12.2SX release notes for information about Release 12.2SX orderable product numbers, feature sets, and image names:
http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a008019e1e9.html

1.2 Additional Information

Cisco IOS Software Release 12.2S
http://www.cisco.com/go/release122s/

Cisco IOS Software Release Feedback and Questions
http://www.cisco.com/warp/public/732/feedback/release/

Release 12.2SX Release Notes
http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

Cisco IOS Software Product Lifecycle Dates and Milestones

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

Cisco IOS Software Center (Please login to Cisco.com before viewing this content)

http://www.cisco.com/kobayashi/library/12.2/index.shtml

2. CISCO IOS PACKAGING IN RELEASE 12.2(18)SXF

Cisco IOS Software is the world's leading network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware support. Currently operating on over ten million active systems, ranging from the small home office router to the core systems of the world's largest service provider networks, Cisco IOS Software is the most widely leveraged network infrastructure software in the world.

Today's users need more flexible and consistent software packaging to address their complex network environments. Cisco is expanding its new Cisco IOS Packaging to Cisco switches via Cisco IOS Software Release 12.2S, creating a new foundation for Cisco IOS Software features and functionality.

For an overview of Cisco IOS Packaging for Cisco switches, including its availability and the associated Cisco IOS Software Release migration strategy, please visit http://www.cisco.com/go/packaging.

3. RELEASE 12.2(18)SXF HARDWARE AND FEATURE HIGHLIGHTS

Cisco IOS Software Release 12.2(18)SXF, the latest customer release of Release 12.2S, adds support for powerful new hardware and software features for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

3.1 Release 12.2(18)SXF Hardware and Feature Highlights

Table 1 and the following sections highlight some of the key hardware and software features available in Release 12.2(18)SXF.

Note: Unless noted otherwise, the following highlighted features were first supported in Release 12.2SX as of Release 12.2(18)SXF. Subsequent releases of Release 12.2SX also support the highlighted features, and might include additional hardware support for the following highlighted features.

Cisco Feature Navigator, which requires an account on Cisco.com, dynamically updates the list of supported hardware as new hardware support is added for the features in the releases of Release 12.2SX. Cisco Feature Navigator can provide a cumulative list of all new and existing features supported in Release 12.2(18)SXF, including hardware and software image support.

Table 1. Release 12.2(18)SXF Hardware and Feature Highlights

Hardware Support	Cisco IOS Security	Cisco IOS Infrastructure	IP Addressing and Services	MPLS and VPNs	IP Multicast
• Cisco 7600 Series SPA Interface Processor 600 • Cisco Catalyst 6500 Series Supervisor Engine 32	• Secure Multicast over GRE with Cisco Catalyst 6500 Series/Cisco 7600 Series IPsec VPN SPA* • Cisco Port Security MIB* • Network Admission Control LAN Port IP* • Per Interface Sticky ARP	• Cisco Catalyst 6500 Series Switch with Cisco IOS Software Modularity**, *** • Cisco IOS Embedded Event Manager 2.1**, *** • Flex Links • EtherChannel Min-Link • Netflow V9 Export Format • Hardware Capacity Monitoring	• 802.1d to PVST+ Bridge Protocol Data Unit (BPDU) Conversion* • IEEE 802.1s—Multiple Spanning Tree (MST) Standard • IP Unnumbered for VLAN-SVI Interfaces • Match Class of Service (CoS) on SIP-400 with GE SPA • Shaped Round Robin (SRR) ***	• P-Bit Transparency* • Hierarchical—Virtual Private LAN Service (H-VPLS) with MPLS Edge • Layer 3 MPLS VPN over GRE	• PIM Snooping DR Flooding Enhancement • Internet Group Management Protocol (IGMP) Static Group Range ***

* This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

** This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF4 with the Supervisor Engine 720.

*** This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF5 with the Supervisor Engine 32.

4.0 HARDWARE SUPPORT

4.1 Cisco 7600 Series SPA Interface Processor 600

Ideal for Service Provider applications, the Cisco 7600 Series SPA Interface Processor 600 (7600-SIP-600) supports up to 10Gbps of bandwidth and a wide range of interfaces. 7600-SIP-600 also provides the unique ability to combine both Layer 2 and Layer 3 services on the same linecard. The combination of native Layer 2 bridging and Layer 3 routing distinguishes this linecard among its peers, particularly in Metro Ethernet applications.

The innovative architecture of this industry leading WAN-services module is designed to deliver cost-effective high-touch features, combining both ASIC and Network Processor technology for an optimal combination of performance and flexibility. The 7600-SIP-600 uses dedicated ASIC technology in the forwarding path (routing/switching, NetFlow, ACLs) as well as for queuing/shaping functions to provide the maximum performance for these foundational features; a programmable network processor is included in the forwarding plane to facilitate flexibility and feature growth. These features are combined with distributed forwarding capabilities that dramatically multiply total system throughput.

7600-SIP-600 initially supports the following SPAs:

Part Number	Description
SPA-OC192POS-LR	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
SPA-OC192POS-XFP	1-port OC-192c/STM-64 POS/RPR SPA, XFP
SPA-OC192POS-VSR	1-port OC-192c/STM-64 POS/RPR SPA, VSR (12.2(18)SXF2)
SPA-1XTENGE-XFP	1-port 10 Gigabit Ethernet SPA, LANPHY SFP Optics
SPA-10X1GE	10-port Gigabit Ethernet SPA, SFP Optics
SPA-5X1GE	5-port Gigabit Ethernet SPA, SFP Optics

Figure 1. Cisco 7600 Series SPA Interface Processor-600 with 10-port Gigabit Ethernet SPA

Benefits

Feature	7600-SIP-600	Benefit
Modularity	One SPA per 7600-SIP-600 module	Offers high performance, dense services while maintaining attractive footprint and scalability
Performance	Up to 25Mpps	Capable of OC192 POS line rate performance with 40 byte IP packets
Packet Memory	256MB	Up to 200ms combined bi-directional buffering
Switch Fabric Connectivity	20Gbps Fabric Channel	Utilizes the 720 Gbps switch fabric for data forwarding capacity
On-Line Insertion and Removal	Supports OIR of the SIP at FCS SPA OIR (post-FCS)	Provides hitless OIR to minimize impact of add/change/remove operations

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Product Management Contact

7600-prod-mgmt@cisco.com

4.2 Cisco 1-port OC-192c/STM-64 POS/RPR Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-600 in Cisco IOS Software Release 12.2(18)SXF. Three optics versions are available:

- **Single Mode, Long Reach**—1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
- **XFP**—1-port OC-192c/STM-64 POS/RPR SPA, XFP
- **Very Short Reach**—1-port OC-192c/STM-64 POS/RPR SPA, VSR (12.2(18)SXF2)

4.3 Cisco 1-port 10 Gigabit Ethernet Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-600 in Cisco IOS Software Release 12.2(18)SXF. LANPHY SFP optics are required.

4.4 Cisco 10-port Gigabit Ethernet Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-600 in Cisco IOS Software Release 12.2(18)SXF. SFP optics are required.

4.5 Cisco 5-port Gigabit Ethernet Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-600 in Cisco IOS Software Release 12.2(18)SXF. SFP optics are required.

4.6 Cisco 1-port OC-48c/STM-16 ATM Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-400 in Cisco IOS Software Release 12.2(18)SXF. SFP optics are required.

4.7 Cisco 2-port Gigabit Ethernet Shared Port Adapter

Supported on the Cisco 7600 Series SPA Interface Processor-400 in Cisco IOS Software Release 12.2(18)SXF. SFP optics are required.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Product Management Contact

7600-prod-mgmt@cisco.com

4.8 Cisco Catalyst 6500 Series PoE, 10/100 Interface Modules

Designed for deployment in wiring closets, high-density Cisco Catalyst 6500 Series 10/100 interface modules provide line-rate 10/100 Ethernet forwarding to the desktop capabilities. These interface modules feature PoE field-installable daughter cards for pay-as-you-grow investment protection and flexibility.

The 96-port 10/100 module (part number WS-X6196-RJ-21) is the industry's first 96-port 10/100 RJ-21 module with IEEE 802.3af support for all 96 ports, helping enable the Cisco Catalyst 6500 Series Switch to deliver the industry's highest port densities ranging from 192 10/100 ports in a Cisco Catalyst 6503 chassis to 1152 10/100 ports in a Cisco Catalyst 6513 chassis for a very cost-effective solution in the wiring closet. With the 802.3af PoE daughter card, this module can support up to 96 Class 2 devices or 62 Class 3 devices per module (960W of PoE per module).

The 96-port 10/100 module (part number WS-X6148X2-RJ-45) is the industry's first 96-port 10/100 RJ-45 module that helps enable the Cisco Catalyst 6500 Series Switch to deliver industry's highest port densities, ranging from 192 10/100 ports in a Cisco Catalyst 6503 chassis to 1152 10/100 ports in a Cisco Catalyst 6513 chassis for a very cost-effective solution in the wiring closet.

The 96-port 10/100 module (part number WS-X6148X2-RJ-45) doubles the port density in the system by allowing it to expand from 48 ports to 96 ports per slot with the addition of a splitter (included), typically mounted at the patch panel. The splitting also can occur at the wall jack, providing another option for doubling the port density of the switch without costly rewiring. This module also can function as a regular 48-port 10/100 module for maximum flexibility and scalability in the future. With the 802.3af PoE daughter card, this module can support up to 48 Class 3 devices per module when operating as a 48-port module, or up to 96 Class 2 devices per module when operating as a 96-port module (960W of PoE per module).

Benefits

Using RJ-21 or RJ-45 connectors, the Cisco Catalyst 6500 Series classic 10/100 modules are ready to be deployed in virtually all wiring-closet environments with the following operational advantages and characteristics:

- **Maximum Port Density per Chassis:**
  - Support up to 1152 10/100 ports or 576 10/100/1000 ports in the Cisco Catalyst 6513 chassis
  - Support up to 768 10/100 ports in the Cisco Catalyst 6509 chassis
  - Support up to 480 10/100 ports in the Cisco Catalyst 6506 chassis
  - Support up to 192 10/100 ports in the small-form-factor Cisco Catalyst 6503 chassis
- **Field-Installable and Upgradable Inline-Power Daughter Cards:** these modules help enable centralized power distribution to IP phones, wireless access points, and other devices by sharing the same Category 5 UTP cabling used for network connections.
- **Forwarding Architecture:** these modules provide centralized Cisco Express Forwarding.
- **Forwarding Performance:** these modules forward packets up to 15 Mpps per system.
- **Fabric Connection:** these modules provide a 32-Gbps shared bus connection.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

These modules work with Supervisor Engine 1A, Supervisor Engine 2, Supervisor 32, or Supervisor Engine 720. These modules can occupy any slot in any Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Router chassis.

Product Management Contact

Sachin Gupta, sagupta@cisco.com

5. CISCO IOS SECURITY

5.1 Secure Multicast over GRE with Cisco Catalyst 6500 Series/Cisco 7600 Series IPsec VPN SPA

Secure multicast over GRE provides a secure and scalable solution to protect multicast traffic in enterprise or managed service provider environment. Each head-end device with the IPsec VPN SPA can support IPsec encrypted multicast traffic for up to 500 remote tunnels. The practical applications include voice/video/data broadcast.

Benefits

- Provides a secure method to transport multicast traffic
- Single box solution simultaneously incorporating GRE encapsulation, IPsec Encryption, and multicast
- Scalable up to 500 remote tunnels

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 32 and Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 32 and Supervisor Engine 720

Considerations

Requires Cisco Catalyst 6500 Series Switch/Cisco 7600 Series Router IPsec VPN SPA and Services SPA Carrier (SSC) module: SPA-IPSEC-2G and 7600-SSC-400.

This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

Additional Information

- http://www.cisco.com/en/US/prod/collateral/routers/ps368/product_data_sheet0900aecd8027c9ee.html
- http://www.cisco.com/en/US/products/ps6267/products_data_sheet0900aecd8027cbb2.html

Product Management Contact

Jay Tsai, jaytsai@cisco.com

5.2 Cisco Port Security MIB

CISCO-PORT-SECURITY-MIB provides SNMP access to configure and retrieve information for port-security. The major areas covered by this MIB include: secure Interface Configuration Table; secure MAC Address Table; and secure VLAN Table.

Benefits

- Allows more flexible management options for port security.

Hardware

Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 32 and Supervisor Engine 720

Considerations

This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

Product Management Contact

Ashish Nagre, ashishcn@cisco.com

5.3 Network Admission Control LAN Port IP

Network Admission Control (NAC) Framework is a foundational component of the Cisco Self-Defending Network strategy, improving the network's ability to automatically identify, prevent, and respond to security threats.

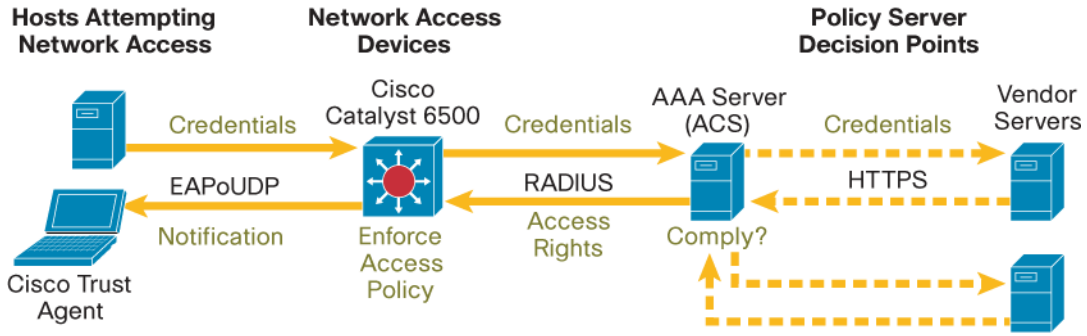
NAC Framework enables the Cisco Catalyst 6500 Series Switches to collaborate with third-party solutions for security-policy compliance and enforcement before a host is permitted to access the network. By deploying NAC framework on the Cisco Catalyst 6500 Series Switches, customers can now restrict non-complaint endpoints that maybe vulnerable or infected with worms, viruses or spyware before they have a chance to enter the Local Area Network (LAN) and potentially infect other enterprise resources.

NAC performs posture validation at the Layer 2 network edge for hosts with or without 802.1x enabled. Vulnerable and noncompliant hosts can be isolated, given reduced network access or directed to remediation servers based on organizational policy. By ensuring that every host complies with security policy, organizations can significantly reduce the damage caused by infected hosts.

Network Admission Control (NAC) LAN Port IP extends NAC support to Layer 2 Ethernet access ports at the network edge. NAC L2 IP is an integral part of Cisco Network Admission Control. It offers the first line of defense for infected hosts connecting to the corporate network. Host device posture validation includes anti-virus state and operating system patch levels. Depending on the corporate access policy and host device posture, a host may be admitted, allowed restricted access, or quarantined to prevent further virus spread across the network.

The device to be validated must be attached to the L2 port within the first Layer 3 hop. LAN Port IP does not require 802.1x support on the hosts. Performing posture validation at the edge maximizes the portion of the network which is protected by the access control, and allows posture validation to be performed within a VLAN. NAC LAN Port IP acts at the same point in the network as the NAC LAN Port 802.1x basic feature, but uses different mechanisms to initiate posture validation, to carry the communication between host and authentication server, and to enforce the resulting access limitations. The posture verification exchange between the supplicant and the switch is over EAPoUDP (Extensible Authentication Protocol over User Datagram Protocol).

Figure 2. Network Admission Control LAN Port IP



Benefits

- **Dramatically Improves Security**—NAC ensures that endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy in order to proactively protect against worms, viruses and spyware.
- **Increases Enterprise Resilience**—NAC provides comprehensive admission control across the LAN to prevent non-compliant and rogue endpoints from impacting network availability.
- **Improve Operational Efficiency**—NAC helps organizations focus operations on prevention, not reaction, reducing OpEx related to identifying and repairing non-compliant, rogue, and infected systems.
- **Extends Existing Investment**—NAC provides broad integration with multivendor security and management software, and extends existing investments in network infrastructure and vendor software. Extends the benefits of NAC to Layer 2 Ethernet Access ports using IP on the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

Additional Information

- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c643/cdccont_0900aecd800fdd58.pdf

Product Management Contact

Ashish Nagre, ashishcn@cisco.com

5.4 Per Interface Sticky Address Resolution Protocol

Currently, Cisco is implementing IP Sticky Address Resolution Protocol (ARP) functionality to prevent hackers or malicious users from spoofing MAC addresses. Sticky ARP entries do not age out, and prevent malicious users from modifying the MAC addresses; however, existing functionality can only be applied to all private VLANs. This enhancement enables users to apply the Sticky ARP functionality to any Layer 3 interface, while allowing the user to overwrite the private VLAN Sticky ARP configuration on a specific interface.

Benefits

This enhancement allows more flexible security options preventing hosts from changing the MAC address of an interface. This is useful for Metro Ethernet Access environments, in which a DSL end station host may attempt to change the MAC address of a Broadband Aggregation Server (BRAS).

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Product Management Contact

Sachin Gupta, sagupta@cisco.com

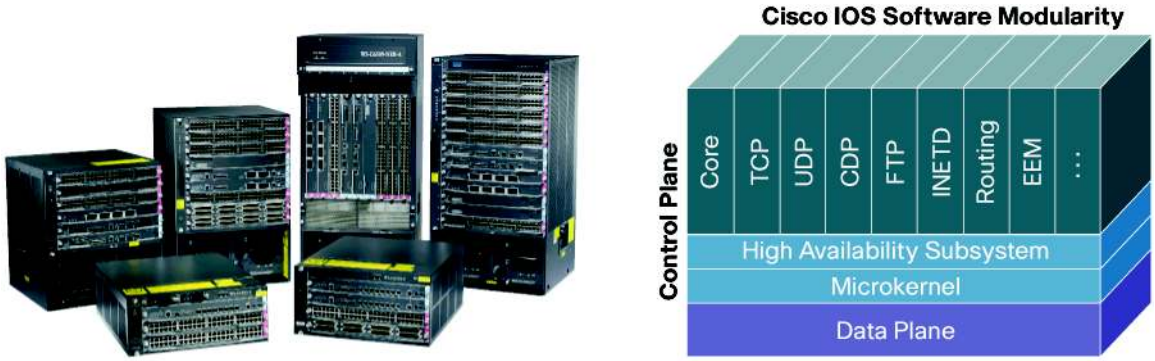
6. CISCO IOS INFRASTRUCTURE

6.1 Cisco Catalyst 6500 Series Switch with Cisco IOS Software Modularity

Cisco Catalyst 6500 Series Switch with Cisco IOS Software Modularity boosts operational efficiency and minimizes downtime through evolutionary software infrastructure advancements. By enabling modular Cisco IOS Software subsystems to run as independent processes, this innovation:

- Minimizes unplanned downtime through self-healing processes
- Simplifies software changes through subsystem In-Service Software Upgrades (ISSU)
- Enables process-level, automated policy control by integrating Embedded Event Manager (EEM)

Figure 3. Cisco Catalyst 6500 Series Switch with Cisco IOS Software Modularity



The Cisco Catalyst 6500 Series Switch delivers hardware based forwarding through ASICs (Application Specific Integrated Circuits) on a central Policy Feature Card (PFC) or Distributed Forwarding Cards (DFC). The control plane functions on the Cisco Catalyst 6500 Series Switch run on dedicated CPUs on the Multilayer Switch Forwarding Card (MSFC) complex.

- **Control Plane**—Handles control traffic such as routing protocol updates and management traffic
- **Data Plane**—Responsible for the actual forwarding of packets using ASICs

A completely separate data plane ensures that traffic forwarding continues even if there is a disruption in the control plane, as long as the software is intelligent enough to program the hardware for non-stop operation. With Supervisor Engine redundancy, the Non-Stop Forwarding (NSF) and Stateful Switchover (SSO) features available on the Cisco Catalyst 6500 Series Switch provide a continuous data plane even in the event of a hardware failure on the active Supervisor.

Cisco IOS Software Modularity combines subsystems into individual processes and enhances the Cisco IOS Software memory architecture in order to provide process level fault isolation and subsystem ISSU capability. These enhancements are delivered on Cisco IOS Software for the Cisco Catalyst 6500 Series Switch Supervisor Engine 720 and Supervisor Engine 32, maintaining the feature richness and operational environment that network operators are familiar with.

Benefits

- **Operational Consistency**—While Software Modularity adds many enhancements to Cisco IOS Software on the Cisco Catalyst 6500 Series Switch, no changes from an operational point of view are necessary. Command Line Interface (CLI) as well as management interface related interfaces such as SNMP or SYSLOG are the same as before. New commands to exec and configuration mode as well as show commands have been added to support the new functionality. Software releases and rebuilds are the same as before with additional support for patching.
- **Protected Memory**—Software Modularity enables a memory architecture where processes make use of a protected address space. Each process and its associated subsystems “live” in an individual memory space. Using this paradigm, memory corruption across process boundaries becomes virtually impossible.
- **Fault Containment**—The benefit of protected memory space is increased availability since problems occurring in one process can not affect other parts of the system. For example, if a less critical system process fails or is not operating as expected, critical functions required to maintain packet forwarding are not affected.
- **Process Restartability**—Building on the protected memory space and fault containment, the modular processes are now individually restartable. For test purposes or non-responding processes, a new CLI command is provided to manually restart processes. This allows fast recovery from transient errors without the need to disrupt forwarding. An integrated high availability subsystem constantly checks the state of processes and keeps track of how many times a process restarted in a defined time interval. In the event a process restart does not restore the system, the high availability subsystem will take more drastic actions such as initiating a Supervisor Engine switchover or a system restart.

- **Modularized Processes**—Several control plane functions have been modularized to cover the most commonly used features. Examples of modular processes include but are not limited to:
  - Routing process
  - Internet Daemon
  - Raw IP processing
  - TCP process
  - UDP process
  - CDP process
  - SYSLOG Daemon
  - Any EEM components
  - IP File System Daemon
  - File system drivers
  - Install Manager
- **Subsystem ISSU**—The most important benefit of the protected memory space and process restartability is the ability to make changes to software during runtime. Cisco IOS Software Modularity enhances the Cisco IOS Software infrastructure to allow selective system maintenance through individual patches (a patch is a single update that can affect one or multiple subsystems). By providing versioning and patch management capabilities, patches can be downloaded, verified, installed and activated without the need to restart the system. Since packet forwarding is not affected during the patch process, the network operator now has the flexibility to introduce software changes at any time. A patch only affects the components required for the update, which means that a network administrator now only has to re-certify the portion of the software associated with the update.

Hardware

Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

This functionality is available on the Supervisor Engine 720 beginning in Cisco IOS Software Release 12.2(18)SXF4. This functionality is available on the Supervisor Engine 32 beginning in Cisco IOS Software Release 12.2(18)SXF5.

Additional Information

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

Product Management Contacts

- Sanjb HomChaudhuri, sanjib@cisco.com
- Sachin Gupta, sagupta@cisco.com
- Siva Valliappan, svalliap@cisco.com

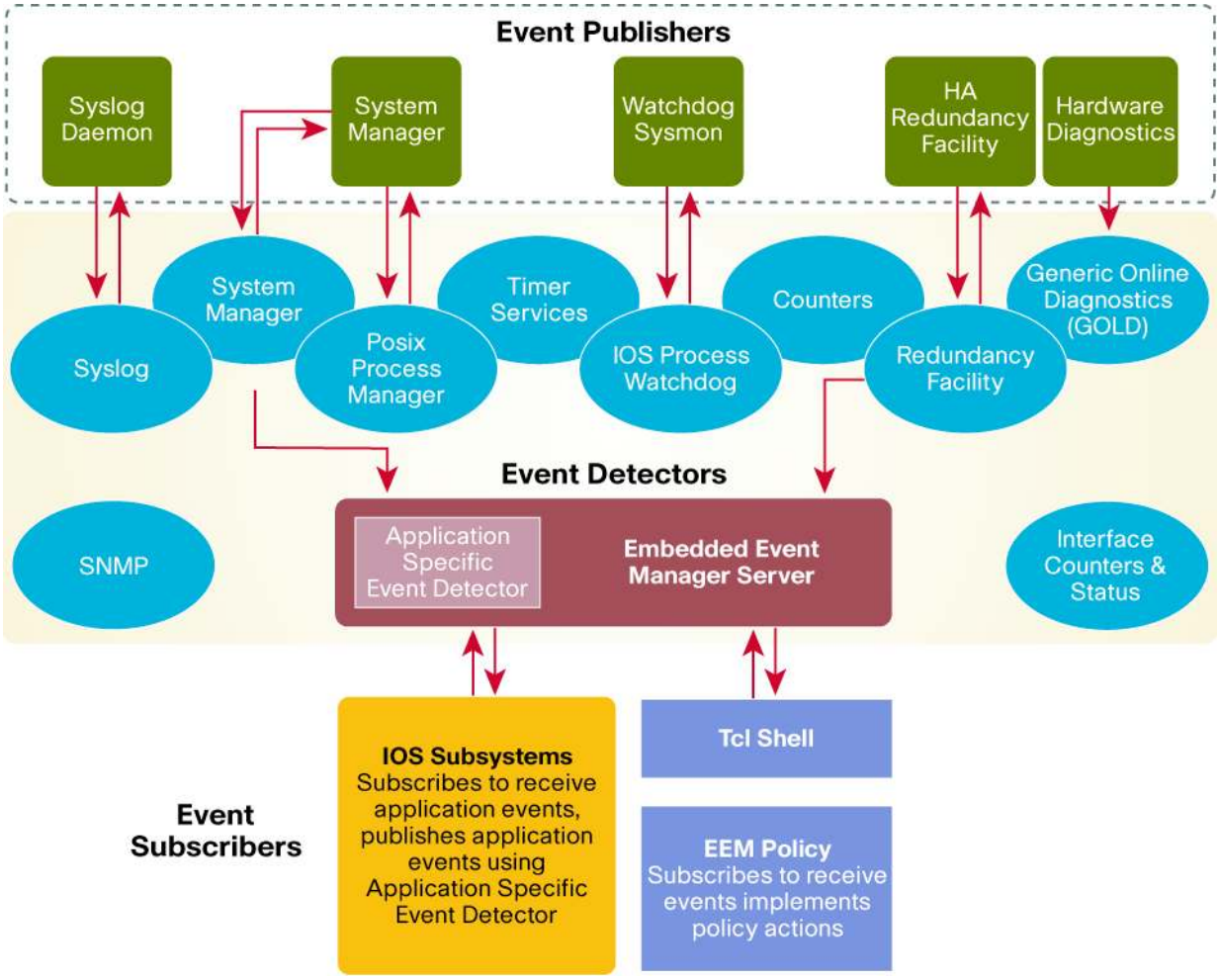
6.2 Cisco IOS Embedded Event Manager 2.1

Cisco IOS Embedded Event Manager (EEM) 2.1 supports a flexible, policy driven framework that supports in-box monitoring of different components of the system with the help of software agents known as event detectors. Event detectors notify the EEM when an event of interest occurs. The EEM policies (configured via CLI or TCL scripting interface) define automatic actions to be taken based on the current state of the system and on the policy specified for the given event. An extendible EEM framework allows new event detectors to be added as needed.

The goal of Cisco IOS Embedded Event Manager 2.1 is to significantly enrich the embedded event management framework in Cisco IOS Software by building on top of EEM 1.0 and adding TCL based event management policy authoring capabilities. EEM 2.1 will also provide a number of additional event detectors and policy action supporting advance monitoring, high availability and serviceability capabilities.

Cisco IOS Embedded Event Manager 2.1 provides a leadership feature to users in the areas of on-device event detection/recovery and supports enhanced ability to identify and correct anomalies within user networks. The users can incorporate consistent logical fault management policies across Cisco IOS Software based products in their networks. Furthermore, the ability to define event management policies reduces operator errors, and establishes rule sets for root- cause analysis. Cisco IOS Embedded Event Manager 2.1 enables a distributed, scalable, and customizable approach to event management (detection, recovery, and automated actions) directly in a Cisco IOS Software device.

Figure 4. EEM 2.1 Block Diagram



Benefits

- Leverage intelligence of Cisco IOS Software
- Enhanced event management and monitoring capabilities through the use of event detectors
- Increased network availability and serviceability through integration with network policy rule sets

- Increased management scalability with integrated event detectors and automated policy actions
- EEM 2.1 provides autonomous scripting capabilities in Cisco IOS Software without requiring the use of an NMS application

Hardware

Routers	Cisco 7600 Series Routers, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

EEM 2.1 is supported in Cisco IOS Software Release 12.2(18)SXF4 for Cisco IOS Modularity for the Cisco 6500 only. Support for EEM 2.1 in Cisco IOS Software images not containing Cisco IOS Modularity is available in Cisco IOS Software Release 12.2(18)SXF5 for both the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

Additional Information

- http://www.cisco.com/en/US/products/ps6017/products_feature_guides_list.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/122sxf18/index.htm

Product Management Contact

Rick Williams, rwill@cisco.com

6.3 Flex Links

Flex Links are a pair of a Layer 2 interfaces (switchports or port channels), in which one interface is configured to act as a backup for the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP), enabling users to turn off STP without sacrificing basic link redundancy. Flex Links are typically configured in service provider or enterprise networks, in which customers do not need to run STP on the switch. If the system is running STP, it is not necessary to configure Flex Links because STP already provides link-level redundancy or backup.

A Flex Link is configured for one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Link or backup link. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the linkup state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Link interfaces.

Benefits

- Flex Links provide fast convergence, with failover in less than three seconds.
- It allows users to configure one of the switchport interfaces to backup another switchport interface for increased network fault tolerance and backup capabilities.
- Eliminates the need for STP.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Product Management Contact

- Sachin Gupta, sagupta@cisco.com
- 7600-prod-mgmt@cisco.com

6.4 EtherChannel Min-Link

This feature allows the user to set a minimum threshold for the number of links in an EtherChannel such that if less than the specified number of links is available, the port channel interface fails over to a standby EtherChannel.

Benefits

Allows greater configuration granularity, so network administrators can declare when a given EtherChannel is available.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Product Management Contact

- Jeevak Bhatia, jeevak@cisco.com
- Sachin Gupta, sagupta@cisco.com

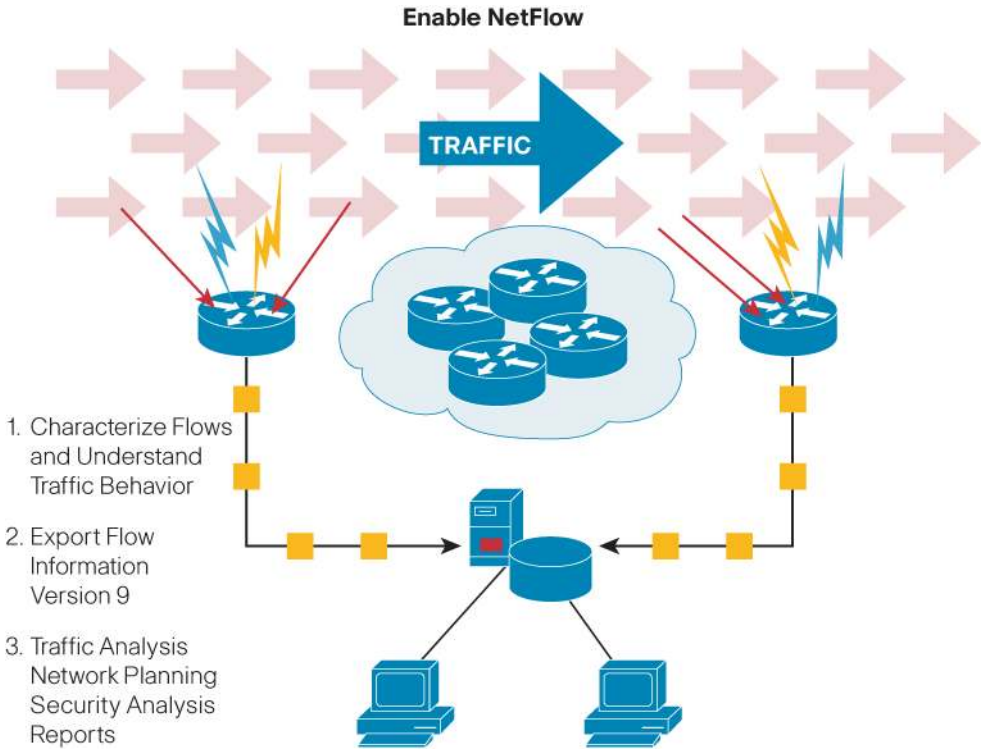
6.5 NetFlow Version 9 Export Format

IP network managers must understand who is using the network and for how long, what protocols and applications users employ, and where the network data flows. IP network managers rely on exported NetFlow data for a variety of purposes, including understanding network telemetry and planning, security monitoring, enterprise accounting, and departmental charge backs, Internet service provider billing, data warehousing, and data mining for marketing purposes.

NetFlow Version 9 is a new flexible and extensible format for exporting IP flow information from Cisco routers and switches, providing rapid support for IP accounting of Cisco technologies. NetFlow version 9 allows support for NetFlow Multicast Ingress and Egress Accounting. The NetFlow version 9 extensible format is being recognized as a new standard for exporting flow information from IP devices and NetFlow version 9 is the basis of the IETF IP Flow information export (IPFIX) working group standard.

When a company is using multicast streaming multimedia to broadcast an event, it is essential to track which users participate, and for how long. Multicast NetFlow is now available to provide information on the utilization of multicast traffic, how much traffic is being propagated and who is utilizing the network.

Figure 5. NetFlow Version 9 Export Format



Benefits

- Provides enhanced management capabilities for NetFlow supported technologies (ie: Multicast, MPLS, NAT, and BGP).
- Minimizes changes to third-party NetFlow application developers.
- Enables network administrators to understand multicast traffic patterns and identify users.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Additional Information

http://www.cisco.com/en/US/products/ps6645/products_ios_protocol_option_home.html

Product Management Contact

- Sachin Gupta, sagupta@cisco.com
- Tom Zingale, tomz@cisco.com

6.6 Hardware Capacity Monitoring

This functionality adds the ability to do Hardware Capacity Monitoring via a “show platform hardware capacity” CLI for the user to get a single, integrated summary of system hardware capacity and utilization information. The command includes a list of the currently available hardware resources, including the utilization of the hardware, forwarding tables, the switch fabric, the CPU(s), and the various memory devices (ie: Flash, DRAM, NVRAM).

The intended user of the show command would be a network engineer or network architect for use in capacity planning. The output of the command can be used to compare the current hardware utilizations to the maximum hardware capacities so that the user can make informed network design decisions based on the product's usage. This command can also be helpful in initial troubleshooting efforts.

Benefits

- Enhanced manageability for hardware.
- Increased troubleshooting and diagnostic capabilities based upon hardware utilization.
- Better network capacity planning based upon hardware utilization.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Product Management Contact

- Sachin Gupta, sagupta@cisco.com
- Jeff Raymond, jeraymon@cisco.com

7. IP ADDRESSING AND SERVICES

7.1 802.1d to PVST+ Bridge Protocol Data Unit (BPDU) Conversion

The 802.1d to PVST+ (Per VLAN Spanning Tree) BPDU Conversion functionality allows for interoperability between 802.1d Spanning Tree BPDUs and PVST+ BPDUs on an ATM interface. This allows the Cisco 7600 Series Router, using PVST+, to participate in the Spanning Tree of switching devices, either Cisco or non-Cisco, that are only able to use 802.1d STP. As a result of this functionality, the network can be extended across switches using either the 802.1d or PVST+ standard and there is investment protection for users purchasing the newer Cisco 7600 Series Router but having devices which only support the 802.1d standard.

Figure 6. 802.1d to PVST+ Bridge Protocol Data Unit (BPDU) Conversion

Benefits

- Allows interoperability between PVST+ and 802.1d switching devices
- Provides investment protection for switching devices only supporting 802.1d

Hardware

Routers	Cisco 7600 Series Router
Switches	Cisco Catalyst 6500 Series Switch

Considerations

The following supervisors are supported: Sup720-3B, sup720-3BXL and Sup32-3B (both 8x1GE and 2x10GE).

The following Line cards are supported: OSM-2OC12-ATM, WS-X6582-2PA, and 7600-SIP-200.

This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

Product Management Contacts

- Ram Haridasa, ramh@cisco.com
- 7600-prod-mgmt@cisco.com

7.2 IEEE 802.1s—Multiple Spanning Tree Standard

Multiple Spanning Tree (MST) is the IEEE 802.1s and is an amendment to 802.1Q. It extends the 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides for both rapid convergence and load balancing in a VLAN environment. The MST protocol is compliant with IEEE 802.1s and is backward compatible with 802.1D STP, 802.1w, the Rapid Spanning Tree Protocol (RSTP), and the Cisco PVST+ architecture that was implemented in previous software releases.

MST allows users to build multiple spanning trees over VLAN trunks and enables them to group and associate VLANs to spanning-tree instances. Each instance can have a topology that is independent of other spanning-tree instances, and each instance can have a different port instance cost and port instance priority. This architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, the existence of different VLAN spanning-tree instance assignments in disparate parts of the network eases the administrative burden and optimizes redundant path utilization. However, a spanning-tree instance can exist only on bridges that have compatible VLAN instance assignments. MST requires that users configure a set of bridges with the same MST configuration information, which allows them to participate in a given set of spanning-tree instances. Interconnected bridges that have the same MST configuration are referred to as an MST region.

Benefits

- Ability to configure multiple spanning trees and group VLANs to a particular tree instance.
- Fast convergence times to minimize the loss of connectivity during link failures.
- Load balancing through the use of alternative paths through the network.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Product Management Contact

Sachin Gupta, sagupta@cisco.com

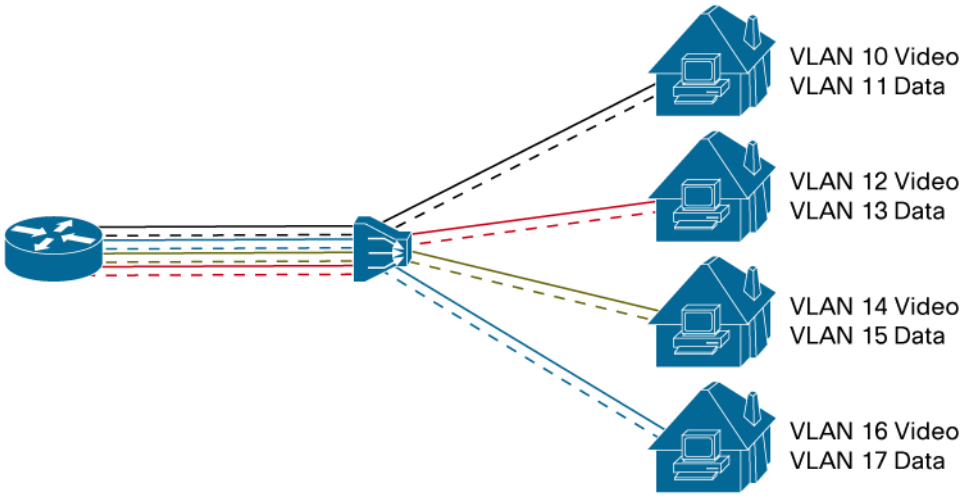
7.3 IP Unnumbered for VLAN-SVI Interfaces

This functionality allows the use of IP unnumbered interface support on the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router. This is useful when it is necessary to enable IP processing on an interface without assigning an explicit IP address to the interface. For Broadband Service Providers looking to migrate ATM DSLAMs to Gigabit Ethernet (GE) uplink DSLAMs, IP Unnumbered support on switches aggregating Ethernet DSLAMs is important for the following reasons:

- Allows better utilization of Dynamic Host Configuration Protocol (DHCP) pools across multiple interfaces.
- Allows for DHCP to delegate different address ranges in the same subnet in support of different applications such as Set Top Boxes that may require a private IP address and Internet Access where a public address is required, even though both devices reside on the same VLAN.
- Allow for easier configuration of aggregation switches, especially on smaller Ethernet switches where each interface may be dedicated to a subscriber.

The IP unnumbered support is offered on VLAN acting as Switched Virtual Interfaces (SVIs) for the aggregation of VLANs from subscriber devices. The IP unnumbered capability will simplify the task of assigning addresses to broadband subscribers.

Figure 7. IP Unnumbered on Router Aggregating VLAN Per Subscriber Service



Benefits

- Simplifies configuration of IP interfaces by not requiring the assignment of a specific IP address.
- Allows better use of DHCP for Broadband Aggregation environments.
- Simplifies the configuration of Aggregation switches in Ethernet DSLAM environments.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Product Management Contact

Chetan Khetani, cpk@cisco.com

8. MULTIPROTOCOL LABEL SWITCHING AND VPNS

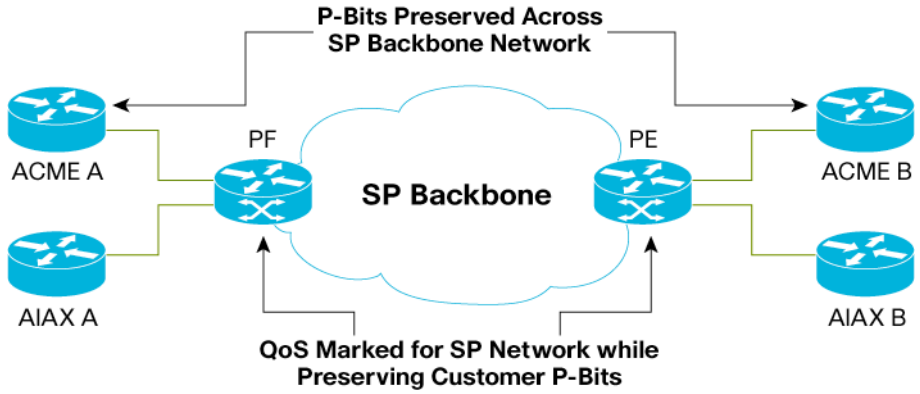
8.1 P-Bit Transparency

P-Bit Transparency enables Service Providers to offer Transparent LAN Services (TLS) with end user and Service Provider controllable Quality of Service (QoS). TLS services such as Virtual Private LAN Services (VPLS) or Ethernet over MPLS (EoMPLS), enable end-users to virtually extend their LANs across Service Provider networks. Now Class of Service (COS) P-Bit markings can be preserved across these core networks while still permitting the Service Provider to remark the traffic for appropriate QoS treatment across the network core.

For example, if a Service Provider were to offer both video (residential) services and TLS (commercial) services across the same physical network, the two traffic types would compete for shared resources (bandwidth). No matter what else may occur in the network, video traffic must have priority over any other data flows. Since the TLS service, based on Virtual Private LAN Services (VPLS), is a Layer 2 service, the commercial customer expects to use the P-Bits within the VLAN tag to implement their specific QoS policy between remote sites. Previously, the customer-specific QoS marking would be lost as the Service Provider would remark all non-video traffic at a lower precedent.

With this new functionality, the original TLS customer's P-Bits will copy into EXP bits of the VC-label which is the inner tag of the VPLS MPLS encapsulation. The Service Provider's transport QoS will be copied into the tunnel label of the VPLS MPLS encapsulation. Upon exiting the ingress PE device, the TLS traffic will flow along with residential video traffic inside the Service Provider's MPLS backbone. The traffic will be MPLS forwarded until it reaches the egress PE device which will de-encapsulate the traffic and preserve the QoS P-Bits of the VPLS customer.

Figure 8. P-Bit Transparency



Benefits

- Allows preservation of P-Bits QoS marking when using a Transparent LAN Service Such as VPLS
- Useful for Video/Voice and Data applications requiring different QoS classes for each traffic type

Hardware

Routers	Cisco 7600 Series Router with OSM-GE-WAN+, Supervisor Engine 720-3B and Supervisor Engine 720-3BXL
Switches	Cisco Catalyst 6500 Series Switch with OSM-GE-WAN+ and Supervisor Engine 720-3B and Supervisor Engine 720-3BXL

Considerations

This functionality is available beginning in Cisco IOS Software Release 12.2(18)SXF2.

Product Management Contact

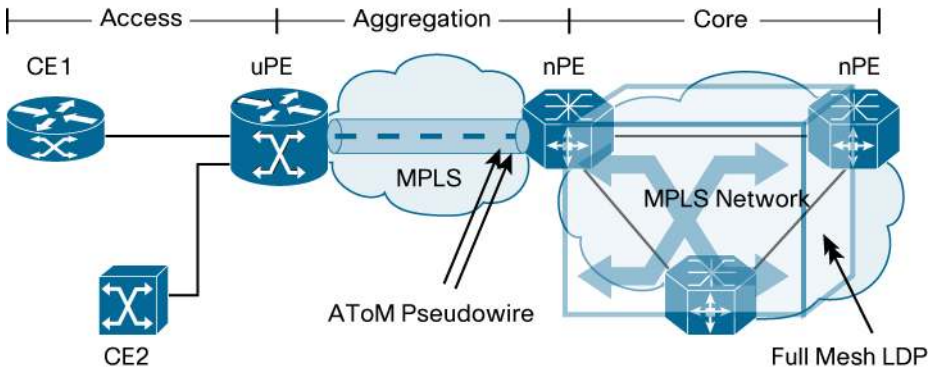
7600-prod-mgmt@cisco.com

8.2 Hierarchical-Virtual Private LAN Service (H-VPLS) with MPLS Edge

Applicable to Service Providers looking to deploy integrated L2 and L3 services using a common access architecture, a traditional VPLS offering requires a full mesh among the Provider Edges (PEs) participating in the multipoint Transparent LAN Service (TLS) instance. This requirement may cause the cost of a PE node to be high as it is required to handle many PseudoWires. Detailed in VPLS draft draft-ietf-l2vpn-vpls-ldp-03.txt, Hierarchical VPLS reduces the VPLS full mesh requirement into manageable domains with high capacity nodes needed only where the full mesh needs to be implemented. This feature also goes by the name of “Hub and Spoke VPLS”, as the PEs which do not implement full mesh are called “Spokes” and the “Hub” provides the bridging function among the spokes.

In addition, H-VPLS with MPLS Edge goes beyond traditional QinQ access by enabling MPLS in the access networks thereby using a single control plane in Access and Core networks and the removal of spanning tree in the access to provide resiliency. Support for the ability to disable split horizon on a per neighbor basis will be provided. This feature will complement the VPLS offerings of Cisco and will be used in situations where MPLS to the edge is a desired deployment model.

Figure 9. H-VPLS with user PE (uPE) and network PE (nPE). Full Mesh VPLS Connectivity is Limited to only the Core Network



Benefits

- Simplified L2 and L3 access networks for Service Provider offered multipoint transparent LAN services (TLS).
- Ability to integrate with MPLS network.
- Improved scalability due to tiered hierarchical approach compared to VPLS.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

Supported on OSM-2+4GE-WAN+ and 7600-SIP-600.

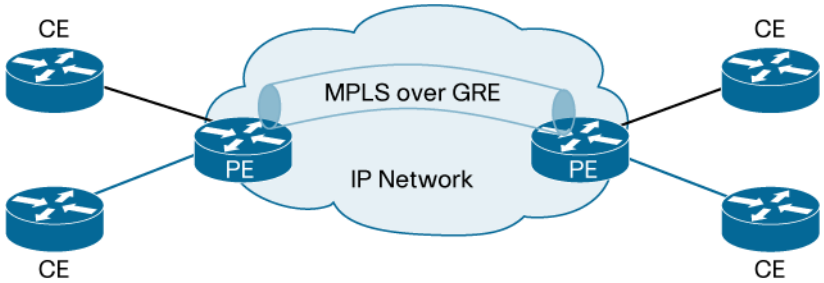
Product Management Contact

- Ram Haridasa, ramh@cisco.com
- Sachin Gupta, sagupta@cisco.com
- Neil Abogado, nabog@cisco.com
- 7600-prod-mgmt@cisco.com

8.3 Layer 3 MPLS VPN over GRE

Layer 3 MPLS VPN over GRE provides a mechanism to transport MPLS packets over a non-MPLS network. While MPLS networks are wide spread, there are still a large number of enterprise and service provider networks requiring the ability to send MPLS traffic over IP networks. For those customers, Layer 3 MPLS VPN over GRE is a bridge allowing integration of both MPLS and IP networks and will work from PE to PE in a point to point topology. This functionality will allow hardware switching on the Cisco 7600 Series Router for Layer 3 MPLS VPN over GRE traffic.

Figure 10. Layer 3 MPLS VPN over GRE



Benefits

Allows L3 MPLS VPN traffic to be sent over an IP network.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

Requires 7600-SIP-400.

Product Management Contact

7600-prod-mgmt@cisco.com

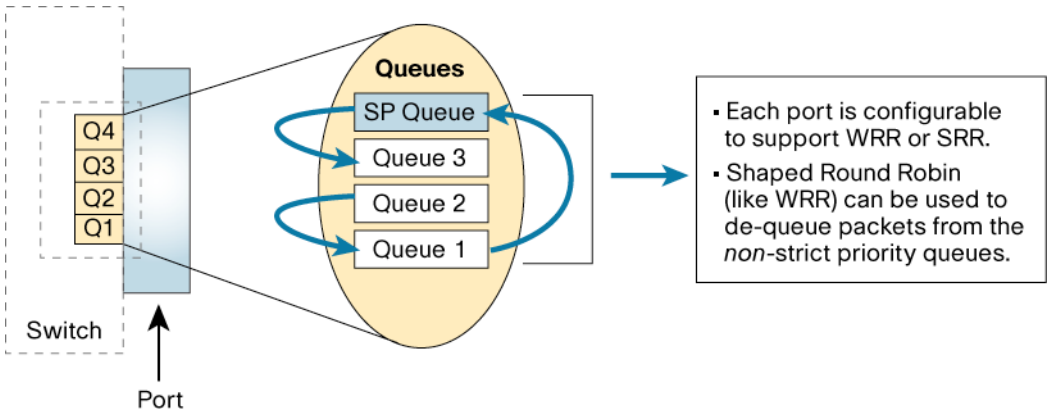
8.4 Shaped Round Robin

Description

This feature introduces support for a new scheduling mechanism, Shaped Round Robin (SRR), to de-queue packets from an egress port queue on a switch. With SRR, each queue on an egress port gets a “share” which translates into a fraction of the output time this queue can send data. Each “share” per queue value is a 16-bit value. For the Gigabit Ethernet (GE) port this translates into a rate of 16Kbs to 1Gbs for each queue.

The SRR solution provides a way to shape outbound traffic to a stated rate. It is similar to policer except that traffic in excess of the rate will be buffered rather than dropped as with a policer. The shaper is implemented on a per-queue basis and has the effect of smoothing transient bursts of data that pass through the port.

Figure 11. SRR on egress port of switch with Strict Priority (SP). Weighted Round Robin (WRR) can alternatively be configured on port.



Benefits

- **Efficient Bandwidth Utilization**—Per queue shaping allows very granular control of bandwidth allocation and results in more efficient bandwidth utilization.
- **Reduced Network Congestion**—Buffering transient bursts of data on switch ports helps to reduce overall network congestion levels.

Hardware

Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 32

Considerations

This feature is only available on uplinks of the Supervisor Engine 32 with Cisco IOS Software Release 12.2(18)SXF5.

Product Management Contact

Sairaj Pakkam, spakkam@cisco.com

Jeff Raymond, jeraymon@cisco.com

9. IP MULTICAST

9.1 PIM Snooping DR Flooding Enhancement

In networks where a Layer 2 switch interconnects several routers, such as an Internet exchange point (IXP), the switch floods IP multicast packets on all multicast router ports by default, even if there are no multicast receivers downstream. With Protocol Independent Multicast (PIM) snooping enabled, the switch restricts multicast packets for each IP multicast group to only those multicast router ports that have downstream receivers joined to that group. When users enable PIM snooping, the switch learns which multicast router ports need to receive the multicast traffic within a specific VLAN by listening to the PIM hello messages, PIM join and prune messages, and bidirectional PIM designated forwarder-election messages.

This feature enhances PIM Snooping by allowing the user to configure whether a multicast stream will go to the Designated Router (DR) for that segment. This is useful in environments where there are multiple source multicast streams that need to be load balanced across routers on a network segment. This enhancement will prevent Designated Router (DR) flooding of multicast traffic when the PIM-Snooping feature is enabled.

Benefits

- Prevents Designated Router (DR) flooding with PIM Snooping.
- Allows load balancing of multicast streams across multiple routers.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Product Management Contact

- Sachin Gupta, sagupta@cisco.com
- Gurvinder Singh, g-singh@cisco.com

9.2 Match Class of Service (CoS) on SIP-400 with GE SPA

This functionality supports the QoS policy ‘match cos’ classification to be applied on the 7600-SIP-400 with the GE SPA. When .1Q encapsulation is configured on the 7600-SIP-400 with GE SPA, the CoS bits in the VLAN tag can be used to differentiate the packet priority and a QoS service policy can be applied to the interface.

Benefits

Allows further configuration granularity by allowing ‘match cos’ to be used on 7600-SIP-400.

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720 and Supervisor Engine 32
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720 and Supervisor Engine 32

Considerations

Requires 7600-SIP-400.

Product Management Contact

Kamlesh Shah, kshah@cisco.com

9.3 Catalyst 6500 Supervisor Engine 32

The Cisco Catalyst 6500 Supervisor Engine 32 delivers industry-leading security, availability, and manageability services for enterprise networks.

This supervisor is ideal for enterprise LAN access that requires maximum uptime and security. Supervisor Engine 32 provides investment protection for current Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router deployments by supporting all existing classic and CEF256 based modules and enabling new applications.

Based on the industry-leading Cisco Catalyst 6500 Series Supervisor Engine 720 technology, the Cisco Catalyst 6500 Series Supervisor Engine 32 allows customers to cost-effectively enable hardware-based security features, such as Denial of Service (DoS) mitigation to protect network application performance, and scalable support for multicast applications at the network edge.

Two uplink options are available: 8-port Gigabit Ethernet Small Form Pluggable (SFP)-based uplinks and 2-port 10-Gigabit Ethernet XENPAK-based uplinks.

Figure 12. Supervisor Engine 32 with 8 Gigabit Ethernet Uplinks

Figure 13. Supervisor Engine 32 with two 10 Gigabit Ethernet Uplinks

Benefits

- Extends Cisco Catalyst 6500 Series Supervisor Engine 720 level of advanced services into the access layer through the Policy Feature Card 3B (PFC3B). Supervisor 32 in conjunction with Supervisor 720 provides an end to end Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Router solution for customers looking to simplify their network operations and management through feature consistency.
- Provides industry leading integrated security through support of HW-based rate limiters, port based access lists, and other authentication and threat defense features.
- Ensures business continuity through support of sub-second Layer 2 stateful switchover, gateway load-balancing protocols, and proactive detection and prevention of network equipment failures using Generic Online Diagnostics (GOLD).

Hardware

Routers	Cisco 7600 Series Router, Supervisor Engine 720
Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 720

Additional Information

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd801ff3ee.html

Product Management Contact

Sachin Gupta, sagupta@cisco.com

9.4 Internet Group Membership Protocol Static Group Range

Description

The Internet Group Membership Protocol (IGMP) Static Group Range command allows the user to configure multiple IGMP groups using a range command; this avoids having to configure Command Line Interface (CLI) for each group and simplifies the task of configuring Cisco IOS Multicast.

This functionality is useful when a Cisco switch needs to act as a receiver of multicast content for a large number of multicast endpoints. In this scenario, a multicast receiver, configured through CLI and the IGMP static group command, needs to be established for each endpoint. When there are a large number of endpoints, this process results in a long configuration. The IGMP Static Group Range support simplifies this task to allow easier configuration with fewer manual errors using a CLI with a range command to configure multiple groups.

Benefits

Simplified Multicast Configuration—The IGMP Static Group Range command simplifies configuration by allowing multiple multicast groups to be configured with a range command.

Hardware

Switches	Cisco Catalyst 6500 Series Switch, Supervisor Engine 32

Considerations

This feature requires Cisco IOS Software Release 12.2(18)SXF5.

Product Management Contact

Tom Zingale, tomz@cisco.com

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA 206634.BO_ETMG_PI_06/06