Cisco IOS Software Release 15.1(1)SY for Cisco Catalyst 6500 Series Switches

Cisco IOS® Software Release 15.1(1)SY is the first converged software release for Cisco® Catalyst® 6500 Series Switches that supports Cisco Catalyst 6500 Series Supervisor Engine 2T (Sup2T) and Cisco Catalyst 6500 Series Supervisor Engine 720 (Sup720-3B and Sup720-10G). Some features might perform better on systems running Sup2T, as they are supported in hardware on the supervisor.

Release 15.1(1)SY adds more than 175 new features for Cisco Catalyst 6500 switches:

- **Cisco Catalyst SmartOperations** features to lower operating costs, including the ability of the Catalyst 6500 to serve as a Smart Install director, dramatically simplify the deployment of downstream switches by controlling Cisco IOS Software images and configurations.
- **More granular application visibility and control features**, including IPv6 bridged flows, IP-aware Multiprotocol Label Switching (MPLS) NetFlow in hardware on Sup2T, medianet metadata, and hierarchical shaping and queuing, which together improve performance, user experience, and monitoring.
- **Resiliency improvements** to optimize business continuity, including nonstop routing, nonstop forwarding, stateful switchover, and graceful restart features.
- **Cisco TrustSec™ security enhancements** to improve end-to-end deployments, including Security Group Tag (SGT) caching to facilitate secure transport across deep packet inspection services and Monitor Mode to enable simulation and testing of access control policies before deployment.

For detailed information about the features and hardware supported in Release 15.1(1)SY, refer to the Cisco IOS Software Release 15.1(1)SY release notes and customer documentation at http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.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.

Supervisor Engine 2T Hardware Support in Release 15.1(1)SY

Cisco IOS Software Release 15.1(1)SY adds support for the following hardware with Sup2T:

- Power over Ethernet/Power over Ethernet Plus (PoE/PoE+) support for WS-X6148E-GE-45AT in VSS mode
- 61xx line cards in standby supervisor slot of 6513-E chassis
- CISCO7613-S
- CISCO7604

New Transceivers

X2-10GB-T:

The Cisco 10GBASE-T module supports link lengths of up to 100m on CAT6A or CAT7 copper cable. Support on Supervisor2T, WS-X6908-10G-2T and WS-X6816-10G-2T.

SFP+ LRM:

Support on Supervisor2T, WS-X6908-10G-2T and WS-X6816-10G-2T with OneX adapter and on WS-X6904-40G-2T with FourX adapter.

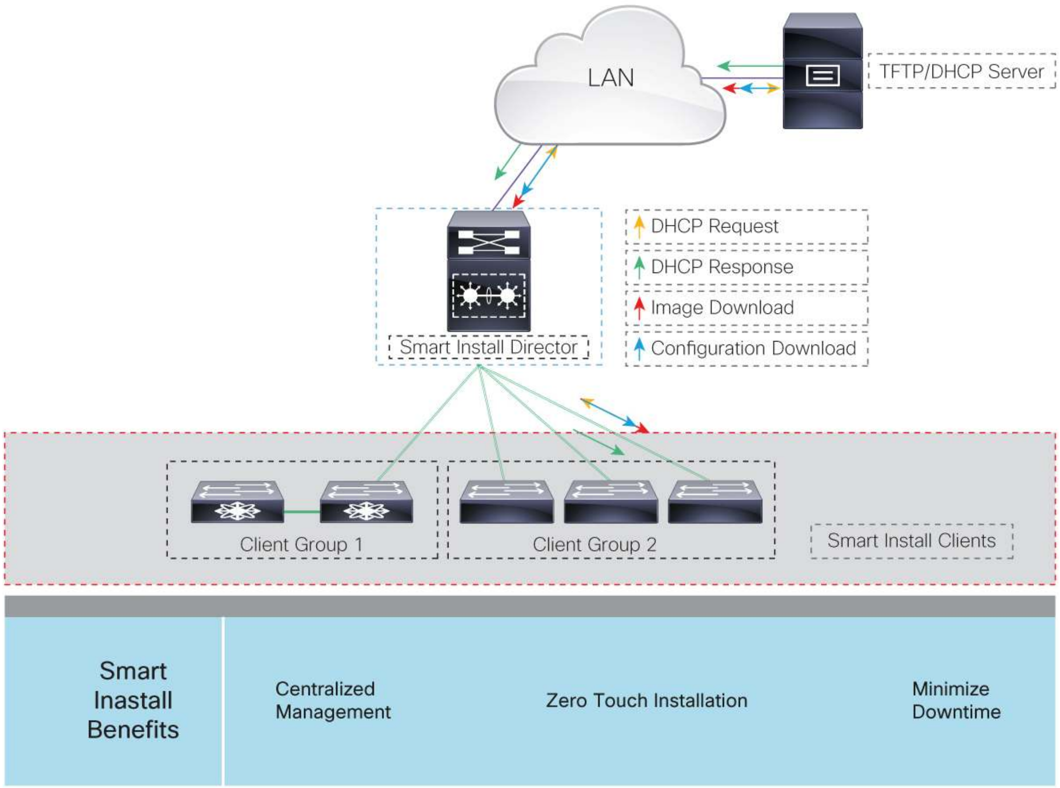
Software Feature Highlights of Release 15.1(1)SY

SmartOperations

- Smart Install

  Smart Install is a part of Cisco Catalyst 6500 Smart Operations that is supported on Supervisor Engine 2T. It consists of a set of tools, capabilities, and available management applications to simplify deployment, management, and troubleshooting of Cisco networks. Smart Install provides a single point of management, zero-touch deployment, replacement, and automatic configuration backups with minimal downtime. Cisco Smart Operations help reduce overall operating expenses.

Smart Install Director



Application Performance

- Flexible NetFlow

  Flexible NetFlow (FNF) is the next generation in flow technology. It allows optimization of the network infrastructure, reduced operation costs, and improved capacity planning and security incident detection with increased NetFlow flexibility and scalability beyond other flow-based technologies available today.

The following new Flexible NetFlow feature enhancements are being introduced in Release 15.1(1)SY for the Cisco Catalyst 6500 Series Switch:

- Flexible NetFlow: IPv6 Bridged Flows

  The Supervisor Engine 2T for the Cisco Catalyst 6500 Series Switch supports IPv6 bridged flows in hardware. With IPv6 bridged flows, the network administrator can get IPv6 traffic information on an L2 trunk/access interface. This feature enables NetFlow accounting for L2 switched/bridged IPv6 traffic. Most of the key and nonkey fields that are matched and collected on IPv6 routed flows today through FNF can be applied to the bridged flows. Bridged flow accounting can be applied only on the ingress interface.

- IP-Aware MPLS NetFlow

  NetFlow is already supported on provider edge (PE) devices. With this new functionality you will get full visibility across your MPLS backbone. The big value add is the end-to-end visibility that was missing on the PE router before. It provides IPv4 information from the MPLS packet.

- NetFlow (TNF) Export L2 MAC and Port Information for IPv4

  This feature gives you a way to find out the NetFlow information for destination and source MAC address along with the port LTL. This is useful when a bot on the network is spoofing the IP address. We will be able to track this down with the MAC address using NetFlow.

- NetFlow Data Export to a Collector in VRF

  NetFlow data export to a collector in virtual routing and forwarding (VRF) allows you to export the NetFlow records to a collector in a VRF.

- Control Plane Policing (CoPP) Microflow Policing

  Sup2T supports microflow policing in hardware. It provides ability to configure microflow policers on CPU-bound traffic. This prevents one rogue device in a group to cause a denial of service for good devices in a group for CPU cycles.

- Medianet Metadata

  Metadata provides explicit information about client needs to the network to enable the application. It identifies flows with the application and provisions network resources for the applications. Metadata-based classification makes the quality-of-service (QoS) policy flow aware and allows users to apply different QoS policy actions to a specific flow or group of flows. It allows users to classify flows in terms of intuitive user-friendly metadata attributes instead of individual flow identifiers.

- Hierarchical Shaping and Two Priority Queues on WS-X6904-40G-2T

  Sup2T supports two-level hierarchical QoS (HQoS) with the 6904 line cards. HQoS MQC policies can contain other “nested” QoS policies within them. Such policy combinations are commonly referred to as hierarchal QoS policies, or HQoS policies. HQoS policies can be constructed within MQC by attaching the service-policy command to a per-class action within a policy map, rather than to an interface.

Table 1 lists additional new application performance features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 1. New Features and Enhancements

Copy-based sampling
Shaping on priority queue
Estelle: per-queue forwarding counters
RSVP support for ingress call admission control
Medianet 2.2 features in Cat6500 IP Base images

Resiliency

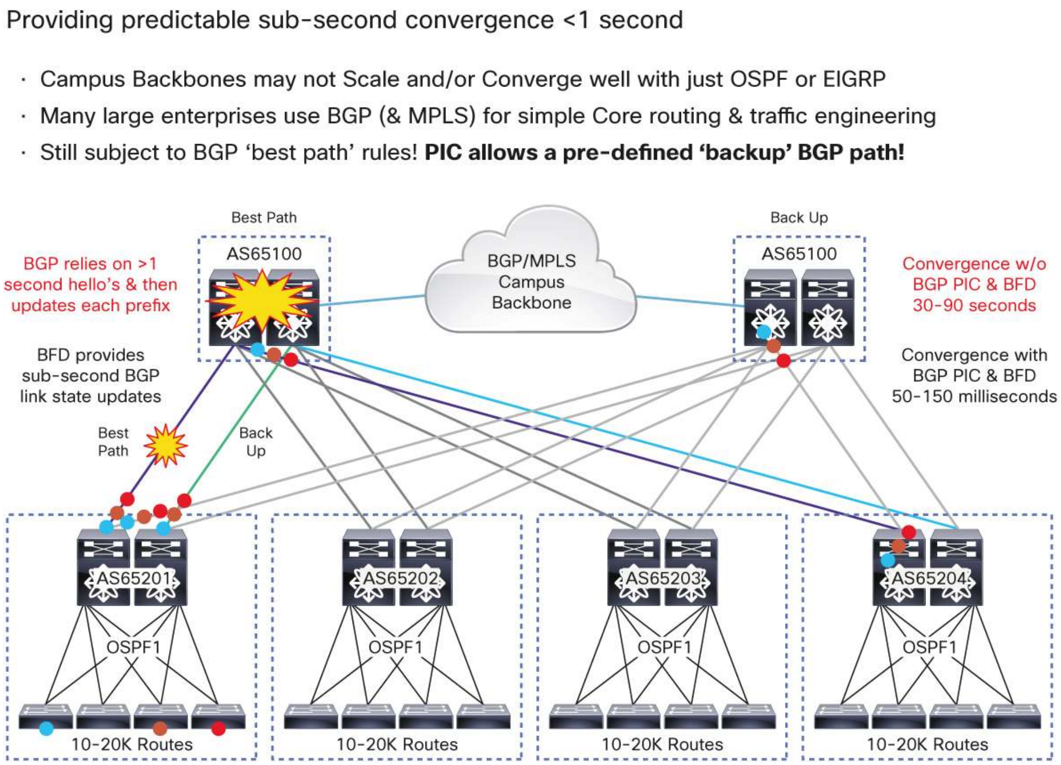
- IP Tunnel: SSO

  Currently IPv4 and IPv6 tunnels do not support stateful switchover (SSO). The IP tunnel SSO feature provides SSO for IPv4 and IPv6 tunnels on switchover. Nonstop forwarding (NSF) with SSO increases network availability. 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.

- BGP PIC Edge and Core for IP/MPLS

  Border Gateway Protocol (BGP) convergence during the BGP peer change is not scalable. When a large number of prefixes are involved in the BGP table, the withdrawal from the local peer might reach the remote peer after a few seconds. This means that convergence time for finding an alternative path for BGP prefixes is not prefix independent. The BGP prefix-independent convergence (BGP PIC) edge for IP and MPLS-VPN feature provides faster convergence after a network failure by storing not only a best path but also a backup path in the FIB table, so when a failure is detected, a backup path can immediately take over, thus enabling fast failover with minimal traffic loss. BGP PIC edge feature enables fast convergence when a BGP neighbor itself has changed caused by link or node failure that disrupts reachability to a given peer.

  The BGP PIC core feature provides subsecond BGP convergence when a BGP neighbor stays the same after a link, path, or node failure in the core but the Interior Gateway Protocol (IGP) recurse-via path has changed.



Providing predictable sub-second convergence <1 second

- Campus Backbones may not Scale and/or Converge well with just OSPF or EIGRP
- Many large enterprises use BGP (& MPLS) for simple Core routing & traffic engineering
- Still subject to BGP 'best path' rules! **PIC allows a pre-defined 'backup' BGP path!**

For more information, visit http://www.cisco.com/en/US/docs/iosxml/ios/iproute_bgp/configuration/15-0s/irg-bgp-mp-pic.html.

- BFD: Static Route Support

  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 blackholed. This feature currently supports directly connected gateways reachable through a single hop.

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

- BFD: VRF Support

  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 VRF technology. Both PE and CE routers can advertise routes contained within their global and VRF routing tables using protocols such as 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.

- BFD Support over Port Channel

  BFD support over port channel extends the benefit of BFD to port channel for better convergence with fast fault detection. With the introduction of BFD over port channels, customers can make use of the high-availability benefits of a fast detection mechanism to help their networks converge quickly.

- BFD IPv6 Encaps Support

  BFD support is extended for IPv6 addresses. This feature improves overall network availability for IPv6 networks. BFD IPv6 encaps support gives the ability to create IPv6 BFD sessions with IPv6 routing protocols. It allows IPv6 encapsulation support for IPv6 BFD clients (for example, Open Shortest Path First Version 3 [OSPFv3] and IPv6 static routes clients).

- BFD over SVI

  Networks where two Layer 3 endpoints are connected over Layer 2 network and SVI is used to provide Layer 2 access networks to Layer 3 routing domain do not have a mechanism of detecting failures in subseconds. The BFD over SVI feature provides faster device failure detection and switchover at Layer 3 device connected through an SVI by Layer 2 aggregated switchports. This feature provides a mechanism to achieve subsecond failovers.

- IPv6: NSF and Graceful Restart for MP-BGP IPv6 Address Family

  IPv6 NSF and graceful restart for MP-BGP IPv6 address family feature allows IPv6 MP-BGP to use Cisco NSF and graceful restart (GR) to allow a route processor (RP) to recover from a disruption in control plane service without losing its IPv6 MP-BGP forwarding state. In case of primary processor hardware or software failure, the secondary processor maintains control plane service in a redundant system, and NSF with SSO provides packet forwarding during the failure.

  The graceful restart capability is supported for IPv6 BGP unicast, multicast, and VPNv6 address families, enabling Cisco NSF functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state. NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover. Forwarding is maintained by synchronizing the FIB between the active and standby RP. On switchover, forwarding is maintained using the FIB.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/ip6-mbgp-nsf-gr-rest.html.

- OSPFv2 NSR

  OSPF nonstop routing (stateful failover) for OSPF Version 2 RFC-2328. This feature allows OSPF to fail over to a redundant processor or Cisco IOS Software process and continue operating without any assistance from neighboring OSPF routers. Unlike the existing NSF methods, this will not require the neighboring routers to implement features beyond the baseline RFC 2328 OSPF protocol, and the neighbors should see no change to their forwarding state when a failover occurs. This feature will be useful when a peer router is from a third party that does not support NSF/SSO.

- OSPF Graceful Shutdown

  The OSPF graceful shutdown feature provides the ability to temporarily shut down the OSPF protocol in the least disruptive manner and notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path. A graceful shutdown of the OSPF protocol can be initiated using the shutdown command in router configuration mode.

  This feature also provides the ability to shut down OSPF on a specific interface. In this case, OSPF will not advertise the interface or form adjacencies over it; however, all of the OSPF interface configuration will be retained. To initiate a graceful shutdown of an interface, use the ip ospf shutdown command in interface configuration mode.

- OSPFv3 Graceful Restart

  The graceful restart feature in OSPFv3 allows nonstop data forwarding along routes that are already known while the OSPFv3 routing protocol information is being restored. A device can participate in graceful restart either in restart mode (such as in a graceful-restart-capable router) or in helper mode (such as in a graceful-restart-aware router).

  To perform the graceful restart function, a device must be in high availability (HA) SSO mode (that is, dual RP). A device capable of graceful restart will perform the graceful restart function when one of the following failures occur:

  - An RP failure that results in switchover to standby RP
  - A planned RP switchover to standby RP

  The graceful restart feature requires that neighboring devices be graceful-restart aware.

  The OSPFv3 LSA and SPF throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability. It also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds.

Table 2 lists more new high-availability features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 2. New Features and Enhancements

OSPFv3 BFD
BFD support for IP tunnel (generic routing encapsulation [GRE], with IP address)
ISIS BFD TLV
ISIS client for BFD c-bit support
ISIS IPv6 client for BFD
HA support for mLDP
NSF/SSO: IPv6 multicast
SSO: MPLS VPN 6VPE and 6PE SSO support
LACP 1:1 hot standby dampening

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 IOS Software Release 15.1(1)SY enables support for the following Cisco TrustSec features:

- Cisco TrustSec SGT Caching

  Deployments that utilize services such as deep packet inspection (DPI) are today SGT unaware. In order to provide end-to-end security through the Cisco TrustSec solution, SGT will need to be transported across these services in the infrastructure. SGT caching enables this functionality wherein when tagged packets arrive, SGT is removed and cached. Untagged packets are sent to DPI services. Upon receipt from DPI at the egress, packets are retagged with appropriate SGT.

- Cisco TrustSec SXP Loop Detection

  SGT Exchange Protocol (SXP) connections can be enabled such that the binding forwarded by one switch for an SXP connection can be received from another SXP connection, resulting in SXP connection loops. SXP loop topology might result in stale binding in the network. SXPv4’s built-in loop detection and prevention mechanism address the stale binding issue whenever there is a loop between SXP nodes.

- SGACL Monitor Mode (Dry Run)

  The SGACL monitor mode feature enables the network administrator to simulate whether an SGACL policy would have the intended effect before deploying the actual SGACL policy.

  This feature gives visibility to the outcome of the SGACL policy actions before enforcement and confirmation that the subject policy meets the business need (deny access to resources if the individuals are not authorized).

- No Service Password-Recovery

  The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM.

Table 3 lists additional new security features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 3. New Features and Enhancements

Cisco TrustSec SGA environment: data change of authority
Cisco TrustSec SGA SGACL policy change of authority
Cisco TrustSec subnet to SGT mapping
Cisco Express Forwarding: Simple Network Management Protocol (SNMP) CEF-MIB support
Cisco TrustSec security group name download
Cisco TrustSec L3 identity port mapping
Client Information Signaling Protocol (CISP)
Password strength and management for Common Criteria
IEEE 802.1x: RADIUS change of authorization (CoA)
RADIUS statistics using SNMP
RADIUS per-VRF server group

IPv6

- IPv6 ACL Extensions for Hop-by-Hop Filtering

  The IPv6 ACL extensions for hop-by-hop filtering feature allows you to control IPv6 traffic that might contain hop-by-hop extension headers. You can configure an access-control list (ACL) to deny all hop-by-hop traffic or to selectively permit traffic based on protocol.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/xe-3s/ip6-acl-ext-hbh-xe.html.

- IPv6 Policy-Based Routing

  IPv6 policy-based routing allows a user to manually configure how received packets should be routed. PBR allows the user to identify packets using several attributes and to specify the next hop or output interface to which the packet should be sent. PBR also provides a basic packet-marking capability.

- IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec

  This feature is intended to secure OSPFv3 traffic using IPsec. OSPF traffic is a mix of unicast and multicast. Manual security associations will be installed on software crypto engine to secure this traffic.

  In order to make sure 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 uses the IP Security (IPsec) secure socket application program interface (API) to add authentication to OSPFv3 packets. This API has been extended to provide support for IPv6.

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

- OSPFv3 IPsec ESP Encryption and Authentication

  IPv6 ESP extension headers can be used to provide authentication and confidentiality to OSPFv3.

- Static Route Support for BFD over IPv6

  The prior IPv6 static route model allowed static route insertions in the IPv6 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 make sure 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.

Table 4 lists additional new IPv6 features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 4. New Features and Enhancements

IPv6 device tracking
IPv6 router advertisement (RA) guard
IPv6 per-interface neighbor discovery cache limit
IP over IPv6 tunnel
IPv6 neighbor discovery inspection
IPv6 neighbor discovery NSF
IPv6 TCL

IPv6 config logger
IPv6 HTTP(S)
LLDP IPv6 address support
DEPRECATE ipv6ip auto-tunnel
IPv6 support for IPsec and IKEv2
Manually configured IPv6 in IPv4 with IPsec
IPv6 neighbor discovery NSF

IP Routing

- BGP Event-Based VPN Import

  The BGP event-based VPN import feature introduces a modification to the existing BGP path import process. BGP virtual private network (VPN) import provides importing functionality for BGP paths where BGP paths are imported from the BGP VPN table into a BGP VRF topology. In the existing path import process, when path updates occur, the import updates are processed during the next scan time, which is a configurable interval of 5 to 15 seconds. The scan time adds a delay in the propagation of routes. The enhanced BGP path import is driven by events; when a BGP path changes, all of its imported copies are updated as soon as processing is available.

  Using the BGP event-based VPN import feature, convergence times are significantly reduced because PE routers can propagate VPN paths to CE routers without the scan time delay. Configuration changes such as adding imported route targets to a VRF are not processed immediately and are still handled during the 60-second periodic scanner pass.

- BGP Best External

  BGP best external provides a faster convergence for prefixes with multiple path reachability when a single path from the multipath list becomes inaccessible. BGP best external is an extension to BGP PIC. It forces a BGP peer to continue announcing its best external path even in case a better path is received using iBGP. This helps in MPLS VPN networks where customers can use BGP communities and BGP local_pref to deploy active/standby routing design and each BGP router has at least have two BGP paths for each prefix to make sure of prefix-independent BGP convergence using inplace modification.

- BGP Remove/Replace Private AS Filter

  The BGP remove/replace private AS filter feature provides the ability for customers to remove/replace private AS numbers in the as-path from outgoing BGP updates.

  For more information, visit http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_remove_as_xe.html.

- BGP per Neighbor SOO Configuration

  The BGP per neighbor SoO configuration feature simplifies the configuration of the site-of-origin (SoO) value. Per neighbor SoO configuration introduces two new commands that can be used under router configuration mode to set the SoO value.

  For more information, visit http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htbgpsoo.html.

- EIGRP Wide Metrics

  The EIGRP composite metric is not scaled correctly for high-bandwidth interfaces, resulting in incorrect or inconsistent routing behavior. 10GE or EtherChannel interfaces appear as a single GE to EIGRP. This might cause undesirable equal cost load balancing. The EIGRP wide metrics feature improves route selection on higher speed interfaces or bundled interfaces. This feature provides ability to support interfaces (either directly or using channeling techniques such as port-channels or ether-channels) up to approximately 4.2 terabits. Routers supporting wide metrics can interoperate with routers that do not support wide metrics.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-1s/config-eigrp.html.

- EIGRP IPv6 VRF-Lite

  The 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, providing 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.

- OSPF TTL Security Check

  The OSPF support for TTL security check feature provides an effective and easy-to-deploy solution to protect OSPF neighbor sessions from CPU utilization-based attacks. When this feature is enabled, a host cannot attack an OSPF session if the host is not a member of the local or remote OSPF network or if the host is not directly connected to a network segment between the local and remote OSPF networks. This solution greatly reduces the effectiveness of denial of service (DoS) attacks against an OSPF autonomous system.

- OSPFv2 Local RIB

  With the OSPFv2 local RIB feature, each OSPF protocol instance has its own local RIB. The OSPF local RIB serves as the primary state for OSPF SPF route computation. The global RIB is not updated with intermediate results during the SPF. Instead, the global RIB is updated only when routes are added, deleted, or changed, thereby reducing global RIB computation. This reduced update activity might result in fewer dropped packets.

- OSPF for Routed Access

  OSPF for routed access is designed specifically to enable customers to extend Layer 3 routing capabilities to the access or wiring closet.

  OSPF for routed access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.

  With the typical topology (hub and spoke) in a campus environment, where the wiring closets (spokes) are connected to the distribution switch (hub) forwarding all nonlocal traffic to the distribution layer, the wiring closet switch need not hold a complete routing table. A best practice design, where the distribution switch sends a default route to the wiring closet switch to reach interarea and external routes (OSPF stub or totally stubby areas configuration), should be used when OSPF for routed access is used in the wiring closet.

  For more information, visit http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html.

- OSPFv3 Address Families

  Previously OSPFv3 supported IPv6 unicast address family only. With the introduction of the OSPFv3 address families feature, OSPFv3 can now support IPv4 and IPv6 address families on a single network infrastructure. It enables IPv4 and IPv6 multicast and unicast traffic to be supported with a single network topology. This feature simplifies configuration management for the networks running dual stack, eliminates the need to maintain parallel networks, and protects an organization's IPv4 technology investment.

  For more information, visit http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps6629/whitepaper_c11-668030.html.

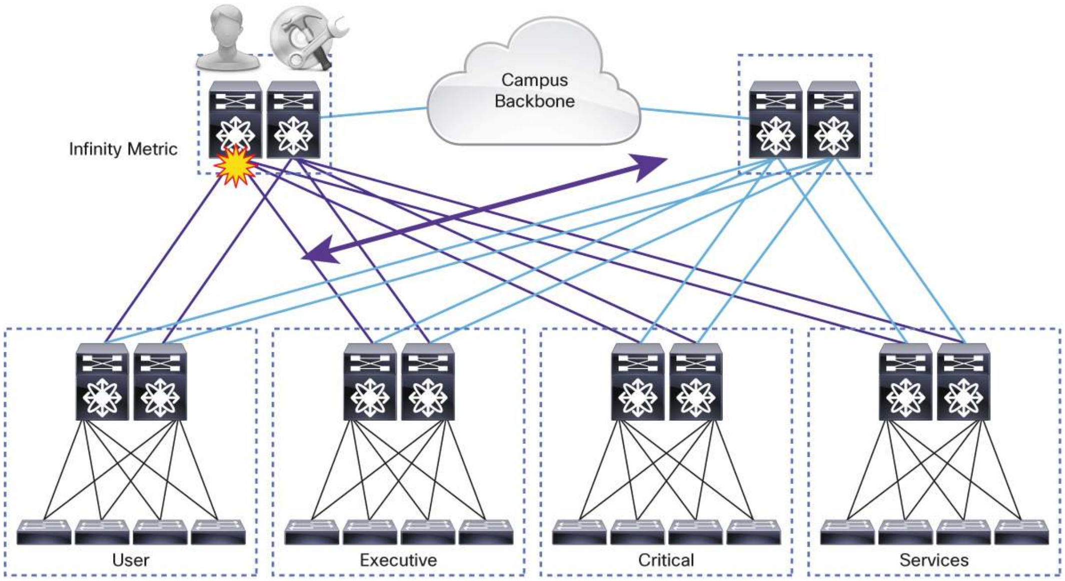
- OSPFv3 Max-Metric Router-LSA

  The OSPFv3 max-metric router LSA feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through the router if there are better alternate paths. After a specified timeout or a notification from BGP, OSPFv3 advertises the LSAs with normal metrics.

  The max-metric LSA control places the OSPFv3 router into the stub router role using its LSA advertisement. A stub router only forwards packets destined to go to its directly connected links. In OSPFv3 networks, a router could become a stub router by advertising large metrics for its connected links, so that the cost of a path through this router becomes larger than that of an alternative path. OSPFv3 stub router advertisement allows a router to advertise the infinity metric (0xFFFF) for its connected links in router LSAs and advertise normal interface cost if the link is a stub network.

Repair your IPv6 network with minimal impact

- Advertise an infinity metric to route traffic on redundant path
- Path through this router becomes larger than that of an alternative path



For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2mt/ip6-route-ospfv3-max-lsa.html.

- OSPFv3 Fast Convergence: LSA and SPF Throttling

  OSPFv3 can use static timers for rate-limiting SPF calculation and LSA generation. Although these timers are configurable, the values used are specified in seconds, which poses a limitation on OSPFv3 convergence. LSA and SPF throttling achieves subsecond convergence by providing a more sophisticated SPF and LSA rate-limiting mechanism that is able to react quickly to changes and also provide stability and protection during prolonged periods of instability.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2mt/ip6-route-ospfv3-fastcon.html.

- OSPFv3 VRF-Lite/PE-CE

  The OSPFv3 VRF-Lite/PE-CE feature enables VRF deployment without a BGP- or MPLS-based backbone. In VRF-Lite, the PE routers are directly connected using VRF interfaces. For OSPFv3, the following needs to operate differently in the VRF-Lite scenario, as opposed to the deployment with BGP or MPLS backbone:

  - DN bit processing: In VRF-Lite environment, the DN bit processing is disabled.
  - ABR status: In VRF context (except default VRF), OSPFv3 router is automatically set as an ABR, regardless to its connectivity to area 0. This automatic ABR status setting is disabled in the VRF-Lite environment. OSPFv3 VRF-Lite and PE-CE support both IPv4 and IPv6 address families.

- SAF Dynamic Neighbors

  When neighbors are not adjacent, normal Cisco SAF peering mechanisms cannot be used to exchange SAF information over the networking cloud. The neighbors are often multiple hops away and separated by dark nets (routers not running SAF).

  To support this type of network, SAF provides the **neighbor** command, which allows remote neighbors to be configured and sessions established through unicast packet transmission. However, as the number of forwarders needing to exchange SAF information over the networking cloud increases, unicast SAF neighbor definitions might become cumbersome to manage. Each neighbor has to be manually configured, resulting in increased operational costs.

  To better accommodate deployment of these topologies, ease configuration management, and reduce operational costs, the dynamic neighbors feature provides support for the dynamic discovery of remote unicast and multicast neighbors (referred to as "remote neighbors"). Remote neighbor support allows Cisco SAF peering to one or more remote neighbors, which might not be known at the time the router is configured, thus reducing configuration management.

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

- VRF-Aware ARP Debug

  The VRF-aware ARP debug feature provides software debug statements for ARP modules in VRF environments.

Table 5 lists more new IP routing features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 5. New Features and Enhancements

Capabilities Manager
IP-RIP delay start
OSPF support for NSSA RFC 3101
Enabling OSPFv2 on an interface using the ip ospf area command
TTL security support for OSPF on IPv6
OSPF SNMP ifIndex value for interface ID
IS-IS support for MT
IS-IS support for an IS-IS instance per VRF for IP
NHRP reformation move to IP services
EIGRP/SAF HMAC-SHA-256 authentication

MPLS and VPNs

- L2VPN Advanced VPLS (A-VPLS)

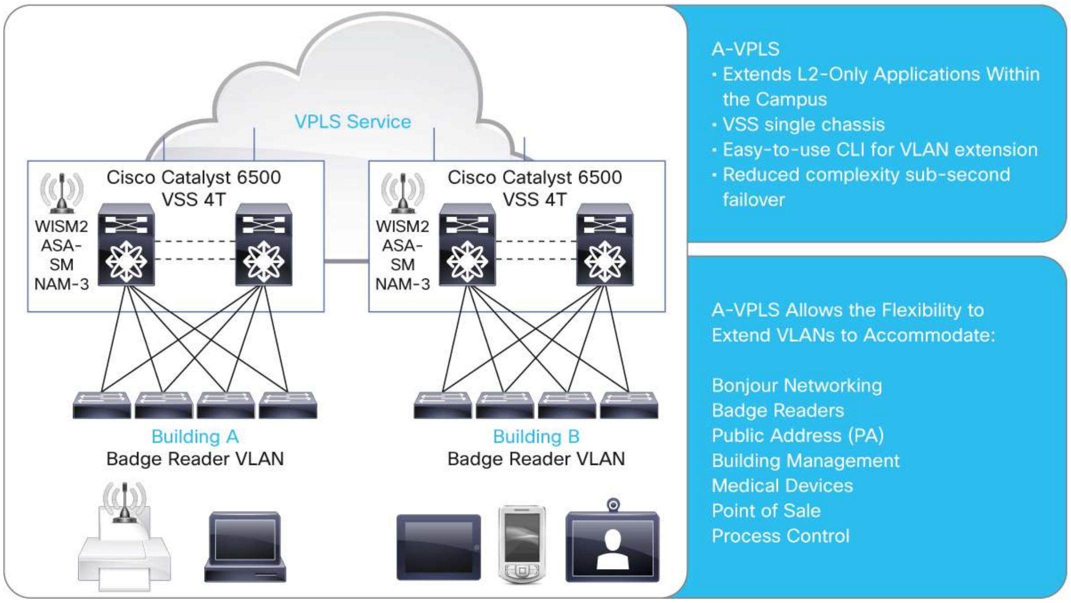
  The Cisco Layer 2 VPN (L2VPN) advanced VPLS (A-VPLS) feature introduces the following enhancements to VPLS:

  ◦ Capability to load-balance traffic across multiple core interfaces using equal-cost multipathing (ECMP)

  ◦ Command-line interface (CLI) enhancements to facilitate configuration of the L2VPN A-VPLS feature

Campus VLAN Extension

Enabling Device Mobility (BYOD) with A-VPLS



A-VPLS

- Extends L2-Only Applications Within the Campus
- VSS single chassis
- Easy-to-use CLI for VLAN extension
- Reduced complexity sub-second failover

A-VPLS Allows the Flexibility to Extend VLANs to Accommodate:

Bonjour Networking
Badge Readers
Public Address (PA)
Building Management
Medical Devices
Point of Sale
Process Control

- VPLS Autodiscovery, BGP Based

  The virtual private LAN service (VPLS) using BGP for autodiscovery and signaling feature adds the capability to automatically discover all the peers belonging to a specific VPLS instance, signal service capabilities, and establish the appropriate pseudowire mesh to support a VPLS service.

- VPLS over GRE and MPLS over GRE

  The VPLSoGRE and EoMPLSoGRE feature allows transport of VPLS or EoMPLS traffic over an IP core by encapsulating with the GRE header.

- MPLS LDP-IGP Synchronization

  When there are periods of convergence in a topology with network virtualization, MPLS LDP-IGP synchronization removes blackholing of traffic.

  This feature helps make sure that the Label Distribution Protocol (LDP) is fully established before the IGP path is used for switching. Without this feature, packet loss can occur because the actions of the IGP and LDP are not synchronized, and forwarding occurs before LDP and IGP are synchronized. Both OSPF and IS-IS are supported in this release.

Table 6 lists additional new MPLS and VPN features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 6. New Features and Enhancements

EVN EIGRP
EVN multicast
EVN OSPF
EVN route replication
EVN routing context
IS-IS: MPLS LDP synchronization
ISSU: MPLS VPN 6VPE and 6PE ISSU support

Multicast

- Multicast Service Reflection

  The multicast service reflection feature provides the capability for users to translate externally received multicast destination addresses to addresses that conform to their organization's internal addressing policy. Using this feature, users do not need to redistribute routes at the translation boundary into their network infrastructure for reverse path forwarding (RPF) to work properly, and users can receive identical feeds from two ingress points in the network and route them independently.

- MLDP-Based MVPN

  The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the multicast virtual private network (MVPN) core network.

  With MLDP you don’t need to enable PIM in the core.

- MLDP Filtering

  The MDLP filtering feature adds filtering capabilities to the Cisco MLDP label-based MVPN solution. It provides the ability to map flows and filter out multicast traffic distributed to different sites using MLDP-based MVPNs.

- Multicast Live-Live

  The multicast live-live feature delivers two multicast streams with the same content over diverse paths in the network. This functionality reduces packet loss because of network failures on any one of the paths.

This feature provides the ability to select a particular unicast routing table for RPF interface used by PIM, based on source and multicast group.

Table 7 lists additional new multicast features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 7. New Features and Enhancements

IGMPv3 host stack
PIMv6: anycast RP solution
MLD group limits
ISSU: IPv6 multicast
MVPN: data MDT enhancements
IP multicast load splitting: equal cost multipath (ECMP) using S, G, and next hop
MET enhancements for VPLS
IPv6 BSR: configure RP mapping
MTR support for multicast

IP Services

- WCCP: Configurable Router ID

  WCCP uses a router ID in its control messages that a WCCP client can use to uniquely identify a particular WCCP server. The router ID is an IP address and is used as the source address of any WCCP-generated GRE frames. Prior to the WCCP: configurable router ID feature, WCCP selected a router ID using an automatic mechanism; the highest reachable IP address on the system (or the highest loopback IP address, if there is one) was used as the WCCP router ID. The highest IP address on the system is not always the best choice as the router ID or as the source address of GRE frames. A change in addressing information on the system might cause the WCCP router ID to change unexpectedly. During this changeover period, WCCP clients briefly advertise the existence of two routers (the old router ID and the new router ID), and GRE frames are sourced from a different address.

  The WCCP: configurable router ID feature enables you to define a WCCP source interface from which the router ID will be obtained. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, the router ID does not change when another IP address is added to the system. The router ID changes only when a new router ID is manually configured using the **ip wccp source-address** or **ipv6 wccp source-address** command or when the address on the manually configured interface is no longer valid.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/15-2mt/iap-wccp-cfg-rtr-id.html.

- VRRPv3 Protocol Support

  Virtual Router Redundancy Protocol (VRRP) enables a group of routers to form a single virtual router to provide redundancy. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. The VRRP Version 3 (v3) protocol support feature provides the capability to support IPv4 and IPv6 addresses, whereas VRRPv2 only supports IPv4 addresses.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-2mt/fhrp-vrrpv3.html.

- WCCP Fast Timers

  The WCCP fast timers feature enables WCCP to establish redirection more quickly when a WCCP client is added to a service group or when a WCCP client fails.

  WCCP routers and WCCP clients exchange keepalive messages at a fixed interval. Prior to the introduction of the WCCP fast timers feature, the WCCP message interval is fixed at 10 seconds. The WCCP fast timers feature enables use of message intervals ranging from .5 seconds to 60 seconds and a timeout value scaling factor of 1 to 5.

  The WCCP message interval capability introduced by the WCCP fast timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result.

  The WCCP router enforces a single message interval per service group. WCCP clients with incompatible message intervals are prevented from joining a service group.

  For more information, visit http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/xe-3s/iap-wccp.html.

- NAT: VRF-Aware NAT

  NAT integration with MPLS VPNs allows multiple MPLS VPNs to be configured on a single device to work together. NAT can differentiate from which MPLS VPN it receives IP traffic even if the MPLS VPNS are all using the same IP addressing scheme. This enables multiple MPLS VPN customers to share services while making sure that each MPLS VPN is completely separate from the other.

  MPLS service providers would like to provide value-added services such as Internet connectivity, domain name servers (DNS), and VoIP service to their customers. This requires that their customers' IP addresses be different when reaching the services. Because MPLS VPN allows customers to use overlapped IP addresses in their networks, NAT must be implemented to make the services possible.

  There are two approaches to implementing NAT in the MPLS VPN network. NAT can be implemented on the CE router, which is already supported by NAT, or it can be implemented on a PE router. The NAT integration with MPLS VPNs feature enables the implementation of NAT on a PE router in an MPLS cloud.

Table 8 lists new IP services features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 8. New Features and Enhancements

DHCP: server port-based address allocation
DHCP relay server ID override and link selection option 82 suboptions
FTP IPv6 support
TFTP IPv6 support
MAC move and replace
Per-port location configuration
Storm control action: port disable
Flex links interface preemption

Infrastructure

- Cisco IOS Shell

  The Cisco IOS shell (IOS.sh) feature provides shell scripting capability to the Cisco IOS Software command-line-interface (CLI) environment. Cisco IOS.sh enhances the process of controlling and configuring a Cisco IOS Software router using the CLI by including variable substitution, paths, conditional statements, loops, pipes, and so on to enhance the user experience of Cisco IOS Software CLI users.

Table 9 lists additional new infrastructure features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 9. New Features and Enhancements

Syslog Common Criteria
VRF-aware NTP
VRF support for TFTP server, TFTP client, and FTP client
NTPv4 orphan mode support, range for trusted key configuration
NTPv4 with support for IPv4 and IPv6
Parser concurrency and locking improvements
Show command section filter
Interface range MAC-limit configure CLI

Mobility

- Network Mobility Services Protocol (NMSP)

  Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the location server and the controller. Transport of telemetry, emergency, and chokepoint information between the location server and the controller is managed by this protocol.

Table 10 lists additional new mobility features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 10. New Features and Enhancements

Custom location type
Geo location type support
Switch location configuration

Manageability

Embedded Management

- Call Home V2 Enhancements

  Call home V2 provides capability to diagnose more issues on the system without the need to upgrade Cisco IOS Software and to provide crash/traceback reporting capability. This release provides part of the call home V2 features, including crash/traceback reporting to allow crash to be reported on reload/process restart and traceback (decode) to be reported to backend for analysis and call home message compression option to bypass AAA when executing CLI source interface support snapshot/telemetry support.

Table 11 lists additional new embedded management features and enhancements available with Cisco IOS Software Release 15.1(1)SY.

Table 11. New Features and Enhancements

Embedded Event Manager (EEM) 4.0
IP SLAs: LSP health monitor with LSP discovery
IP SLAs VRF-aware 2.0
XML-PI
Web Services Management Agent (WSMA)
Configuring ITU-T Y.1731 fault management functions
VRF-aware source interface for syslog transactions
IP unnumbered Ethernet polling

Cisco EnergyWise

- EnergyWise Pre-Phase 2.5

  For more information, see this publication: http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/release/notes/OL19810.html

- EnergyWise 2.5

  Cisco EnergyWise™ Phase 2.5 shows the platforms and software revisions currently supported by Cisco EnergyWise.

  For more information, see this publication: http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2_5/ios/release/notes/ol23554.html

- LLDP Inline Power Negotiation for PoE+

  This feature enables inline power negotiation using LLDP on the Cisco Catalyst 6500 Series platforms

MIBs

Table 12 lists MIB enhancements.

For details, visit ftp://ftp-sj.cisco.com/pub/mibs/supportlists/wsc6000/wsc6000-supportlist-ios.changes.

Table 12. Cisco IOS Software Release 15.1(1)SY MIB Enhancements

4293 IP-MIB (IPv6 only) and RFC 4292 IP-FORWARD-MIB (IPv6 only)
BFD MIB Version 2
CISCO-AUTH-FRAMEWORK-MIB enhancement of MAC move and replace
Cisco Express Forwarding: SNMP CEF-MIB support
CISCO-CALLHOME-MIB enhancement for Call Home Version 2
CISCO-IP-URPF-MIB support
CISCO-PORT-STORM-CONTROL-MIB enhancement for shutdown and trap actions
CISCO-POWER-ETHERNET-EXT-MIB enhancement for power priority and LLDP statistics
CISCO-SWITCH-CEF-MIB
CISCO-TRUSTSEC-INTERFACE-MIB trap enhancement
CISCO-TRUSTSEC-POLICY-MIB enhancement for C6K MA2 release
CISCO-TRUSTSEC-SERVER-MIB enhancement for Cisco TrustSec key wrap and notifications
CISCO-VIRTUAL-SWITCH-MIB enhancement for adding switch location info
CISCO-VIRTUAL-SWITCH-MIB enhancement for monitoring VSS dual active detection feature

EIGRP MIB
IEEE 802.1ab LLDP local and remote system MIBs
IEEE8021-PAE-MIB enhancement for supplicant statistics
IGMP MIB support enhancements for SNMP
IP-TUNNEL-MIB
MSDP MIB
Multicast MIB VRF support
NTPv4 MIB
PIM MIB extension for IP multicast
POWER-ETHERNET-MIB enhancement for power priority
SNMP trap of CISCO-TRUSTSEC-MIB for Cisco TrustSec keystore
SNMP trap of CISCO-TRUSTSEC-SXP-MIB for Cisco TrustSec
TCP MIB for RFC4022 support
UDP MIB for RFC4113 support

Supervisor Support

This table shows the features that are available with the current release.

Certain features are supported on the supervisors in an earlier release, but 15.1(1)SY is where parity for both supervisors for certain features is achieved.

Table 13. 15.1(1)SY Feature and Supervisor Support

Feature	Supervisor Support
VRF Aware NAT	Sup2T
Per VRF AAA	Sup720, Sup2T
TrustSec: Per session change of Authorization	Sup720, Sup2T
OSPFv3 Multi-AF support (addr-alt)	Sup720, Sup2T
IPv6 OSPFv3 vrf-aware VRF-Lite and PE-CE	Sup720, Sup2T
IPv6 Core HA (ND NSF)	Sup720, Sup2T
TCP/UDP MIBs	Sup720, Sup2T
NTPv4 - NTP for IPv6	Sup720, Sup2T
PIM and IGMP snooping for VPLS	Sup2T
VPLS Auto-discovery	Sup2T
VRF aware NTP	Sup720, Sup2T
VRF Aware BFD	Sup720, Sup2T
TrustSec: Diagnostics Toolkit	Sup2T
IP aware MPLS netflow	Sup2T
IPv4 over IPv6 tunnel	Sup2T
IPv6 PBR	Sup720, Sup2T
MPLSoGRE	Sup2T
LDP - IGP Synchronization (OSPF)	Sup720, Sup2T
LDP - IGP Synchronization (IS-IS)	Sup720, Sup2T
LSM Label Switched Multicast - mLDP with PIM signaling	Sup720, Sup2T
VLAN ACL support for IPv6 VACL	Sup720, Sup2T

Feature	Supervisor Support
BFD for IPv6	Sup720, Sup2T
BFD support on port channels	Sup720, Sup2T
Network Edge Authentication Topology (NEAT)	Sup720, Sup2T
LLDP MIB	Sup720, Sup2T
Service Advertisement Framework (SAF)	Sup720, Sup2T
Port Security for L2 EtherChannel Interface	Sup720, Sup2T
XML Programmatic interface	Sup720, Sup2T
URPF-MIB	Sup720, Sup2T
IP-TUNNEL-MIB	Sup720, Sup2T
HTTP over IPv6	Sup720, Sup2T
TCL over IPv6	Sup720, Sup2T
Config Logger support for IPv6	Sup720, Sup2T
LSM: mLDP HA	Sup720, Sup2T
VRF aware SSH	Sup720, Sup2T
Copy-based Packet Sampling	Sup2T
IPv6 LLDP support	Sup720, Sup2T
PoEP Linecard Support	Sup720, Sup2T
NMSP Protocol for integration with location server	Sup720, Sup2T
IPv6 Router Advertisement Guard (RA Guard)	Sup720, Sup2T
Web Services management agent	Sup720, Sup2T
IPv6 Interface MIB	Sup720, Sup2T
VRF aware FTP	Sup720, Sup2T
TrustSec Identity Port Mapping	Sup720, Sup2T
Radius Session CoA	Sup720, Sup2T
MAC move & replace	Sup720, Sup2T
SFP+ LRM Support	Sup720, Sup2T
IPv6 Static BFD client	Sup720, Sup2T
X2-10GBaseT support	Sup720, Sup2T
BFD For SVIs	Sup720, Sup2T
CISCO-VLAN-GROUP-MIB support	Sup720, Sup2T
Auto Interleaved Port-priority for LACP	Sup720, Sup2T
EnergyWise Phase 2.5	Sup720, Sup2T
OSPF for routed access	Sup720, Sup2T
EIGRP MIB Support	Sup720, Sup2T
TrustSec: SXP Loop Detection (and other enhancements)	Sup720, Sup2T
L3 Identity Port Mapping (L3 enforcement)	Sup720, Sup2T
Subnet to SGT mapping	Sup720, Sup2T
TrustSec: SGT Caching	Sup2T
TrustSec: Per Policy based CoA	Sup2T
BGP: neighbor soo command	Sup720, Sup2T
BGP event based VPN import	Sup720, Sup2T

Feature	Supervisor Support
BGP RT changes without PE-CE neighbor impact	Sup720, Sup2T
BGP for IPv6 address family NSF & Graceful Restart	Sup720, Sup2T
IP-RIP: Delay start	Sup720, Sup2T
SSO - MPLS VPN 6VPE & 6PE SSO support	Sup720, Sup2T
ISSU - MPLS VPN 6VPE & 6PE ISSU support	Sup720, Sup2T
OSPF Graceful Shutdown	Sup720, Sup2T
OSPFv2 Local RIB	Sup720, Sup2T
Enabling OSPFv2 on an Interface Using the ip ospf area Command	Sup720, Sup2T
OSPF TTL Security Check	Sup720, Sup2T
OSPFv3 Fast Convergence Enhancements - LSA and SPF throttling	Sup720, Sup2T
Graceful Restart for OSPFv3	Sup720, Sup2T
IGMPv3 host stack CSCdz51758	Sup720, Sup2T
Multicast Support with MTR	Sup720, Sup2T
Enhanced Multicast Multipath	Sup720, Sup2T
NSF/SSO IPv6 Multicast	Sup720, Sup2T
ISSU IPV6 Mulitcast	Sup720, Sup2T
Multicast MIB VRF support	Sup720, Sup2T
BGP PIC Edge	Sup720, Sup2T
BGP Best External IPv4	Sup720, Sup2T
BGP Remove Private-AS	Sup720, Sup2T
Static Routes for BFD	Sup720, Sup2T
IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec	Sup720, Sup2T
OSPFv3 BFD	Sup720, Sup2T
OSPFv3 IPSec ESP Encryption and Authentication	Sup720, Sup2T
Multicast Service Reflection - Destination address translation and packet replication service	Sup720, Sup2T
Anycast RP for IPv6 multicast	Sup2T
MPLS TE FRR Client Support for BFD	Sup2T
BFD over GRE support	Sup720, Sup2T
Channel hot-standby dampening	Sup720, Sup2T
TACACS+ for IPv6	Sup720, Sup2T
storm control with SNMP trap	Sup720, Sup2T
2-level shaping on Estelle	Sup2T
NHRP reformation move to IP Services	Sup720, Sup2T
BGP PIC CORE	Sup720, Sup2T
Advanced VPLS	Sup2T
Console Disconnect	Sup720, Sup2T
IPv6 access lists to filter hop-by-hop protocol	Sup2T
Netflow Exporting Layer 2 and Port information for IPv4	Sup720, Sup2T
Location 3.0	Sup720, Sup2T
TrustSec: SGACL Monitor-Mode (Dry Run)	Sup2T
MVPN Enhancements	Sup720, Sup2T

Feature	Supervisor Support
BGP RT Constrained - RFC 4684	Sup720, Sup2T
Multicast Live-Live	
EIGRP IPv6 VRF-lite	Sup720, Sup2T
BFD MIB Support	Sup720, Sup2T
NSR for OSPFv2	Sup720, Sup2T
EEM 4.0	Sup720, Sup2T
VRRPv3 protocol support	Sup720, Sup2T
Medianet metadata 1	Sup2T
6VPE for VRF-Lite	Sup720, Sup2T
MPLS Pseudowire Status Signalling	Sup720, Sup2T
Tunnel HA NSF/SSO IPv4 and IPv6	Sup720, Sup2T
ip unnumbered ethernet polling	
VRF Aware for TCP, FTP, HTTP and DNS Operations	Sup720, Sup2T
Netflow FNF Flexible Netflow with bridged IPv6 (layer 2 vlan traffic)	Sup2T
IPv6 OSPFv3 max-metric LSA	Sup720, Sup2T
Flexlink Preempt support Sup720 & Sup2T	Sup720, Sup2T
IEEE8021-PAE-MIB Enhancement for supplicant statistics	Sup720, Sup2T
CISCO-PORT-STORM-CONTROL-MIB Enhancement for storm shutdown/trap actions	Sup720, Sup2T
VPLSoGRE / EoMPLSoGRE support on SUP2T	Sup2T
IP FRR (PI Code Only)	Sup2T
CoPP - Microflow Policing	Sup2T
Multicast Label Distribution Protocol (MLDP) - MLDP filtering	Sup2T
Callhome V2 (incl diagnostic signatures, crashdump alertgroup)	Sup720, Sup2T
EIGRP Wide Metric Sup720 Sup2T	Sup720, Sup2T
Multicast IGMP L2 Snooping Querier redundancy support	Sup720, Sup2T
IPv6 Device Tracking - FHS phase	Sup720, Sup2T
Capabilities Manager Phase 1	Sup720, Sup2T
SAF Neighbor Enhancements	Sup720, Sup2T
HMAC SHA-256	Sup720, Sup2T
TrustSec: Environement data change of Authorization	Sup720, Sup2T
IP Tunnels mGRE IPv6 support	Sup720, Sup2T
IPv6 - Per interface ND cache limit	Sup720, Sup2T
Energywise 2.5	Sup720, Sup2T
BGP - Cisco-BGP-MIBv2	Sup720, Sup2T
BGP IPv6 PIC Edge	Sup720, Sup2T
AAA: Radius over IPv6 Support	Sup720, Sup2T
AAA: SNMP Improvements	Sup720, Sup2T
AAA: Domain stripping based on server groups	Sup720, Sup2T
AAA: ISSU Improvements	Sup720, Sup2T
sshv2 enhancements for rsa keys	Sup720, Sup2T
NTPv4 enhancements - Orphan mode, SNTP with MD5 support, range for trusted keys	Sup720, Sup2T

Feature	Supervisor Support
WCCP Fast Timers	Sup720, Sup2T
WCCP Configurable Router ID	Sup720, Sup2T

Ordering Information

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center. Table 13 lists ordering information for Cisco IOS Software Release 15.1(1)SY.

Table 14. Cisco IOS Software Release 15.1(1)SY 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
Cisco CAT6000-VS-S2T IOS UPD IOS ADV IP 2 ADV ENT ENCRYPT	S2TAIAE9-15001SY=
Cisco CAT6000-VS-S2T IOS UPD IOS IP SRV 2 ADV ENT ENCRYPT	S2TIAE9-15001SY=
Cisco CAT6000-VS-S2T IOS UPD IOS ADV IP 2 ADV ENT NPE	S2TAAE9N-15001SY=
Cisco CAT6000-VS-S2T IOS UPD IOS IP SRV 2 ADV ENT NPE	S2TIAE9N-15001SY=
Cisco CAT6000-VS-S2T IOS UPD IP SRV 2 ADV IP ENCRYPT	S2TIAI9-15001SY=
Cisco CAT6000-VS-S2T IOS UPD IP SRV 2 ADV IP NPE	S2TIAI9N-15001SY=

Product Management Contacts

For more information, contact the Cisco Catalyst 6500 Marketing Team.

Cisco IOS Software Center

Download Cisco IOS Software releases and access software upgrade planners at http://www.cisco.com/cisco/web/download/index.html.

Support

Cisco IOS Software Release 15.1(1)SY follows the standard Cisco support policy. For more information, visit http://www.cisco.com/en/US/products/products_end-of-life_policy.html.

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 of 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 C25-717747-02 02/13