Cisco IOS Software Release 15.0(1)SY1 New Features and Hardware Support

PB696622

Cisco IOS® Software Release 15.0(1)SY1 supports Cisco® Catalyst® 6500 Series Supervisor Engine 2T only. Release 15.0(1)SY1 continues to extend the rich set of features from Releases 15.0(1)SY and 12.2(50)SY and adds several new software and hardware features specifically developed for Cisco Catalyst 6500 Series platforms with the Supervisor 2T.

Cisco IOS Software Release 15.0(1)SY1 is a rebuild of the extended maintenance release for the Supervisor Engine 2T. 15.0(1)SY1 does not support Cisco Catalyst 6500 VS-S720-10G-3C/3CXL or other older supervisor modules.

Cisco IOS Software Release 15.0(1)SY1 includes the following:

- Support for the Cisco Catalyst 6904 4-port 40 Gigabit Ethernet Interface Module
- Support for the Cisco Catalyst 6500 Series Network Analysis Module 3 (NAM-3)
- Support for the Cisco Catalyst 6500 Series ASA Services Module (ASA-SM)
- More than 40 new software and hardware features

There are no special memory requirements to upgrade from Release 12.2 SY to Release 15.0 SY on Cisco Catalyst 6500 Series platforms. This release follows the same rigorous test procedure as all Cisco Catalyst 6500 Series software releases and is Cisco Safe Harbor tested.

The naming convention and maintenance lifecycle for 15.0 releases is explained in the Cisco IOS Software Release Strategy document for Cisco Catalyst 6500 at: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd804f0694.html.

For detailed information about the features and hardware supported in Release 15.0(1)SY1, refer to the Cisco IOS Software Release 15.0(1)SY1 release notes and customer documentation at: http://www.cisco.com/en/US/partner/products/hw/switches/ps708/tsd_products_support_series_home.html.

New Features

New Hardware

Release 15.0(1)SY1 provides added support with Supervisor 2T for the new modules listed in Table 1.

Table 1. Supported Modules

Module Description	Part Number
Cisco Catalyst 6900 Series 4-Port 40 Gigabit Ethernet Fiber Module	WS-X6904-40G-2T WS-X6904-40G-2TXL
Catalyst 6500 Series ASA Services Module (ASA-SM)	WS-SVC-ASA-SM1-K9
Cisco Catalyst 6500 Series Network Analysis Module 3 (NAM-3)	WS-SVC-NAM3-6G-K9

Cisco Catalyst 6900 Series 40 Gigabit Ethernet Interface Module

The Cisco Catalyst 6900 Series 4-Port 40 Gigabit Ethernet Fiber Module (Figure 1) is the first 40 Gigabit Ethernet Module for the Cisco Catalyst 6500 Series Switch and fully supports IEEE 802.3ba. The 6900 Series 4-port 40 Gigabit Ethernet Fiber Module works only with Supervisor Engine 2T-based systems at 80 Gbps per slot and offers outstanding Layer 2 and Layer 3 features and flexibility for Cisco Catalyst 6500 Series customers. These features include:

- 40 Gigabit Ethernet Oversubscribed mode (default).
  - Four 40 Gigabit Ethernet ports using CFP transceivers.
- 10 Gigabit Ethernet Oversubscribed mode.
  - 16 10 Gigabit Ethernet ports using FourX adapters.
  - Each FourX adapter has 4 SFP+ transceivers.
- Mixed 10/40 Gigabit Ethernet mode.
  - One-half of the module uses two CFP transceivers for 2 x 40 Gigabit Ethernet ports, while the other half uses two FourX adapters for 8 x 10 Gigabit Ethernet ports.
- Virtual Private LAN Service (VPLS) on every port.
- Security: Layer 2 and Layer 3 CiscoTrustSec™ technology Security Group Tags and Security Group Access Control Lists (SGT & SGACL) and wired rate IEEE 802.1ae (MACsec) Layer 2 encryption in hardware.
- 40 Gigabit Ethernet C Form-Factor Pluggable (CFP) optics module.
- 10 Gigabit Ethernet mode via FourX adapter, which converts each 40 Gigabit Ethernet port to 4 Small Form-Factor Pluggable Plus (SFP+) ports.
- Virtual Switch Link (for Virtual Switching System [VSS]).
- Supports Cisco Generic Online Diagnostics (GOLD).

Figure 1. Cisco Catalyst 6900 Series 4-Port 40 Gigabit Ethernet Fiber Module

For more information on Cisco GOLD, visit: http://www.cisco.com/en/US/products/ps7081/products_ios_protocol_group_home.html.

Cisco Adaptive Security Services Module

The Cisco Adaptive Security Appliance Services Module (ASA-SM) for the Cisco Catalyst 6500 Series delivers superior technology that seamlessly integrates with Cisco Catalyst 6500 Series switches to provide unmatched security, reliability, and performance. Based on the Cisco ASA platform, the most widely deployed firewall in the industry, the Cisco ASA-SM supports the highest throughput, five times the concurrent connections, and twice as many connections per second as competitive network security modules, to meet the growing needs of today's most dynamic organizations - all in a single-blade architecture.

The ASA-SM makes it easy to add full firewall capabilities to an existing infrastructure by sliding a blade into an empty slot in an existing Cisco Catalyst 6500 Series Switch. No additional rack space, cabling, power, or physical interface is required (Figure 2). It also works in tandem with other modules in the chassis to deliver robust security throughout the entire chassis, effectively making every port a security port. The ASA-SM delivers superior return on investment (ROI) and greatly simplifies maintenance and management.

Figure 2. Cisco ASA Services Module

For more information on Cisco Adaptive Security Appliance Services Module (ASA-SM), visit: http://www.cisco.com/en/US/products/ps11621/index.html.

Cisco Network Analysis Module 3 (NAM-3)

The Cisco Catalyst 6500 Series Network Analysis Module 3 (NAM-3) (Figure 3) provides unparalleled network and application visibility to simplify operational manageability of network resources in enterprise campus, data center, and WAN deployments of multiple Gigabit Ethernet. NAM-3 allows users to optimize network resources and deliver consistent application performance to help ensure that network performance meets the rigorous demands of the business. The module also reduces the time required to find and resolve problems from days to minutes.

Figure 3. Cisco Network Analysis Module 3 (NAM-3)

For more information on the Cisco NAM-3 Module, visit: http://www.cisco.com/en/US/partner/products/ps11659/index.html.

Hardware Innovations

New features of the hardware abstraction layer (HAL) are as follows:

- This solution allows seamless insertion of future new line cards without new supervisor software
- New transceiver types can be used with existing software with just an update

Software Innovations

Software innovations span multiple technology areas, including high availability with bidirectional forwarding detection (BFD) and graceful restart, Flexible NetFlow, network virtualization, optimized media delivery, and IPv6.

Network Virtualization and Routing

Cisco Easy Virtual Networks

Cisco Easy Virtual Network (EVN) enables traffic separation based on role or group policies - between different departments, to enable vendors to share selected resources, or to restrict access during mergers and acquisitions. This practice is often called network virtualization. Several well-adopted solutions are available, but they can be difficult to deploy and manage. EVN simplifies the process by creating separate logical networks on a single physical infrastructure, each with different security and routing polices, traffic separation, and path isolation. EVN takes advantage of existing protocols, along with virtual routing and forwarding (VRF) technology, in a complete network virtualization solution with shared services and enhanced management. Features of this technology include:

- EVN (VNET) trunk
- OSPF and EIGRP routing protocol support
- Routing Context support
- Shared Services support
- Multicast support
- EVN MIB and Multicast MIB VRF

EIGRP IPv6 VRF-Lite

The Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 VRF-Lite feature provides EIGRP IPv6 support for multiple VRFs. EIGRP for IPv6 can operate in the context of a VRF. The EIGRP IPv6 VRF-Lite feature provides separation between routing and forwarding, resulting in an additional level of security because no communication between devices belonging to different VRFs is allowed unless it is explicitly configured. The EIGRP IPv6 VRF-Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF. This feature allows routing inside a VPN using EIGRPv6. EIGRP 6PE/6VPE is not included with this current enhancement.

For more information on EIGRPv6, visit:
http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html.

OSPF for IPv6 (OSPFv3) Authentication Support with IPsec

The Open Shortest Path First (OSPF) feature allows routers to secure their neighbor adjacencies with IPv6.

In order to ensure that OSPFv3 packets are not altered and resent to the router, causing the router to behave in a way not desired by its managers, OSPFv3 packets must be authenticated.

OSPFv3 requires the use of IP Security (IPsec) to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec needed for use with OSPFv3.

For more information on OSPFv3 security, visit:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html.

Multicast mVPN Support with MPLS VPN over mGRE

Multicast mVPNs are now supported with the Layer 3 VPN over multi-point GRE (mGRE) feature.

This feature allows multicast within VRFs to be transmitted over IP so that the VRFs are relevant at remote locations. This extends network virtualization across the WAN and allows multicast media to stay segregated within the VRF-over-IP portions of the network.

For more information on Layer 3 VPN over mGRE, visit:
http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_mplsvpnomgre.html.

Enhanced IPv6 Neighbor Discovery Cache Management

Improvements and optimizations were made with this feature to allow customers to scale their IPv6 networks to a larger number of neighbor discovery entries.

For more information on the IPv6 enhancements, visit:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/features.html#wp4808396.

Security

Cisco TrustSec Technology

This release enhances Cisco TrustSec™ technology on Cisco Catalyst 6500 Series Switches with advanced features geared to improve deployment of 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 checks, and data-path replay protection mechanisms.

Cisco TrustSec technology 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.

Because the SGT contains the security group of the source, the tag can be referred to as the source SGT. The destination device is also assigned to a security group (the destination SG) that can be referred to for simplicity as the destination group tag (DGT), although the actual Cisco TrustSec packet tag does not contain the security group number of the destination device. The egress network device must determine the SGT of the packet in order to apply an SG access control list (ACL).

With Cisco IOS Software Release 15.0(1)SY1, several features were added to get the SGT and DGT of a packet:

- **Layer 3 Identity Port Mapping:** Look up source SGT is based on the source identity. Identity Port Mapping (IPM) enables manual configuration of the Layer 3 link with the identity of the connected peer. The network device requests policy information, including SGT and trust state, from the authentication server.
- **Cisco TrustSec VLAN to SGT Mapping:** Look up the source SGT based on the source VLAN.
  The VLAN-SGT mapping feature is intended to be used in two primary scenarios. The first is to help with the backward compatibility with existing VLAN segmented environments. As VLANs are frequently used for segmentation of network devices, SGTs will be compatible with these configurations and allow for easy

migration. The second case is to help deploy SGT with equipment that is not capable of SGT tagging but is VLAN capable - for example, wireless controllers or access points and legacy switches.

- **Cisco TrustSec Subnet to SGT Mapping:** Just as with the VLAN-SGT mapping feature, VLANs or routed subnets are commonly used for asset segmentation. Subnet-SGT mapping allows for ease of migration and ease of use. Both IPv4 and IPv6 are supported.

For more information on Cisco TrustSec, visit: http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html.

IPv6 VACL

VACLs can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN or a WAN interface for VACL capture. Unlike the regular Cisco IOS Software standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, VACLs apply to all packets and can be applied to any VLAN or WAN interface. VACLs are processed in hardware. IPv6 VACLs are also used in IPv6 First Hop Security configurations.

High Availability

BFD Support for VRF

BFD support for VRF enables fast failure detections of the routing protocols between the service provider and the enterprise networks. Service providers can serve multiple customers over a shared customer edge (CE) router using distinct routing domains per customer by way of VPN Routing and Forwarding (VRF) technology. Both the Provider Edge (PE) and CE routers can advertise routes contained within their global and VRF routing tables using protocols such as Border Gateway Protocol (BGP). As the availability of these technologies increases in service provider networks, the need for maintaining a secure, highly available VPN service for customers is increasingly important. BFD on VRF capable interfaces allows for fast detection of routing protocol failures between PE and CE routers over a single hop.

For more information, visit: http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html.

Fast UDLD

Unidirectional Link Detection (UDLD) enables automatic detection of bidirectional communication failures on Layer 2 fiber and copper links by sending messages at time intervals between 7 and 90 seconds. With the increasing requirements to run highly reliable enterprise networks, there is a need to detect Layer 2 link failures in subseconds and to minimize false positives due to control plane instabilities. Fast UDLD optimizes the time intervals to between 200 and 1000 milliseconds, providing a per-port configuration option that enables unidirectional link detection in subseconds. For more information, visit: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html#wp1040116.

BFD for Static Routes over IPv4

Bidirectional Forwarding Detection (BFD) for static routes provides failure detection capabilities for statically defined routes in a network. One of the characteristics of static routes is that traffic does not get rerouted upon changes in the network or failures between two statically defined nodes. A typical scenario occurs when the gateway in a static route goes down while the interface stays up, resulting in the static route not being removed from the Routing Information Base (RIB). BFD for static routes helps detect such failures, thereby preventing traffic from getting black-holed. This feature currently supports directly connected gateways reachable through a single hop.

For more information, please visit: http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1097340.

Static Route Support for BFD over IPv6

The prior IPv6 static route model allowed static route insertions in the IPv6 Routing Information Base (RIB) when the associated interface is both up and administratively enabled for IPv6. The static route support for the BFD over IPv6 feature helps to ensure that next-hop reachability is considered before traffic is directed out, preventing situations where traffic is sent to an unreachable neighbor. In addition to support for configuration, debugging of IPv6 Static BFDv6 Neighbors will provide automatic association between the IPv6 Static Route and IPv6 Static BFDv6 Neighbor. For more information, visit: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes.html#wp1027184.

VSS Multicast Fast Redirect

VSS Multicast Fast Redirect is a best-effort solution to reduce multicast traffic loss when member ports of a Layer 2 trunk Multichassis EtherChannel (MEC), connected to a physical chassis within a VSS domain experience a link flap event. Prior to the availability of this feature, a VSS multicast system in egress replication forwarding mode, could experience a significant traffic disruption upon a member port flap of the MEC. The traffic disruption is based on the number of multicast groups joined from the VLANs carried by the MEC during events such as switchover or single-chassis reload. The traffic disruption is primarily due to the computational overhead involved in reactively programming the line card interface ports. VSS Multicast Fast Redirect enhances the convergence time for the multicast traffic by proactively reprogramming all the pertinent hardware shortcuts on the line card interfaces.
For more information, visit: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Multicast_Protocols.

Other features supported in this release include the following:

- OSPF SNMP if Index Value for Interface ID
- Sup2T NVRAM Battery Monitor GOLD test
- Cisco Wireless Services Module 2 (WiSM2) 1000 Access Point Support (previously 500 access points were supported)
- VRF-Lite aware NAT for nonoverlapping IP addresses
- IPv6 Route Health Injection (IPv6 RHI) on Cisco ACE 30 Application Control Engine

Network Management

Flexible NetFlow - 32-Bit AS Number Support

One of the current scaling properties of the Border Gateway Protocol (BGP) routing protocol is the autonomous system (AS) numbers. The higher number of domains, as well as interdomain interconnection density, drove the increase of the size of the AS number pool space from 16 to 32 bits.

With Cisco IOS Release 15.0(1) SY1, Flexible NetFlow supports 32-bit AS numbers. Flexible NetFlow can capture and export 32-bit numbers as well as 16-bit numbers. The 32-bit AS numbers have a different v9 export type than that used for 16-bit AS numbers. The collector and analysis infrastructure can process values for 32-bit AS numbers.

Manageability

MIB enhancements in Cisco IOS Release 15.0(1)SY1 include:

- CISCO-HW-MODULE-CONTROL-MIB
- CISCO-INTERFACETOPN-EXT-MIB
- CISCO-UDLDP-MIB
- Easy Virtual Network MIB and context-based SNMP simplification
- Multicast MIB VRF support

For more information about these enhancements, visit: ftp://ftp-sj.cisco.com/pub/mibs/supportlists/wsc6000/wsc6000-supportlist-ios.changes/.

Additional Information

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

Cisco IOS Software Information

- http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.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 users 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 15.0(1)SY1 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 2 lists ordering information for Cisco IOS Software Release 15.0(1)SY1.

Table 2. Cisco IOS Software Release 15.0(1)SY1 Ordering Information

Product Name	Part Number
Cisco CAT6000-VS-S2T IOS ADV ENT SERV FULL ENCRYPT	S2TAEK9-15001SY
Cisco CAT6000-VS-S2T IOS ADVANCED ENTERPRISE SERVICES NPE	S2TAEK9N-15001SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES FULL ENCRYPT	S2TAIK9-15001SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES NPE	S2TAIK9N-15001SY
Cisco CAT6000-VS-S2T IOS IP SERV FULL ENCRYPT	S2TISK9-15001SY
Cisco CAT6000-VS-S2T IOS IP SERV NPE	S2TISK9N-15001SY
Cisco CAT6000-VS-S2T IOS IP BASE FULL ENCRYPT	S2TIBK9-15001SY
Cisco CAT6000-VS-S2T IOS IP BASE NPE	S2TIBK9N-15001SY

For More Information

For more information about the Cisco Catalyst 6500 Series, visit the product home page 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 C25-696622-01 11/13