EPRODUCT BULLETIN, NO. 2368

CISCO IOS SOFTWARE RELEASE 12.2(17B)SXA FOR CISCO CATALYST 6500 SERIES SWITCHES AND CISCO 7600 SERIES ROUTERS EQUIPPED WITH THE CISCO SUPERVISOR ENGINE 720

HARDWARE FEATURES

Cisco IOS® Software Release 12.2(17b)SXA maintains support for all modules in Cisco IOS Software Release 12.2(17a)SX. Cisco IOS Software Release 12.2(17b)SXA incorporates support for new hardware, listed in Table 1.

Table 1. New Hardware Supported with the Supervisor Engine 720 in Cisco IOS Software Release 12.2(17b)SXA

Hardware	Description
WS-SUP720-3BXL	Supervisor Engine 720 PFC3BXL for the Cisco® Catalyst® 6500 Series and Cisco 7600 Series
WS-F6K-PFC3BXL	Policy Feature Card-3BXL for Supervisor Engine 720 on the Cisco Catalyst 6500 and Cisco 7600
WS-X6582-2PA	Enhanced Fabric-Enabled FlexWAN
PA-POS-2OC3	2-port Packet over SONET OC-3c/STM-1 Port Adapter

Cisco IOS Software Release 12.2(17b)SXA resumes support for the following line card modules previously supported in Cisco IOS Software Release train 12.1E, listed in Table 2.

Table 2. Supported with the Supervisor Engine 720 in Cisco IOS Software Release 12.2(17b)SXA

Hardware	Description
OSM-2+4GE-WAN+	Enhanced Optical Service Module (OSM) with 4 GE WAN ports and 2 GE LAN ports
OSM-4GE-WAN-GBIC	4-port GE OSM, GIBC
OSM-4OC3-POS-SI+	Enhanced 4-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-8OC3-POS-SI+	Enhanced 8-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-8OC3-POS-SL+	Enhanced 8-port OC-3/STM-1 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-16OC3-POS-SI+	Enhanced 16-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-4OC3-POS-SI	4-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-8OC3-POS-SI	8-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-8OC3-POS-SL	8-port OC-3/STM-1 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-8OC3-POS-MM	8-port OC-3/STM-1 SONET/SDH OSM, Multimode, with 4 GE
OSM-16OC3-POS-SI	16-port OC-3/STM-1 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-16OC3-POS-SL	16-port OC-3/STM-1 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-16OC3-POS-MM	16-port OC-3/STM-1 SONET/SDH OSM, Multimode, with 4 GE
OSM-2OC12-POS-SI+	Enhanced 2-port OC-12/STM-4 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-2OC12-POS-MM+	Enhanced 2-port OC-12/STM-4 SONET/SDH OSM, Multimode, with 4 GE
OSM-4OC12-POS-SI+	Enhanced 4-port OC-12/STM-4 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-2OC12-POS-SI	2-port OC-12/STM-4 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-2OC12-POS-SL	2-port OC-12/STM-4 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-2OC12-POS-MM	2-port OC-12/STM-4 SONET/SDH OSM, Multimode, with 4 GE

Hardware	Description
OSM-4OC12-POS-SI	4-port OC-12/STM-4 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-4OC12-POS-SL	4-port OC-12/STM-4 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-4OC12-POS-MM	4-port OC-12/STM-4 SONET/SDH OSM, Multimode, with 4 GE
OSM-1OC48-POS-SS+	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Short Reach, with 4 GE
OSM-1OC48-POS-SI+	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-1OC48-POS-SL+	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-1OC48-POS-SS	1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Short Reach, with 4 GE
OSM-1OC48-POS-SI	1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Intermediate Reach, with 4 GE
OSM-1OC48-POS-SL	1-port OC-48/STM-16 SONET/SDH OSM, Single mode, Long Reach, with 4 GE
OSM-2OC48/1DPT-SI	2-port OC-48/STM-16 POS/DPT OSM, Single mode, Intermediate Reach, with 4 GE
OSM-2OC48/1DPT-SL	2-port OC-48/STM-16 POS/DPT OSM, Single mode, Long Reach, with 4 GE
OSM-2OC12-ATM-SI+	Enhanced 2-port OC-12/STM-4 ATM OSM, Single mode, Intermediate Reach, with 4 GE
OSM-2OC12-ATM-MM+	Enhanced 2-port OC-12/STM-4 ATM OSM, Multimode, with 4 GE
OSM-1CHOC12/T3-SI	1-port Channelized OC-12/STM-4 to T3/E3 OSM, Single mode, Intermediate Reach, with 4 GE
OSM-1CHOC12/T1-SI	1-port Channelized OC-12/STM-4 to T1/E1 and DS0 OSM, Single mode, Intermediate Reach, with 4 GE
OSM-12CT3/T1	12-port Channelized DS-3 to DS1/DS0 OSM
WS-X6582-2PA	FlexWAN Module for Cisco 7600 and Cisco Catalyst 6000
PA-4T+	4-port Serial Port Adapter, Enhanced
PA-8T-V35	8-port Serial, V.35 Port Adapter
PA-8T-232	8-port Serial, 232 Port Adapter
PA-8T-X21	8-port Serial, X.21 Port Adapter
PA-H	1-port HSSI Port Adapter
PA-2H	2-port HSSI Port Adapter
PA-A3-8E1IMA	8-port ATM Inverse MUX E1 (120 Ohm) Port Adapter
PA-A3-8T1IMA	8-port ATM Inverse MUX T1 Port Adapter
PA-A3-E3	1-port ATM Enhanced E3 Port Adapter
PA-A3-T3	1-port ATM Enhanced DS3 Port Adapter
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 Single mode Intermediate Reach Port Adapter
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 Single mode Long Reach Port Adapter
PA-A6-E3	1-port ATM E3 Port Adapter, Enhanced
PA-A6-T3	1-port ATM DS3 Port Adapter, Enhanced
PA-A6-OC3MM	1-port ATM OC-3c/STM-1 Multimode Port Adapter, Enhanced
PA-A6-OC3SMI	1-port ATM OC-3c/STM-1 Single mode Intermediate Reach Port Adapter, Enhanced
PA-A3-OC3SML	1-port ATM OC-3c/STM-1 Single mode Long Reach Port Adapter, Enhanced
PA-E3	1-port E3 Serial Port Adapter with integrated E3 DSU
PA-2E3	2-port E3 Serial Port Adapter with integrated E3 DSU
PA-T3+	1-port T3 Serial Port Adapter Enhanced
PA-2T3+	2-port T3 Serial Port Adapter Enhanced
PA-MC-E3	1-port Multichannel E3 Port Adapter
PA-MC-T3	1-port Multichannel T3 Port Adapter
PA-MC-2T3+	2-port Multichannel T3 Port Adapter

Hardware	Description
PA-MC-2T1	2-port Multichannel T1 Port Adapter with integrated CSU/DSU
PA-MC-4T1	4-port Multichannel T1 Port Adapter with integrated CSU/DSU
PA-MC-8T1	8-port Multichannel T1 Port Adapter with integrated CSU/DSU
PA-MC-8TE1+	8-port Multichannel T1/E1 8PRI Port Adapter
PA-MC-2E1/120	2-port Multichannel E1 Port Adapter with G.703 120 ohm interface
PA-MC-8E1/120	8-port Multichannel E1 Port Adapter with G.703 120 ohm interface
PA-POS-OC3MM	1-port Packet over SONET OC3c/STM1 Multimode Port Adapter
PA-POS-OC3SMI	1-port Packet over SONET OC3c/STM1 Single mode Intermediate Reach Port Adapter
PA-POS-OC3SML	1-port Packet over SONET OC3c/STM1 Single mode Long Reach Port Adapter
PA-MC-STM-1MM	1-port Multichannel STM-1 Multimode Port Adapter
PA-MC-STM-1SMI	1-port Multichannel STM-1 Single mode Port Adapter
WS-SVC-IPSEC-1	IPSec VPN Security Module for Catalyst 6500 and Cisco 7600

SOFTWARE FEATURES

Cisco IOS Software Release 12.2(17b)SXA incorporates all software features supported in Cisco IOS Software Release 12.2(17a)SX, and adds support for new features listed in Table 3.

Note: MPLS feature require Supervisor Engine 720 with PFC3BXL

Table 3. New Software Features Supported with the Supervisor Engine 720 in Cisco IOS Software Release 12.2(17b)SXA

Feature	Description
MPLS Virtual Private Network (MPLS VPN)	MPLS VPN allows a network, based on Cisco IOS Software, to deploy scalable IPv4 Layer 3 VPN backbone services. VPNs are the foundation for deploying or administering value-added services including applications and data hosting network commerce, and telephony services to business customers. Supported natively on the Supervisor Engine 720, RFC2547 MPLS VPNs offer the following benefits: • A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce • Privacy and security equal to that provided by Layer 2 VPNs by limiting the distribution of VPN routes to only those routers that are members of the VPN seamless integration with customer intranets. For more information about the MPLS VPN feature, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134ac9.html

Feature	Description
MPLS VPN Carrier Supporting Carrier	MPLS VPN Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers, such as Internet service providers (ISPs) or a Border Gateway Protocol (BGP)/MPLS VPN service providers, to use a segment of its backbone network. Two methods can be used to transport routes and MPLS labels between the backbone carrier provider edge (PE) routers and the customer carrier customer edge (CE) routers: • IPv4 BGP Label Distribution • LDP and IGP Label Distribution IPv4 BGP Label Distribution enables a CSC network to be configured using BGP to transport routes and MPLS labels between the backbone carrier PE routers and the customer carrier CE routers. The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be either an ISP with an IP core or an MPLS service provider with or without VPN services. Label Distribution Protocol (LDP) and an Internal Gateway Protocol (IGP) can also be used between PE and CE routers to achieve the same goal. Using BGP to distribute IPv4 routes and MPLS label routes has the following benefits: • BGP takes the place of an IGP and LDP. You can use BGP to distribute routes and MPLS labels. Using a single protocol instead of two simplifies the configuration and troubleshooting. • BGP is the preferred routing protocol for connecting two ISPs, mainly because of its routing policies and ability to scale. ISPs commonly use BGP between two providers. This feature enables those ISPs to use BGP. For more information about the MPLS VPN CSC feature, refer to the Cisco document at the following locations: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134abd.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134adc.html
MPLS VPN Inter-Autonomous System	MPLS VPN Inter-Autonomous System enables a VPN service provider network to exchange IPv4 routes with MPLS labels. Using Inter-Autonomous System a local PE router needs to know the routes and label information for the remote PE router. This information can be exchanged between the PE routers and autonomous system boundary routers (ASBRs) in one of two ways: • **IGP and LDP:** The ASBR can redistribute the IPv4 routes and MPLS labels that it learned from EBGP into IGP and LDP and vice versa. • **Internal Border Gateway Protocol (iBGP) IPv4 label distribution:** The ASBR and PE router can use direct iBGP sessions to exchange VPNv4 and IPv4 routes and MPLS labels. Using BGP to distribute IPv4 routes and MPLS label routes has the following benefits: Improved scalability because the route reflectors store VPNv4 routes • Ability to enable a non-VPN core network to act as a transit network for VPN traffic • Elimination of the need for any other LDP between adjacent label switch routers (LSRs) For more information about the MPLS VPN Inter-Autonomous System feature, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134ac8.html
MPLS VPN ID	MPLS VPN ID allows VPNs to be identified by an identification (ID) number, as described in RFC 2685. Multiple VPNs can be configured in a router using a unique ASCII string to reference a specific VPN. **Note:** Configuration of a VPN ID for a VPN is optional. In addition, the MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates. For more information about the MPLS VPN ID feature, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134aa8.html

Feature	Description
MPLS DiffServ Tunneling	MPLS DiffServ Tunneling allows service providers to manage the quality of service (QoS) provided to an MPLS packet in an MPLS network. MPLS DiffServ Tunneling on the Cisco 7600 and Cisco Catalyst 6500 conforms to the IETF draft standard for Uniform and Short Pipe modes and provide a common set of per-hop behaviors (PHBs) to different service provider customers. Short Pipe mode provides transparency, standard edge service, and scalability so the customer's set of PHBs is applied on both the egress PE-to-CE link and on the ingress CE-to-PE link. Customers are likely to use Uniform mode if they have no markings or few markings. The customer lets the ISP mark the packets and retain their markings. In Uniform mode, all changes to QoS markings are reflected at each level (that is, IGP, BGP, and IP). For more information about the MPLS DiffServ Tunneling feature, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bd5.html
Ethernet over MPLS (EoMPLS)	EoMPLS allows the point-to-point transport Layer 2 Ethernet VLAN packets from various customers over an MPLS backbone. EoMPLS extends the usability of the MPLS backbone by enabling it to offer Layer 2 services in addition to already existing Layer 3 services. The MPLS backbone network can be configured to accept Layer 2 VLAN packets by configuring the PE routers at both ends of the MPLS backbone. For more information about the Cisco Any Transport over MPLS (AToM) features, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide_book09186a0080134a17.html
Virtual Private LAN Service (VPLS)	VPLS is a multipoint L2-VPN service allowing multiple sites to be connected over a simulated Ethernet broadcast domain that is supported across a provider provisioned MPLS / IP network. In other words, VPLS delivers a multipoint Layer 2 service over a Layer 3 network architecture. VPLS evolved as a logical extension of Ethernet over MPLS (EoMPLS), developed to deliver point-to-point Ethernet-based L2-VPN services. For more information about VPLS features, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/hw/routers/ps368/products_white_paper09186a00801df1df.shtml
Frame Relay over MPLS (FRoMPLS)	FRoMPLS works by encapsulating Frame Relay protocol data units (PDUs) in MPLS packets and forwarding them across the MPLS network to other Frame Relay destinations. The process of transporting the PDU differs, depending on whether you set up DLCI-to-DLCI connections or port-to-port connections. This is useful in providing point-to-point transport of Frame Relay circuits across a packet network. Service providers can quickly add new sites with less effort than with typical Frame Relay provisioning. For more information about AToM features, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide_book09186a0080134a17.html
ATM Single Cell Relay over MPLS—VC Mode (CRoMPLS)	ATM CRoMPLS allows ATM cells to be transported across MPLS networks transparently. ATM PVCs are transported by encapsulating ATM Cells in MPLS. Service providers can now offer Layer 2 services along with Layer 3 services. This setup allows transportation of ATM signaling and operations, administration, and maintenance (OAM) cells across a packet network, making a packet network invisible to the ATM network. The ATM CRoMPLS feature enables service providers to use the same tools for provisioning and to aggregate the existing frame and ATM installations to a high-speed packet core that is based on IP/MPLS. For more information about AToM features, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide_book09186a0080134a17.html
ATM AAL5 over MPLS (AAL5oMPLS)	The AAL5oMPLS feature provides an ATM permanent virtual circuit (PVC) for transporting ATM Adaptation Layer 5 (AAL5) PDUs across an IP/MPLS backbone with rate-limit policing and configurable PVC priority values. A dynamic MPLS tunnel is configured to enable label imposition and disposition of encapsulated ATM PDUs transported between two edge routers having a Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP) neighbor relationship. ATM AAL5 extends the usability of the MPLS backbone by enabling it to offer Layer 2 services in addition to already existing Layer 3 services. You can enable the MPLS backbone network to accept AAL5 PDUs by configuring the PE routers at both ends of the MPLS backbone. For more information about AToM features, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide_book09186a0080134a17.html

Feature	Description
Multilink Frame Relay (FRF.16)	Multilink Frame Relay (FRF.16) introduces functionality based on the Frame Relay Forum's Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single higher bandwidth virtual bundle. This is most critical for FR customers who need physical access bandwidth between a T1/E1 line and a T3/E3 line. Multilink Frame Relay is supported on User-Network Interfaces (UNI) and Network-to-Network Interfaces (NNIs) in Frame Relay networks and is supported on sub-T1/E1 links channelized optical services modules (OSMs) as well as port adapters used in the FlexWAN modules. For more information about the Multilink Frame Relay feature, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a9e.html
Automatic Protection Switching (APS) 1+1	APS is a means to provide redundancy on SONET equipment to guard against line failures. Previously supported on packet over SONET (POS) optical services modules (OSMs), APS 1+1 is now supported on the 2-port OC-12/STM-4 ATM OSM. SONET Linear APS 1+1 (GR-253) requires that for every working line, there must exist a redundant protection line. Traffic protected by the redundancy is carried via the working line and the protection line simultaneously. The "Working" and "Protect" channels can exist either on the same card, on different cards in the same system or in different routers. This implementation supports manually configured line protection for PVCs in both bidirectional and unidirectional modes. Note: Automatic configuration of protect interface is planned for a future release. For more information about APS 1+1, refer to the Cisco document at the following location: http://www.cisco.com/warp/public/127/aps_support_16140.pdf
ATM Virtual Circuit (VC) Bundling	ATM VC Bundling allows the assignment of different QoS parameters to different VCs to allow different types of traffic to traverse the VCs. IP-to-ATM CoS mappings can be applied in order to divide traffic to the different VCs depending on the desired class of service. Once separated to the desired bundle, advanced queuing and bandwidth management functionality like CBWFQ, WRED or LLQ can be applied to each VC. With MPLS traffic, the experimental (EXP) bits in the MPLS label can be used to determine which VC in the bundle to be used to forward packets. For more information about ATM VC Bundling, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd9ea.html and http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801b2410.html

Feature	Description
IPv6 Support on WAN Interfaces	First introduced in Cisco IOS Software Release 12.2(17a)SX1), IPv6 support is extended to cover WAN interfaces on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers delivering best-in-class industry performance when using the Supervisor Engine 720 . The following IPv6 features are supported in this release: • Base IPv6 protocol, including Internet Control Message Protocol Version 6 (ICMPv6), neighbor discovery, and stateless auto-configuration • IPv6 routing protocols—Static routes, Routing Information Protocol Next Generation (RIPng), Open Shortest Path First Version 3 (OSPFv3), Intermediate System-to-Intermediate System (IS-IS) for IPv6, and Multiprotocol Border Gateway Protocol Version 4 (MP-BGP4) • Data link layers as supported on the Cisco Catalyst 6500 Series and Cisco 7600 Series routers, including IEEE 802.1Q VLAN • IPv6 packet filtering—Standard and extended access control lists (ACLs) • Management services over an IPv6 transport—Domain Name System (DNS), Telnet, SSH, Trivial File Transfer Protocol (TFTP) client • Transition mechanisms—Configured, automatic, generic routing encapsulation (GRE), connection of IPv6 domains with IPv4 clouds (6to4), Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels the Cisco Supervisor Engine 720 supports IPv6 in hardware, offering up to 200-Mpps system performance with fabric-enabled line cards such as 4-port 10 Gigabit Ethernet (part number WS-6704-10GE), 24-port Gigabit Ethernet (part number WS-6724-GE-SFP), and 48-port 10/100/1000 (part number WS-6748-GE-TX) equipped with a distributed forwarding card (DFC3). In centralized forwarding mode, a system performance of 24 Mpps can be achieved. All the classic Cisco Express Forwarding 256 and distributed Cisco Express Forwarding 256 line cards that are currently supported with Supervisor Engine 720 can now be configured for IPv6 in centralized or distributed forwarding modes. Environments such as data centers, campuses, Internet exchange points, and infrastructures can now support IPv6 using various deployment options, including: • IPv6 over IPv4 tunnels—Over WAN (configured, 6to4) and LAN (ISATAP) • Dual stack networks—Native IPv4 and IPv6 configured For more details about IPv6 deployment strategies, refer to: http://www.cisco.com/en/US/tech/tk872/technologies_white_paper09186a00800c9907.shtml
IPv6 Provider Edge Router over MPLS	IPv6 Provider Edge Router over MPLS provides a method of sending IPv6 packets originating from an IPv6 edge router across an MPLS network backbone running an IPv4 control plane, without making changes to the software or hardware on the MPLS P routers. This solution configures a dual stack PE router, so the IPv6 traffic coming from the attached sites can be transparently transported over the MPLS core which is unaware of this IPv6 traffic, no need to run an IPv6 control plane. The IPv6 forwarding is done by label switching, eliminating the need for either IPv6 over IPv4 tunnels or for an additional Layer 2 encapsulation, allowing the appearance of a native IPv6 service to be offered across the network. The core network continues to run MPLS and any of the Cisco IOS Software-supported IPv4 interior routing protocols, eliminating the requirement for upgrades to the hardware for native IPv6 forwarding and allowing the network to continue with current proven releases of Cisco IOS Software. For more details about IPv6 deployment strategies, refer to: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d6636.html
Gateway Load Balancing Protocol (GLBP)	GLBP provides automatic router backup for IP hosts that are configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load between them. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail. For more information about GLBP, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a35.html

Feature	Description
OSPF Sham Link for MPLS/VPNs	In MPLS VPN configurations, the Open Shortest Path First (OSPF) protocol is one way to connect CE routers to PE routers in the VPN backbone. OSPF is often used by customers who run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone. Using an OSPF sham-link in an MPLS VPN has the following benefits: • Client site connection across the MPLS VPN backbone: A sham-link overcomes the OSPF default behavior for selecting an intra-area backdoor route between VPN sites instead of an inter-area (PE-to-PE) route. A sham-link ensures that OSPF client sites that share a backdoor link can communicate over the MPLS VPN backbone and participate in VPN services. • Flexible routing in an MPLS VPN configuration: In an MPLS VPN configuration, the OSPF cost configured with a sham-link allows you to decide if OSPF client site traffic will be routed over a backdoor link or through the VPN backbone.
OSPF Shortest Paths First Throttling	The OSPF Shortest Paths First Throttling feature makes it possible to configure Shortest Paths First (SPF) scheduling in intervals of milliseconds and to delay SPF calculations during network instability. SPF calculates the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events. The interval at which SPF runs is dynamically chosen, based on the frequency of topology changes. However, this automatically selected interval is still within the range of values that are defined by the user. If the network topology is unstable, SPF throttling calculates SPF scheduling intervals to be of longer duration until the network topology becomes stable again. For more information about the OSPF Shortest Paths First Throttling, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134ad8.html
RFC-1483 Bridging on FlexWAN	RFC 1483 bridging, as implemented on the FlexWAN and Enhanced FlexWAN modules for Cisco 7600 and Cisco Catalyst 6500 with an ATM port adapter (part number PA-A3-OC3), supports point-to-point and point-to-multipoint bridging of Layer 2 PDUs between Ethernet ports and the ATM interfaces on the ATM port adapter. RFC 1483 bridging for the FlexWAN is supported on AAL5-MUX and AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulated PVCs. For more information about the RFC-1483 Bridging feature, refer to the Cisco document at the following location: http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/atm.htm#xtocid10
IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	The IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication feature adds an HMAC-MD5 digest to each IS-IS PDU. HMAC is a mechanism for message authentication codes (MACs) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change. For more information about the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134751.html

Feature	Description
MPLS Label Distribution Protocol (LDP) MIB	The MPLS LDP MIB has been implemented to enable standard, Simple Network Management Protocol (SNMP)-based network management of the label switching features on the Cisco 7600 and Cisco Catalyst 6500 Series. Providing this capability requires SNMP agent code to execute on a designated network management system (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MPLS LDP MIB. The extensive label switching capabilities supported in Cisco IOS Software provide an integrated approach to managing the large volumes of traffic carried by WANs. These capabilities are integrated into the Layer 3 network services, thus optimizing the routing of high volume traffic through ISP backbones while, at the same time, helping to ensure the resiliency of the network to link or node failures. The Cisco 7600 Series routers and Cisco Catalyst 6500 Series switches support the following MPLS LDP MIB functionality in this release of Cisco IOS Software: • Generation and sending of event notification messages to signal changes in the status of LDP sessions • Enabling and disabling of event notification messages by means of extensions to existing SNMP command-line interface (CLI) commands • Specification of the name or the IP address of an NMS workstation in the operating environment to which Cisco IOS Software event notification messages are to be sent to serve network administrative and management purposes • Storage of the configuration that pertains to an event notification message into the NVRAM of the NMS For more information about the MPLS LDP MIB, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a95.html
MPLS Label Switch Router MIB	The MPLS LSR MIB allows SNMP to remotely monitor an LSR that is using the MPLS technology. The MPLS LSR MIB mirrors the Cisco Label Switching subsystem, specifically, the LSR management information that is provided by the Label Forwarding Information Base (LFIB). The MPLS LSR MIB contains managed objects that support the retrieval of label switching information from a router and is based on Revision 05 of the IEFT MPLS LSR MIB. This implementation enables a network administrator to get information on the status, character, and performance of the following: • MPLS capable interfaces on the LSR • Incoming MPLS segments (labels) to an LSR and their associated parameters • Outgoing segments (labels) at an LSR and their associated parameters In addition, the network manager can retrieve the status of cross-connect entries that associate MPLS segments with each other. For more information about the MPLS LSR MIB, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a79.html
MPLS VPN MIB	The MPLS VPN MIB is based on Revision 05 of the IETF MPLS VPN MIB provide the following data: • Describes managed objects for modeling a MPLS/BGP VPN • Configures and monitor routes and route targets for each VPN Routing and Forwarding (VRF) instance on a router • Facilitates provisioning VRF instances on MPLS interfaces • Measures the performance of MPLS/BGP VPNs For more information about the MPLS VPN MIB, refer to the Cisco document at the following location: http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a0080080d04.html
VLAN Translation	VLAN Translation simplifies management of VLAN 802.1Q tags by permitting customers to keep their pre-defined tags when accessing a Service Provider's Metro Ethernet network. In a Metro Ethernet environment, VLAN tags may overlap as disparate customers converge on common PE device to access to SP services such as Internet Access, IP VPN access, Transparent LAN Service (TLS). Forcing customers to renumber their VLANs to accommodate the Service Provider's environment would be a cumbersome and limiting exercise. Utilizing VLAN Translation, the customer tag is translated to a Service Provider tag at the PE device allowing forwarding decisions to be made on the new Service Provider tag.

Feature	Description
COS Mutation	COS mutation allows re-writing of COS value in the Service Provider tag reflecting the COS parameters from customer tag. 802.1Q Tunneling enables a Service Provider's PE device to add a second 802.1Q tag on top of the customer's 802.1Q tag thereby scaling the number of customers that can be served by any one PE device beyond 4096 VLANs. In a QinQ domain of a service provider metro network, switching decisions are based on the outermost service provider tag, ensuring customer SLA's for voice, video, data traffic are met. To deliver this service, the Service Provider tag must carry the appropriate COS values from the customer tag.
DSCP Mutation	Service Providers must have the flexibility to trust or remark the DSCP values on Ethernet frames entering a Metro Ethernet network. Using DSCP Mutation in a Supervisor 720 system allows customers to configure a DSCP map of up to 15 values and can choose to trust or rewrite the DSCP based on the configured map.
Layer 2 Protocol Tunneling Enhancements	Layer 2 Protocol Tunneling (L2PT) enables L2 protocol communication between customer sites connected across a service provider network by transparently tunneling Protocol Data Units (PDUs) such as CDP, STP & VTP. Previous software versions supported per-protocol and per-port rate limiting for tunneled PDUs using mechanisms implemented in software. L2PT Enhancements allow customers to control tunneled PDUs arriving on non L2PT enabled ports using a global configuration option. Additionally, Supervisor 720 provides hardware-based L2PT rate limiting, conserving the CPU processing.

ORDERABLE SOFTWARE IMAGES

Table 4 lists the software versions and applicable ordering information for the Cisco Catalyst 6500 Series/Cisco 7600 Series Supervisor Engine 720. Cisco IOS Software runs on the distributed forwarding card (DFC) to provide distributed Cisco Express Forwarding support. This image is bundled as part of the Supervisor Engine 720 image and is not released separately.

Table 4 lists the only product IDs that will be orderable. Once re-releases of Cisco IOS Software Release 12.2(17b)SXA are available, ordering these product IDs will automatically result in the most current release being shipped.

Caution: Always back up the switch configuration file to a TFTP server or Flash device before upgrading or downgrading the switch software, to avoid losing all or part of the configuration stored in NVRAM. When downgrading switch software, the configuration will be lost.

Table 4. Software Versions and Ordering Information

Product ID	Description	Image
S733AK9H-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise Firewall with MPLS, IPv6, and SSH	s72033-jk9o3sv-mz.122-17.SXA.bin
S733AK9H-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise Firewall with MPLS, IPv6, and SSH (SPARE)	s72033-jk9o3sv-mz.122-17.SXA.bin
S733AK9-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise with IPv6 and SSH	s72033-jk9sv-mz.122-17.SXA.bin
S733AK9-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise with IPv6 and SSH (SPARE)	s72033-jk9sv-mz.122-17.SXA.bin
S733ALK9-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise with IPv6 and SSH LAN only	s72033-jk9s-mz.122-17.SXA.bin
S733ALK9-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 Enterprise with IPv6 and SSH LAN only (SPARE)	s72033-jk9s-mz.122-17.SXA.bin
S733ZK9M-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 IP with MPLS, IPv6, SSH, and Border Gateway Protocol (BGP) License	s72033-pk9sv-mz.122-17.SXA.bin
S733ZK9M-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 IP with MPLS, IPv6, SSH, and BGP License (SPARE)	s72033-pk9sv-mz.122-17.SXA.bin
S733ZK9-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 IP with SSH	s72033-pk9sv-mz.122-17.SXA.bin
S733ZK9-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 IP with SSH (SPARE)	s72033-pk9sv-mz.122-17.SXA.bin
S733ZLK9-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 IP with SSH LAN only	s72033-pk9s-mz.122-17.SXA.bin

Product ID	Description	Image
S733ZLK9-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 IP with SSH LAN only (SPARE)	s72033-pk9s-mz.122-17.SXA.bin
S733Z-12217SXA	Cisco Catalyst 6500 Supervisor Engine 720 IP	s72033-psv-mz.122-17.SXA.bin
S733Z-12217SXA=	Cisco Catalyst 6500 Supervisor Engine 720 IP (SPARE)	s72033-psv-mz.122-17.SXA.bin
S763AK9H-12217SXA	Cisco 7600 Supervisor Engine 720 Enterprise Firewall with MPLS, IPv6, and SSH	s72033-jk9o3sv-mz.122-17.SXA.bin
S763AK9H-12217SXA=	Cisco 7600 Supervisor Engine 720 Enterprise Firewall with MPLS, IPv6, and SSH (SPARE)	s72033-jk9o3sv-mz.122-17.SXA.bin
S763ZK9M-12217SXA	Cisco 7600 Supervisor Engine 720 IP with MPLS, IPv6, SSH, and BGP	s72033-pk9sv-mz.122-17.SXA.bin
S763ZK9M-12217SXA=	Cisco 7600 Supervisor Engine 720 IP with MPLS, IPv6, SSH, and BGP (SPARE)	s72033-pk9sv-mz.122-17.SXA.bin
S763ZK9-12217SXA	Cisco 7600 Supervisor Engine 720 IP with SSH	s72033-pk9sv-mz.122-17.SXA.bin
S763ZK9-12217SXA=	Cisco 7600 Supervisor Engine 720 IP with SSH (SPARE)	s72033-pk9sv-mz.122-17.SXA.bin
S763Z-12217SXA	Cisco 7600 Supervisor Engine 720 IP	s72033-psv-mz.122-17.SXA.bin
S763Z-12217SXA=	Cisco 7600 Supervisor Engine 720 IP (SPARE)	s72033-psv-mz.122-17.SXA.bin

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

Pa/LW8140 03/05

Printed in USA