Cisco IOS Software Release 12.2(50)SY New Features and Hardware Support

PB661245

This product bulletin introduces Cisco IOS® Software Release 12.2(50)SY and includes the following sections:

- Cisco IOS Software Release 12.2(50)SY Introduction
- Packaging
- Hardware
- Service Module Support
- New Features
- Additional Information
- Support

Cisco IOS Software Release 12.2(50)SY Introduction

Release 12.2(50)SY is the first software release to enable the power and innovation of the new Supervisor Engine 2T of the Cisco® Catalyst® 6500 Series Switch. This release provides new hardware and software innovations that span multiple technology areas, including application performance with flexible netflow, advanced security and identity with Cisco TrustSec® security, Embedded Management with EEM and CMP, advanced IP routing, video and medianet with advanced services and multicast enhancements, IPv6 services and multicast, IPv6 Support, EVC, and VPLS.

Release 12.2(50)SY adds more than 200 new software features to the Cisco Catalyst 6500 Series, reinforcing its position as the most comprehensive switching platform available today.

For detailed information about the features and hardware supported in Release 12.2(50)SY, refer to the Cisco IOS Software Release 12.2(50)SY release notes and customer documentation at:

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

Not all features may be supported on all platforms. Use the Cisco Feature Navigator to find information about platform support and Cisco IOS Software image support:

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

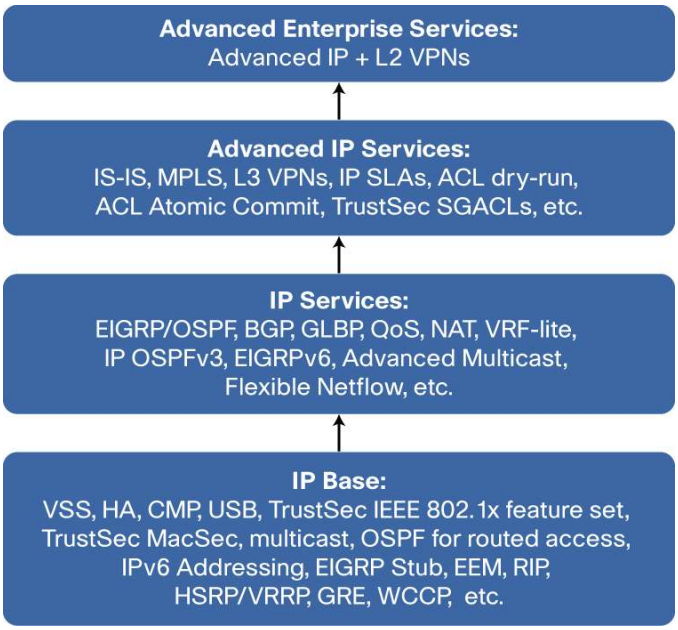
You must have an account on Cisco.com to access the Cisco Feature Navigator.

Cisco IOS Software Release 12.2(50)SY is developed for and intended to run on Cisco Catalyst 6500 Series Switches with Supervisor Engine 2T only.

Packaging

Cisco IOS Software is the world's leading network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware support. The traditional Cisco IOS Software packaging of Cisco Catalyst 6500 will be used for the new Supervisor Enginte 2T. Four image sets will be available: IP Base, IP Services, Advanced IP Services, and Advanced Enterprise Services. Each one of this sets will be available in two types: regular and No Payload Encryption (NPE). The regular images contains SSH as well as the possibility to encrypt traffic at line rate using the IEEE 802.1ae standard. The NPE images are targeted for countries with import restrictions and include control plane encryptions services such as SSH and SNMPv3, but they excludes the ability to encrypt data with IEEE 802.1ae.

Figure 1. Cisco IOS feature set map starting from 12.2(50)SY



Hardware

- **Cisco Catalyst 6500 Series Supervisor Engine 2T**

The Cisco Catalyst 6500 Supervisor Engine 2T (Figure 2) is the newest addition to the family of supervisor engines. The Supervisor Engine 2T is designed to deliver 3 times the performances, 4 times the scalability, and enhanced hardware-enabled features. Supervisor Engine 2T integrates a high-performance 2-Terabit crossbar switch fabric that enables 80 Gbps switching capacity per slot on all Cisco Catalyst 6500 E-Series Chassis. The forwarding engine on Supervisor Engine 2T is capable of delivering high-performance forwarding for Layer 2 and Layer 3 services. Supervisor Engine 2T delivers many new hardware-enabled innovations in the areas of security, quality of service (QoS), virtualization, manageability and much more. The rich feature set of Supervisor Engine 2T enhances applications such as traditional IP forwarding, Layer 2 and Layer 3 Multiprotocol Label Switching (MPLS) VPNs, and VPLS. The Cisco Catalyst 6500 with Supervisor Engine 2T and all the features and the technical advancements establish product leadership in borderless networks as well as data center deployments.

Figure 2. Cisco Catalyst 6500 Supervisor Engine 2T

- **6900 Series Ethernet Interface Module for Cisco Catalyst 6500 Series Switches**

The Cisco Catalyst 6500 Series Switches offer a variety of 10 Gigabit Ethernet modules to serve different needs in the campus and data center for enterprise, commercial, and service provider customers. The 6900 Series 8-port 10 Gigabit Ethernet Fiber Module is the first 10 Gigabit Ethernet Module for the Cisco Catalyst 6500 Series Switch that supports Cisco TrustSec® security and Layer 2 Encryption in HW to enable IEEE 802.1ae (MACSec) encryption as well as security group access control lists (SGACLs). The module has two 40 Gbps connections (for a total of 80 Gbps) to the 2Tbps switch fabric of the Supervisor Engine 2T and therefore is able to deliver 10 Gigabit performance on all 8 ports for larger than 128 bytes size packets at line rate. The new 6900 Series 8-port 10 Gigabit Ethernet Fiber module supports Virtual Switch Link (VSL) on all 8 ports. The 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module is only compatible with the new Cisco Catalyst 6500 Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), enabling the system to deliver three times the performance and four times the scalability for Cisco Catalyst 6500 Series Switches in comparison to the previous generation.

The new 6900 Series 8-Port 10 Gigabit Ethernet Fiber module (Figure 3) is designed for deployment in the distribution and core of the campus and data center for traffic aggregation in a network requiring Security, Manageability, Virtualization, Application Performance and Video. With its large 256 MB packet buffers per port, no oversubscription and distributed forwarding with high scalability, the new 6900 Series 8-port 10 Gigabit Ethernet Fiber module is able to deliver secure and predictable performance for bandwidth-intensive applications such as market data feeds in the financial vertical or video broadcast in the Campus networks.

The 8-Port 10 Gigabit Ethernet Fiber Module provides up to 88 10 Gigabit Ethernet Fiber ports in a single Cisco Catalyst 6513-E chassis and 178 10 Gigabit Ethernet ports in a Cisco Catalyst 6500 Virtual Switching System (VSS) 4T.

Figure 3. 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module

For more information, refer to the 6900 Series Ethernet Interface Module for Cisco Catalyst 6500 Series Switches product bulletins at:

- http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletins_list.html.
- **6800 Series Ethernet Interface Module for Cisco Catalyst 6500 Series Switches**

The modules in this family include the new 6800 Series 48-port 1 Gigabit Ethernet Copper Module, 16-port 10 Gigabit Ethernet Copper Module, 48-port 1 Gigabit Ethernet Fiber Module and 24-port 1 Gigabit Ethernet Fiber Module.

For more information, refer to the 6800 Series Ethernet Interface Module for Cisco Catalyst 6500 Series Switches product bulletins at:

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

Service Module Support

Release 12.2(50)SY provides supports for the service modules listed in Table 2.

Table 1. Supported Service Modules

Service Module Description	Part Number
Application Control Engine 20 Hardware	ACE20-MOD-K9
Firewall blade for 6500 and 7600, VFW License Separate	WS-SVC-FWM-1-K9
Cisco Catalyst 6500 Network Analysis Module-2	WS-SVC-NAM-2
Cisco Wireless Services Module (WISM)	WS-SVC-WiSM-1-K9

For an overview of Cisco IOS Software Packaging for Cisco switches, including its availability and the associated Cisco IOS Software release migration strategy, visit:

- http://www.cisco.com/go/packaging

New Features

In addition to the support of new hardware, and substantial feature set from 12.2(33)SXI, Table 1 lists the new.features and enhancements available with this Cisco IOS Software release.

Table 2. New Features and Enhancements

Application Performance	Security and Identity	Embedded Management	IP Services
• Flexible Netflow • Egress Netflow • Sampled Netflow • CPU friendly NDE export • Netflow on CoPP interface • QoS Distributed Policer • Monitoring with third party applications like wireshark.	• Authenticated networking infrastructure with 802.1X • Ingress Security Group Tagging • Secure communication with MACSec Encryption • Cisco TrustSec Reflector • Layer 3 ACL Dry Run • ACL Hitless Atomic Update • New ACL Classification Options	• Connectivity Management Processor • Embedded Event Manager (EEM) 3.0 • Control Plane Policing • Web Services Support • Per Protocol statistics • USB support • XML API	• NAT - Static Mapping of a Port Range • uRPF 16 path support • WCCP Enhancements

IP Multicast	IPv6	Network Virtualization	Metro Technologies
• CoPP for multicast on Cisco Catalyst 6500 • MFIB and Distributed MFIB for IPv4 Multicast • Hardware Acceleration support for PIM Register packets • IGMPv3 Snooping: Full Support • IPv4 Multicast Support on MFIB (Infrastructure) • IPv6 Boot Strap Routing (BSR) - Configure RP mapping • ISSU - MFIB IPv4 Multicast • Multicast Bidirectional PIM support for 8 Rendezvous	• IPv6 uRPF • IPv6 Neighbor Discovery Protocol Inspection (NDP Inspection) • IPv6 Device Tracking • IPv6 RA-Guard • IPv6 Port Access Control List (PACL) • IPv4 and IPv6 support for RFC 4292 - IP Forwarding Table MIB • IPv4 and IPv6 support for RFC 4293 - MIB for the Internet Protocol (IP) • IPv6 statistics and counters	• MPLS Pseudowire Status Signaling • MPLS Traffic Engineering (TE) - Path Protection • L2oGRE • NSF/SSO - Any Transport over MPLS (AToM) • VPLS • H-VPLS	• EOAM • EVC

IP Multicast	IPv6	Network Virtualization	Metro Technologies
Points (RP) in Hardware • MVPN Scalability Improvements • NSF/SSO - IPv4 Multicast • SSO - IPv4 MFIB	• IPv6 - Cisco Networking Services (CNS) Agents • IPv6 - HTTP(S) • IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect) • IPv6 - Netconf • IPv6 - SOAP • IPv6 - TCL • IPv6 Flexible Netflow • IPv6 Unicast Flows • IPv6 ACL Scalability (Support for 4K ACL Labels) LLDP IPv6 address support		

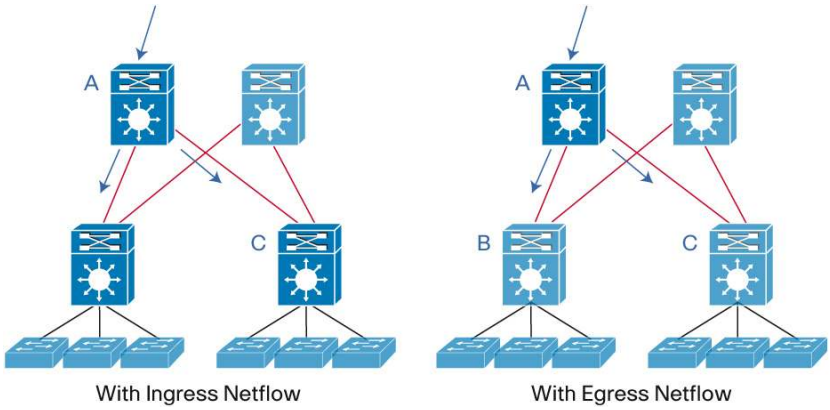
Application Performance

Supervisor Engine 2T introduces a whole set of new netflow hardware features and this release provides the software to take advantages of this new hardware.

- **Flexible Netflow:** Flexible NetFlow is the next-generation in flow technology. It allows optimization of the network infrastructure, reducing operation costs, improved capacity planning and security incident detection with increased NetFlow flexibility and scalability beyond other flow based technologies available today. Flexible NetFlow advantages include:
  - Flexibility, scalability, and customization of flow data
  - The ability to monitor a wider range of packet information
  - Enhanced network anomaly and security detection
  - User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
  - Convergence of multiple accounting technologies into one accounting mechanism
  - Multiple configurable flow caches

  Flexible Netflow in 12.2(50)SY takes advantage of the increased Netflow table of Sup2T as well as the improved hash efficiency. The system is able to monitor up to 13 million flows on a 13 slots chassis. Flexible netflow on Supervisor Engine 2T enables application visibility per flow.
- **Egress Netflow:** Traditionally netflow could only be applied at the ingress. Supervisor Engine 2T gives more flexibility to the user and allows monitoring flow at the egress as well as the ingress interfaces. In Figure 4, if the user wants to monitor traffic going to B and C with ingress netflow, he has to configure the feature on 2 interfaces on 2 different systems (B and C). With egress netflow, he only needs to configure on it on 1 system (A). This simplifies management as well as network operations cost. Egress netflow also allows the user to monitor each multicast flow egressing the system, so the user gets a deeper visibility of the network multicast traffic.

Figure 4. Ingress Netflow points of management compared to Egress Netflow



- **Sampled Netflow:** The Supervisor Engine 2T for the Cisco Catalyst 6500 Series Switch supports the ability to perform Netflow sampling in the hardware. Prior to the introduction of the Supervisor Engine 2T, all PFC3-based supervisor engines for the Cisco Catalyst 6500 Series Switch performed Netflow sampling in the software, without preventing population of the Netflow Table. The most common use case to use sampling is in an environment where the number of flows far exceeds the number of Netflow Entries supported by the system. In such a case, sampling gives a better representation of the overall traffic.
- **CPU friendly NDE export:** Netflow export is a very CPU intensive application. Controlling CPU utilization is key to protect against undesirable side effects on the network. This helps ensure that the NDE process will not affect other functions, such as the processing of Layer 2 protocols, Layer 3 protocols, or other system management processes. This new feature introduced on Supervisor Engine 2T allows a user to control the CPU utilized by the Netflow Data Export process when Netflow records are being exported to a collector. Netflow statistics collection is performed in the hardware, with no effect on forwarding performance.
- **Netflow on Control Plane interface:** Properly configuring control plane policing is very important to ensure scalability with stability of the system. Using Flexible Netflow (FNF), the user can monitor control-plane traffic on a per flow basis to develop realistic traffic rates which can then be used in developing custom control-plane service-policies. Flexible Netflow provides granular traffic classification and allows for policies which target specific traffic flows without affecting other legitimate control-plane traffic.
- **QoS Distributed Policer:** Supervisor Engine 2T based systems support an optional distributed policing capability where multiple forwarding engines can communicate and synchronize the amount of traffic transmitted for a specific policer. The Supervisor Engine 2T supports up to 16,384 (16K) total policers; 4096 (4K) of these can be distributed policers. The distributed policing functionality provides a significant benefit for a Cisco Catalyst 6500 with multiple DFCs installed. The distributed policing functionality reduces if not eliminates the need for the software-based policing associated with the non-distributed implementation. The distributed policing functionality is an optional feature and can be enabled using a global command.
- **Monitoring with third party applications:** Supervisor Engine 2T supports the mini protocol analyzer. With this feature, the user can capture traffic in hardware and send it to the control plane for analysis. The command line interface allows for deep packet inspection, or alternatively the user can decide to export the captured buffer to a pcap file for off the box analysis with a network analyzer like Wireshark.

Security and Identity

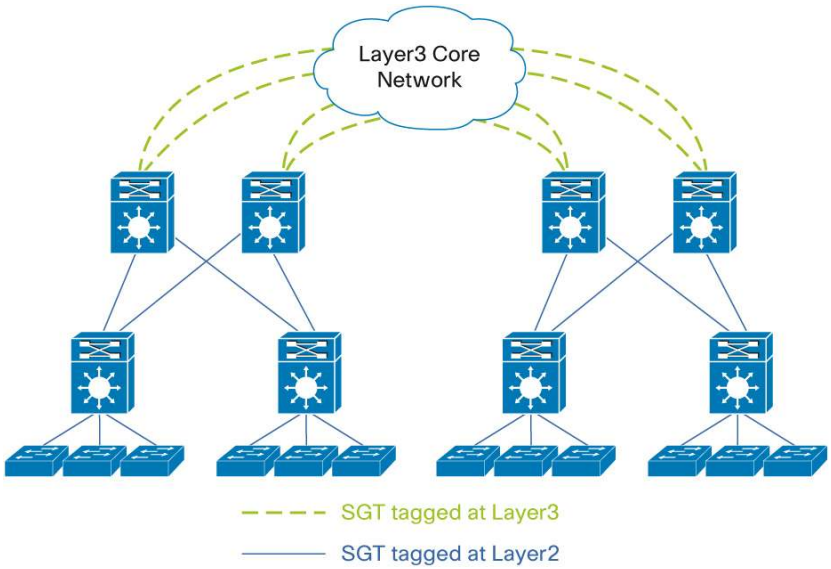
This release enhances Cisco TrustSec on Cisco Catalyst 6500 Series Switches with advanced features geared to improve scalability, manageability, and operation. With Supervisor Engine 2T and 12.2(50)SY, Cisco Catalyst 6500 plays a central role in the overall Cisco TrustSec solution. This architecture builds secure networks by establishing domains of trusted network devices, with each device in the domain authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

- **Authenticated networking infrastructure with 802.1X:** 12.2(50)SY implements the full 802.1X security features set, so users and device can be authenticated in the Cisco TrustSec domain.
- **Secure communication with MACSec Encryption:** 12.2(50)SY enables MACSec hardware encryption on all the new 69XX line cards as well as on the Supervisor Engine 2T. Communication on each link between devices in the domain can be secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

Cisco TrustSec uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

- **Ingress Security Group Tagging:** Access policies within the Cisco TrustSec domain are topology-independent, based on the roles (as indicated by security group number) of source and destination devices rather than on network addresses. Supervisor Engine 2T introduces hardware-based SGT imposition so individual packets are tagged in hardware with the security group number of the source. 12.2(50)SY and Supervisor Engine 2T not only tag the packets at Layer 2 but can also do it at Layer 3. This functionality allows to easy propagation of SGT tagged traffic on top of an existing Layer 3 infrastructure. The migration to Cisco TrustSec gets simplified.
- **Egress Security Group Enforcement:** At the egress point of the Cisco TrustSec domain, an egress Supervisor Engine 2T uses the source SGT and the security group number of the destination entity (the destination SG, or DGT) to determine which access policy to apply from the SGACL policy matrix.

Figure 5. Layer 3 SGT tagging and forwarding to pass SGT over a heterogeneous Layer 3 network.



Supervisor Engine 2T and 12.2(50)SY also help the deployment of Cisco TrustSec by providing investment protection to existing Cisco Catalyst 6500 users with the use of:

- **Cisco TrustSec Reflector:** This feature allows the user to plug non Cisco TrustSec capable line cards in a 6500 chassis with Supervisor Engine 2T. The traffic ingressing and egressing from those line cards will be reflected to the supervisor so it can add or remove the SGT tag to ingressing and egressing traffic.
- **SXP Support:** Network devices not supporting SGT imposition in hardware use SXP to exchange the SGT/IP binding. 12.2(50)SY provides SXP support to Supervisor Engine 2T, allowing the user to interconnect with such devices.

12.2(50)SY improves the ACL utilization with the following features.

- **Layer 3 ACL Dry Run:** Configuring large ACLs can be quite a tedious task. ACLs that do not fit in the hardware resources could cause software forwarding and possible high CPU utilization. This new feature allows the user to verify if the ACL changes will fit within the hardware resources before applying it. By doing so, the user can change its ACLs configuration without risking side effects on the control plane of its device.
- **ACL Hitless Atomic Update:** This new feature makes sure that the production traffic is not affected by ACL modification. The traffic will use the new ACL only when this one is fully programmed in hardware. It also avoids unanticipated network disruption by allowing the update of multiple features at once (IPv4, IPv6, RACL, VACL, and so on).
- **New ACL Classification Options:** 12.2(50)SY adds more granularity to ACL definitions by offering to classify the traffic based on new options such as dscp, fragments, IP options, time-range, ttl, and so on.

Embedded Management

- **Connectivity Management Processor (CMP)**

CMP is a dedicated management processor to access the switch, restore it and prevent downtime caused by maintenance or troubleshooting. Below are 4 primary benefits of CMP:

1. Users can access the console remotely (SSH/telnet) without a terminal server for troubleshooting and recovery (even when the route processor is not responsive).
2. Users are able to quickly recover image via TFTP/USB remotely without terminal server or on-site personnel requirements.
3. Users are able to reset the Supervisor Engine 2T remotely without any external power management devices.
4. In a situation where the primary console is unresponsive or the Cisco IOS Software image is unresponsive and the Cisco IOS Software image on compact flash is corrupted, the CMP provides the ability to access the switch logs, in order to determine the possible causes.

- **Embedded Event Manager (EEM) 3.0**

Embedded script engine to customize device monitoring and automate tasks. EEM allows users to conduct network operations based on triggers or event scripts. This allows tasks to be automated based on real-time network traffic detection and reaction via flexible netflow.

- **Control Plane Policing (CoPP)**

CoPP is a critical feature in making sure that the CPU of the supervisor engine is protected and regulated from traffic spikes. The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS Software routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

IP Services

- **IP NAT - Static Mapping of a Port Range:** The Cisco Catalyst 6500 performs NAT in hardware with high throughput. In this software release, one IP NAT improvement is the ability to configure a static ip NAT mapping and indicate a range of contiguous ports. Previously only one specific port was permitted in a static NAT.
- **WCCP improvements:** Supervisor Engine 2T has new hardware and software capabilities that improve WCCP operations. These improvements include Egress Netflow Support, Egress ACL rewrite, and WCCP GRE Decapsulation hardware support. Egress NetFlow can be used for egress WCCP features when NetFlow is needed. Ingress WCCP uses Ingress NetFlow entry and the Egress WCCP feature uses Egress NetFlow entry whenever a NetFlow entry is required for hardware packet redirection. WCCP GRE return packet processing is also implemented in hardware.
- **VRF aware WCCP:** The WCCP VRF Support feature enhances the existing WCCPv2 protocol by implementing support for Virtual Routing and Forwarding (VRF). The WCCP VRF Support feature allows service groups to be configured on a per VRF basis in addition to those defined globally.

IP Multicast

Multicast is used in many Enterprise networks today for financial data, video training, and other multimedia applications. Supervisor Engine 2T and the 12.2(50)SY software release added many multicast enhancements for Cisco Catalyst 6500 customers. (See Table 3.)

One of the largest improvements is the dedicated Multicast Forwarding Information Base (mFIB). This is a dedicated multicast forwarding table which improves scalability. There are many other enhancements in this software release that also improve the multicast failover and throughput customers will experience.

Table 3. Multicast Enhancements for Supervisor Engine 2T in 12.2(50)SY

Unified IPv4/IPv6 mFIB Infrastructure	Optimized hardware infrastructure, designed for Layer 2/Layer 3 scalability.
New Egress Replication (EDC Server and Client) Design	Optimizes multicast frame distribution, between modules.
New Multicast LTL and Multicast Expansion Table (MET) "Sharing" Design	Saves internal forwarding resources, for commonly-used paths.
Up to 256 K IPv4 Multicast Routes in the FIB-XL	Provides unprecedented hardware-based multicast scalability.
PIM-SM Source Register Support in Hardware	Saves CPU and memory usage and minimizes source register time.
PIM-SM Dual-RPF Support in Hardware	Saves CPU and memory usage and minimizes SPT switchover time.
Simplified Global Layer 2 IGMP Snooping Design	Provides a simplified Layer 2 snooping configuration and querier redundancy.
IP-Based (Compared to DMAC-Based) Layer 2 Forwarding Lookups	Removes the IP-to-MAC address overlap, for Layer 2 multicast.
IGMPv3 and MLDv2 Snooping Host Tracking in Hardware	Faster join and leave updates of IPv4/IPv6 PIM-SSM Layer 2 host tables.
New Layer 2 Optimized Multicast Flood (OMF) Design	Saves forwarding resources and bandwidth, for "source-only" VLANs.
Multicast VPN (MVPN) Egress-Replication Support	Saves switch fabric bandwidth when forwarding MVPN/eMVPN.
Support for 8 PIM-BIDIR Hardware RPDF Entries	Allows for eight simultaneous RPs to be defined, in hardware.
IPv6 Multicast (*,G) and (S,G) Entries in FIB TCAM	Improved IPv6 hardware-based forwarding, decreases latency.
Enhanced Multicast HA Using the New Infrastructure	High availability, built on the new infrastructure, optimizes switchover.
CoPP Exception Cases and More Granular Multicast Rate Limits	Improved control-plane protection for multicast traffic sent to the CPU.
NetFlow (v9 and FnF) Special Fields and Processing for Multicast	All new NFv9 + flexible NetFlow and egress NDE support for multicast flows.

IPv6

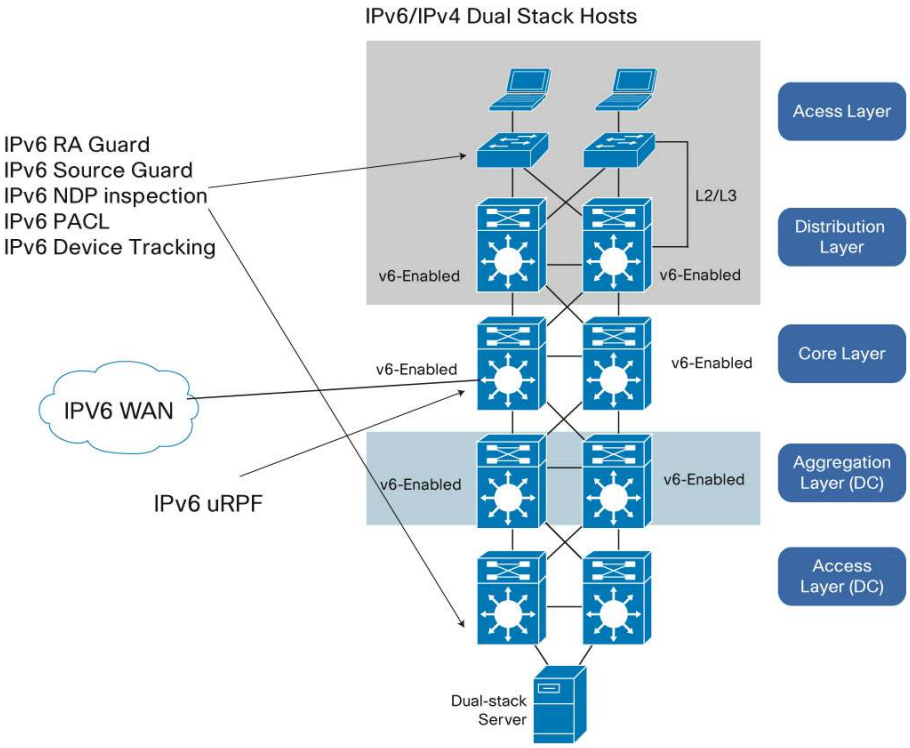
Networks today are predominately IPv4. The networks of the future will need to grow and that growth will be in the IPv6 space. The Cisco Catalyst 6500 preserves the IPv4 network investment and continues to offer customers new IPv6 services to prepare for the orderly transition to IPv6.

For more information on IPv6 Campus Design, see:

- http://www.cisco.com/en/US/partner/solutions/ns340/ns414/ns742/ns815/landing_cIPv6.html

Figure 6 shows where to deploy in the network the new IPv6 Security Features.

Figure 6. Network Placement Where New IPv6 Features for First Hop Security and IPv6 uRPF Apply



- **IPv6 Unicast Reverse-Path Forwarding (uRPF):** IPv6 uRPF is a security feature that checks to see if traffic is spoofed. The IPv6 uRPF feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. If URPF does not find a reverse path for the packet, uRPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the ipv6 verify unicast source reachable-via command. In this software release, uRPF increases from 6 to 16 paths for both IPv4 and IPv6.

  For more information on uRPF, read:

  - http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

- **IPv6 Neighbor Discovery Protocol Inspection (NDP Inspection):** IPv6 Neighbor Discovery Protocol Inspection (NDP Inspection) prevents spoofing attacks due to NDP vulnerabilities. IPv6 NDP Inspection learns and secures bindings for stateless auto configuration addresses in the Layer 2 Neighbor Cache.

  NDP inspection can verify the signature of ND message containing CGA (Cryptographically Generated Address) IPv6 address. If the verification fails, then it drops the NDP messages.

- **IPv6 Device Tracking:** The tracking command in NDP inspection policy configuration mode overrides the default tracking policy set by the ipv6 neighbor tracking command on the port on which this policy applies. This function is useful on trusted ports where, for example, one may not want to track entries but wants an entry to stay in the binding table to prevent it from being stolen. The switch probes secure nodes at regular intervals by sending unicast Neighbor Solicitation messages with source ip address as unspecified address. The Active Node responds with a neighbor advertisement.

  A Failure to receive response results in removing node's entry from neighbor cache and its access privileges are revoked by the guard features.

  For more information on Neighbor Discovery, read:

  - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-563156.html
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html#wp1282543

  For more information on IPv6 First Hop Security, read:

  - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-602135.html
- **IPv6 RA-Guard Host Mode:** IPv6 RA-Guard protects from Rogue RA generated maliciously or unintentionally. The content of the RA message is inspected and the decision of dropping it can be based on almost all RA fields including prefixes. This sometimes happens due to unauthorized or improperly configured IPv6 hosts when operating IPv6 in a shared Layer 2 network environment.

  For more information visit:

  - http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Campus/CampIPv6.html
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **IPv6 Port-Based Access Control List (IPv6 PACL) Support:** Port-based access control list (PACL) provides a mechanism to filter incoming packets based on Layer 2 through 4 parameters at Layer 2 port level for IPv6 traffic. This feature increases the level of security available to the Cisco Catalyst 6500 when IPv6 is configured.

  IPv6 PACLs function the same way as IPv4 PACLs except that they apply to IPv6 traffic.

  EtherChannels also behave the same way as with IPv4 PACLs.
- **IPv4 and IPv6 support for RFC 4292 (IP Forwarding Table MIB) and RFC 4293 (MIB for the Internet Protocol)**
- **IPv6 statistics and counters:** Supervisor Engine 2T has new hardware functionality to support separate ingress and egress statistics for IPv6 traffic. Supervisor Engine 2T allows for the accounting of traffic for IPv4, IPv6, and MPLS traffic separately which gives more visibility to the network management. Supervisor Engine 720 only supported egress statistics for IPv6 traffic. With this new Supervisor Engine 2T functionality, RFC 4292 and RFC 4293 can be supported with both ingress and egress statistics.
- **IPv6 Cisco Networking Services (CNS) Agents:** IPv6 addressing is supported with Cisco Networking Services (CNS). CNS is a foundation technology for linking users to networking services and provides the infrastructure for the automated configuration of large numbers of network devices. When standard configurations do not exist or have been modified, the time involved in initial installation and subsequent upgrading is considerable.
- **IPv6 Config Logger:** IPv6 Configuration Logger is used to monitor who is making changes to the network. IPv6 support for Config Logger is now available. Configuration logger tracks and reports configuration changes. Config logger supports two content types:
  - Plain text - With plain-text format, the config logger reports configuration changes only.

- XML - The config logger uses Extensible Markup Language (XML) to report the configuration change details (for example, what changed, who changed it, when changes were made, parser return code (PRC) values, and incremental NVGEN results).

- **HTTP(S) IPv6 Support:** This feature enhances the HTTP(S) client and server to support IPv6 addresses. The HTTP server in Cisco IOS Software can service requests from both IPv6 and IPv4 HTTP clients. The HTTP client in Cisco IOS Software supports sending requests to both IPv4 and IPv6 HTTP servers.
- **IP SLAs for IPv6:** Cisco IOS Software IP Service Level Agreements (SLAs) are a portfolio of technology embedded in Cisco IOS Software that allows Cisco customers to analyze IPv6 service levels for IPv6 applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLAs uses active traffic monitoring - the generation of traffic in a continuous, reliable, and predictable manner - for measuring network performance. IP SLAs can be used to proactively monitor VoIP quality levels in your network, allowing you to guarantee VoIP quality levels to your users in IPv4 or IPv6 networks.
- **IPv6 NETCONF:** The Network Configuration Protocol (NETCONF) defines a mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. NETCONF uses XML-based data encoding for the configuration data and protocol messages.

  For more information about NETCONF, see "Network Configuration Protocol" in the Cisco IOS Software Network Management Configuration Guide:

  - http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_netconf.html
- **IPv6 SOAP Message Format:** IPv6 Service-Oriented Access Protocol (SOAP) protocol provides a way to format the layout of Cisco Networking Services (CNS) messages in a consistent manner. SOAP uses XML technologies to define an extensible messaging framework that provides a message format that can be exchanged over a variety of underlying protocols.

  For more information about Cisco Networking Services see the Cisco IOS Software Network Management Configuration Guide:

  - http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- **IPv6 TCL:** Tool command language (TCL) is used in Cisco IOS Software IPv6 to support features such as embedded event manager (EEM).

Network Virtualization

Many Cisco Catalyst 6500 customers use Network Virtualization to segment their network for solving business problems related to compliance, infrastructure utilization, rapid service provisioning, and lowering capital and operating costs. Network Virtualization functionality, performance, and features improved with the 12.2(50)SY software release due to the new improved hardware capabilities of the Supervisor Engine 2T.

For more information on Network Virtualization in Campus designs, see:

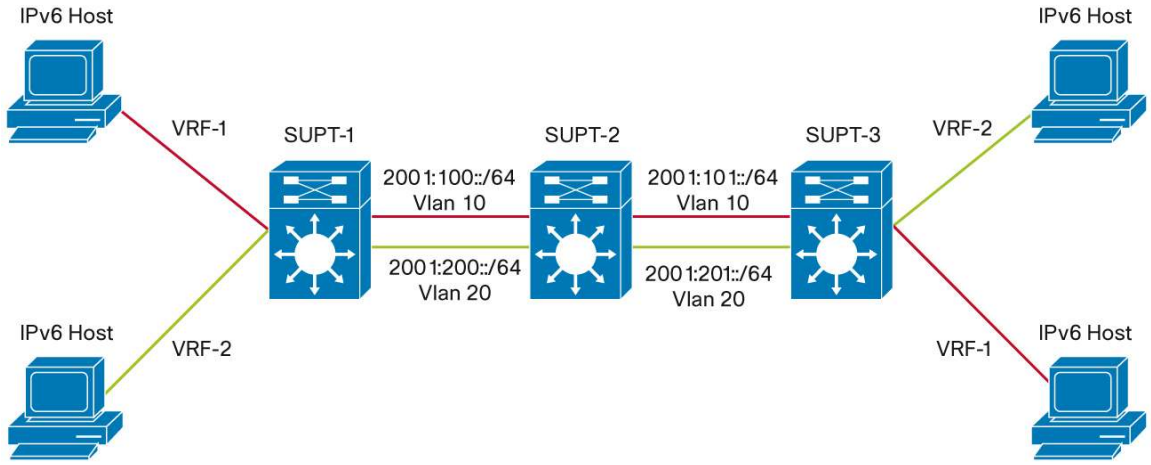
- http://www.cisco.com/en/US/partner/solutions/ns340/ns414/ns742/ns815/landing_cNet_virtualization.html

- **MPLS Throughput:** One of the improvements is increased MPLS packet throughput because the software support packets with up to 5 MPLS labels before recirculation is required. This functionality doubles the MPLS throughput with this software release.
- **MPLS Management:** Management of MPLS is easier with this software release because MPLS per interface, per protocol, and aggregate label statistics are also supported now.

VPLS support on the Cisco Catalyst 6500 with Supervisor Engine 2T is now native. Previously, VPLS support was only through SPA Interface Processor (SIP) WAN line card. With this software release, VPLS is supported on LAN line cards.

- **Bridge Domain Logical Interface (BD/LIF):** This is an infrastructure improvement which allows multiple functionalities. We can support 4096 VLANS and with the new Bridge Domain concept, we can support 16,384 internal bridge domains. There are several features that can use this improvements including VLAN reuse. Where VLANs were a shared resource before between VRFs, with Supervisor Engine 2T, we can scale VRFs and VLANS to 16,000 total. For example, we can have 4 VRFs with 4,000 VLANS each. Or have 8 VRFs with 2,000 VLANS each. With previous deployments prior to Supervisor Engine 2T, the limitation was 4,000 VLANs shared among all VRFs total. Other features, not just MPLS benefit from BD/LIF. Others technologies such as multicast for egress mVPN are enabled by BD/LIF and the new mFIB uses BD/LIF.
- **VLAN Re-use:** VRF-Lite deployments are now easier due to VLAN Re-use capabilities. This is where the same VLAN number can be used on subinterfaces under the same primary interface. Before this functionality, VRF-Lite scalability was limited due to the need for different VLAN between sub-interface which complicated deployment. (See Figure 8.)

Figure 7. VLAN Reuse Example Where Same VLAN Number Can Be Used on Different Interfaces from Same Switch Using VRF-Lite; IPv4 and IPv6 Supported



- **MPLS Pseudowire Status Signaling:** The MPLS Pseudowire Status Signaling feature enables you to configure the router so it can send pseudowire status to a peer router, even when the attachment circuit is down. This feature can be used to prevent blackholing of traffic because of a circuit down at the remote end.

  For more information, see:

  ◦ http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_pw_status.html
- **MPLS Traffic Engineering (TE) - Path Protection:** The MPLS Traffic Engineering (TE): Path Protection feature provides an end-to-end failure recovery mechanism (that is, full path protection) for Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  For more information on MPLS Traffic Engineering (TE) - Path Protection, see:

  ◦ http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html
- **Layer 2 over GRE (L2oGRE):** Layer 2 over GRE is a new feature which allows Layer 2 and Layer 3 packets to be bridged over a GRE tunnel. This behavior is similar to Layer 2 Tunneling Protocol (L2TP) which is not currently supported natively in hardware on the Cisco Catalyst 6500.

- **NSF/SSO - Any Transport over MPLS (AToM):** The NSF/SSO - Any Transport over MPLS and AToM Graceful Restart feature allows Any Transport over MPLS (AToM) to use Cisco nonstop forwarding (NSF), stateful switchover (SSO), and Graceful Restart (GR) to allow a Route Processor (RP) to recover from a disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

  NSF with SSO is effective at increasing availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

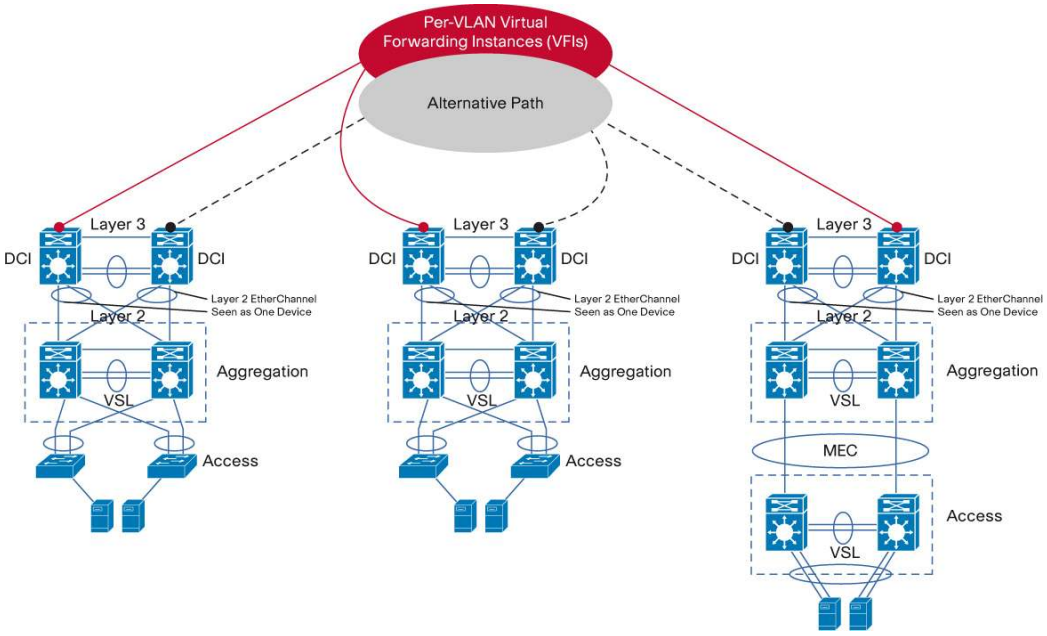
  For more information, see:

  - http://www.cisco.com/en/US/docs/ios/ios_xe/mpls/configuration/guide/mp_trnsprt_mlps_atom_xe.html
- **VRF aware NTP:** To configure the software clock to synchronize a peer or to be synchronized by a peer in a virtual private network (VPN) routing forwarding instance (VRF) for routing to the destination instead of to the global routing table.
- **VRF support for TFTP server, TFTP Client, and FTP client:** TFTP and FTP are now VRF aware in this software release. To use this feature, the source interface is specified and if the interface is in a VRF then the source of the TFTP or FTP will be from that VRF.
- **VPLS:** Supervisor Engine 2T supports VPLS natively in 12.2(50) SY release which is highly scalable with sub-second convergence. With a standards based approach, VPLS allows Campus LAN extensions and enables Remote DataCenter connectivity (DCI) using LAN extensions.

  VPLS is a class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP or MPLS network. VPLS presents an Ethernet interface to customers, simplifying the LAN or WAN boundary for enterprise customers and enabling rapid and flexible service provisioning, because the service bandwidth is not tied to the physical interface. All services in a VPLS network appear to be on the same LAN, regardless of location (Figure 7).

  VPLS uses edge routers that can learn, bridge, and replicate on a per-VPN basis. These routers are connected by a full mesh of tunnels, enabling any-to-any connectivity. VPLS operation emulates an IEEE Ethernet bridge.

Figure 8. DCI LAN Extension with VPLS



- **H-VPLS:** Hierarchical VPLS (H-VPLS) mode enables highly scalable bridging domains. Supervisor Engine 2T supports H-VPLS natively from 12.2(50)SY release. It also offers VLAN overlapping at the edge, which is a critical feature in multiple-tenant data centers.

Metro Technologies

Native VPLS support, EVC and E-OAM significantly enhances the value proposition for Carriers and Service Providers in Metro Ethernet deployments. Native VPLS support was discussed in the Network Virtualization Section. EVC and E-OAM features are discussed below:

- EVC Framework: 12.2(50)SY release significantly enhances the EVC services framework that comply with the MEF, IEEE and IETF standards. Features supported in this release include:
  - MST on Bridge Domains
  - Advance VLAN Translation and Service Mapping based on IEEE 802.1ah
  - IEEE 802.1ad Provider Bridges support with BPDU Handling
  - Point-to-point and multipoint EVC
- **Ethernet OAM (E-OAM):** 12.2(50)SY release supports a rich set of standards based Ethernet OAM (E-OAM) features on Sup2T

  E-OAM facilitates deployment of Ethernet services over multiple access technologies and thereby provides service independence from access and transport. The features and standards supported include:
  - IEEE 802.3ag: Connectivity Fault Management (CFM) for Untagged and QinQ, CFM with VLAN and CFM on EVC Bridge Domains
  - ITU-T Y.1731: E-OAM functions and mechanisms
  - IEEE 802.3ah support, AIS Interworking with 802.3ah
  - MEF E-LMI: Ethernet Local Management Interface
  - Cisco IP SLAs: Performance Management using IP, CFM and Y.1731 Mechanisms

Manageability

For MIB enhancements details (Table 4), visit:

- ftp://ftp-sj.cisco.com/pub/mibs/supportlists/wsc6000/wsc6000-supportlist-ios.changes/

Table 4. 12.2(50)SY MIB Enhancements

MIB
IP-MIB
IP-FORWARD-MIB
CISCO-DOT3-OAM-MIB
CISCO-BRIDGE-DOMAIN-MIB
CISCO-BRIDGE-EXT-MIB
CISCO-CALLHOME-MIB
CISCO-CAT6K-CROSSBAR-MIB
CISCO-DATA-COLLECTION-MIB
CISCO-DHCP-SNOOPING-MIB
CISCO-ENTITY-DIAG-MIB
CISCO-ENTITY-DISPLAY-MIB
CISCO-ENTITY-SENSOR-MIB
CISCO-ERR-DISABLE-MIB
CISCO-ETHERLIKE-EXT-MIB
CISCO-IGMP-SNOOPING-MIB
CISCO-LAG-MIB
CISCO-PAE-MIB
CISCO-PAGP-MIB
CISCO-SWITCH-ENGINE-MIB
CISCO-SWITCH-MULTICAST-MIB
CISCO-SWITCH-NETFLOW-MIB
CISCO-SWITCH-QOS-MIB
CISCO-SWITCH-STATS-MIB
CISCO-TRUSTSEC-INTERFACE-MIB
CISCO-TRUSTSEC-MIB
CISCO-TRUSTSEC-POLICY-MIB
CISCO-TRUSTSEC-SERVER-MIB
CISCO-TRUSTSEC-SXP-MIB
CISCO-VLAN-MEMBERSHIP-MIB
ETHERLIKE-MIB
CISCO-EVC-MIB
RFC2982-MIB
IEEE8021-PAE-MIB
IP-TUNNEL-MIB
MSDP-MIB

Additional Information

Cisco TrustSec security

- http://www.cisco.com/go/trustsec

Cisco IOS Software Information

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

Release SX and SY Information

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

Cisco IOS Software Product Lifecycle Dates and Milestones

- http:/www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd801eda8a_ps6441_Products_Bulletin.html

Cisco IOS Software Center

- Download Cisco IOS Software releases and access software upgrade planners: http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

Cisco Software Advisor (Requires Cisco.com Account)

- Determine the minimum supported software for platforms: http://tools.cisco.com/Support/Fusion/FusionHome.do

Cisco Feature Navigator (Requires Cisco.com Account)

- A Web-based application that allows you to quickly match Cisco IOS Software releases, features, and hardware: http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS Software Planner (Requires Cisco.com Account)

- View all major releases, all platforms, and all software features from a single interface: http://www.cisco.com/pcgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

Cisco Catalyst Switching Portfolio

- View the full Cisco's Catalyst Switching Portfolio in one document: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/CatalystPoster_Final.pdf

Product Management Contact

6500 Marketing Team (cco-6500-external@cisco.com)

Support

Cisco IOS Software Release 12.2(50)SY follows the standard Cisco support policy. For more information, visit:

- http://www.cisco.com/en/US/products/products_end-of-life_policy.html

Ordering Information

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center. Table 5 lists ordering information.

Table 5. Ordering Information

Product Name	Part Number
Supervisor Engines	
Cisco Catalyst 6500 Series Supervisor Engine 2T	VS-S2T-10G
Cisco Catalyst 6500 Series Supervisor Engine 2T XL	VS-S2T-10G-XL
Cisco Catalyst 6500 Series Supervisor Engine 2T Spare	VS-S2T-10G=
Cisco Catalyst 6500 Series Supervisor Engine 2T XL Spare	VS-S2T-10G-XL=
Cisco Catalyst 6500 Compact Flash Memory 1GB	MEM-C6K-CPTFL1GB
Cisco Catalyst 6500 Compact Flash Memory 1GB Spare	MEM-C6k-CPTFL1GB=
Software Parts	
Cisco CAT6000-VS-S2T IOS ADV ENT SERV FULL ENCRYPT	S2TAEK9-12250SY
Cisco CAT6000-VS-S2T IOS ADVANCED ENTERPRISE SERVICES NPE	S2TAEK9N-12250SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES FULL ENCRYPT	S2TAIK9-12250SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES LAN ONLY NPE	S2TAIK9N-12250SY
Cisco CAT6000-VS-S2T IOS IP BASE LAN ONLY FULL ENCRYPT	S2TIBK9-12250SY
Cisco CAT6000-VS-S2T IOS IP BASE LAN ONLY NPE	S2TIBK9N-12250SY
Cisco CAT6000-VS-S2T IOS IP SERV LAN ONLY FULL ENCRYPT	S2TISK9-12250SY
Cisco CAT6000-VS-S2T IOS IP SERV LAN ONLY NPE	S2TISK9N-12250SY
10 Gigabit Ethernet Fiber Modules	
Cisco Catalyst 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module with DFC4 (Requires X2)	WS-X6908-10G-2T
Cisco Catalyst 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module with DFC4XL (Requires X2)	WS-X6908-10G-2TXL
Cisco Catalyst 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module with DFC4 (Requires X2) Spare	WS-X6908-10G-2T
Cisco Catalyst 6900 Series 8-Port 10 Gigabit Ethernet Fiber Module with DFC4XL (Requires X2) Spare	WS-X6908-10G-2TXL
Cisco Catalyst 6500 Dist Fwd Card- DFC4XL Spare, for WS-X6908-10G-2T	WS-F6K-DFC4-EXL
Cisco Catalyst 6800 Series 10 Gigabit Copper, Gigabit Fiber, and Gigabit Copper Modules	
Cisco Catalyst 6800 Series 16-Port 10 Gigabit Ethernet Copper Module 4 and DFC4XL	WS-X6816-10T-2T and 2TXL
Cisco Catalyst 6800 Series 16-Port 10 Gigabit Ethernet Fiber Module with DFC4 and DFC4XL	WS-X6816-10G-2T and 2TXL
Cisco Catalyst 6800 Series 24-Port 1 Gigabit SFP Fiber Ethernet Module with DFC4 and DFC4XL	WS-X6824-SFP-2T and 2TXL
Cisco Catalyst 6800 Series 48-Port 1 Gigabit SFP Fiber Ethernet Module with DFC4 and DFC4XL	WS-X6848-SFP-2T and 2TXL
Cisco Catalyst 6800 Series 48-Port 1 Gigabit Copper Ethernet Module with DFC4 and DFC4XL	WS-X6848-TX-2T and 2TXL

Cisco Services

Cisco Services integrate closely with CMO teams as an essential element of any technology solution. If you have not already received targeted services content blocks for integration, contact your Cisco Services marcom manager. If you are not sure of the appropriate contact, send an email to ca-marcom@cisco.com.

Cisco Services make networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

For More Information

For more information about the Cisco Catalyst 6500 Series, visit the product homepage at http://www.cisco.com/go/6500 or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C25-661245-00 07/11