Cisco IOS Software Release 15.1(1)SY1 for Cisco Catalyst 6500 Series Switches

PB728597

Cisco IOS® Software Release 15.1(1)SY1 is the second converged software release for Cisco® Catalyst® 6500 Series Switches that supports Cisco Catalyst 6500 Series Supervisor Engine 2T (Sup 2T) and Cisco Catalyst 6500 Series Supervisor Engine 720 (Sup 720-3B and Sup 720-10G).

Release 15.1(1)SY1 adds 22 primary new features for Cisco Catalyst 6500 switches:

- **Cisco Catalyst Virtual Switching System Quad-Supervisor Stateful Switchover (VS4O)** brings further network resiliency to campus switching with support for four supervisors and replicated control plane in the two VSS switches. VS4O supports hot standby redundancy over four supervisors by introducing VSS active standby and in-chassis active standby roles to add complete control-plane redundancy for five-nines high availability. The functionality will be supported with Sup 2T hardware.
- **Locator/ID Separation Protocol (LISP)** is introduced on the Cisco Catalyst 6500 switch with this release. LISP is an evolutionary routing architecture designed for Internet scalability and global reach across organizations. In the campus core and distribution, LISP enables IPv6 transition, virtualization, and multihoming.
- **Cisco TrustSec® security enhancements** to improve end-to-end deployments such as security group tag (SGT) name export in NetFlow and security group access lists (SGACL) monitor mode. Cisco TrustSec is supported on 1 Gig interfaces with addition of 802.1AE MACsec encryption for end-to-end Cisco TrustSec on Cisco Catalyst platforms.
- **Application visibility and control** have new capabilities with Web Cache Communication Protocol (WCCP) v2 IPv6 support to enable customers to take advantage of WAN optimization for web security appliances that support IPv6. Quality of service (QoS) has new features such as egress microflow destination policing, global QoS policies, and policer rate increase.
- **Routing and switching** feature additions include Virtual Private LAN services (VPLS)**,** Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) snooping on LAN interfaces, Multiprotocol Label Switching Traffic Engineering (MPLS TE) support on bundle interfaces, and Dynamic Host Configuration Protocol (DHCP) v6 relay chaining.

For detailed information about the features and hardware supported in Release 15.1(1)SY1, refer to the Cisco IOS Software Release 15.1(1)SY1 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.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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

Cisco IOS Software Release 15.1(1)SY1 adds support for the following hardware:

WS-X6904-40G-2T switching module support for:

- GLC-LH-SMD
- GLC-T
- GLC-SX-MMD
- Supervisor Engine 2T support on 7606S chassis

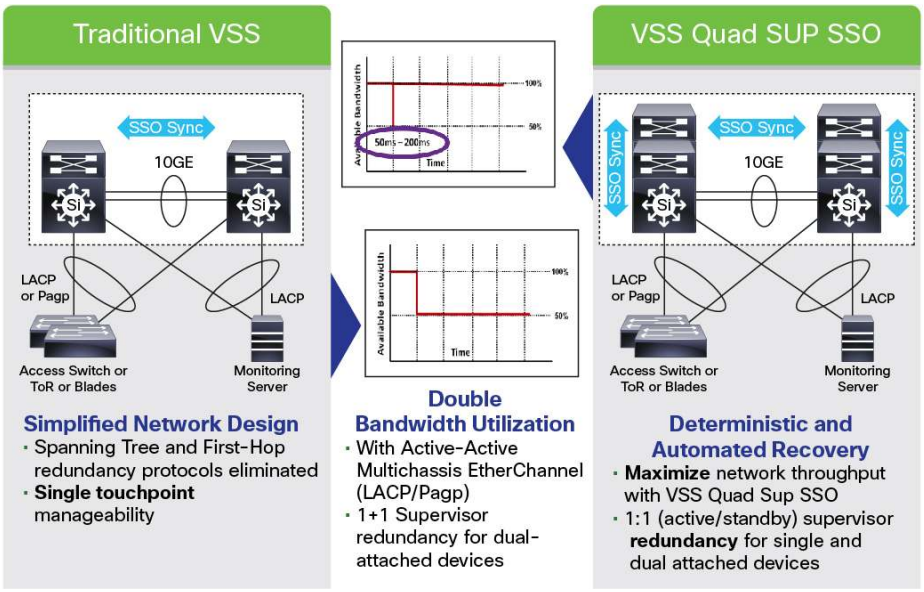
Software Feature Highlights of Release 15.1(1)SY1

Resiliency

- **VS4O:** Cisco Catalyst 6500 VSS now supports quad supervisors in the switches part of the VSS pair. The four supervisors as assigned roles in the VSS and in-chassis domains as:
  1. VSS active
  2. VSS standby
  3. In-chassis active
  4. In-chassis standby

  Redundancy is maintained between the corresponding active and standby supervisor cards during the normal boot-up and operation of switches. The standby supervisors are hot standby and have all the control-plane and protocol states synced up with the active supervisors. If there is a failure of the VSS active supervisor card, then there are two simultaneous failovers in the two domains that make sure the recovery is within 50 milliseconds, providing five-nines high availability in campus networks. The infrastructure is also used for Enhanced Fast Software Upgrade (EFSU) by loading the newer versions of the software in parallel, resulting in improved EFSU times. (See Figure 1.)

Figure 1. VSS Quad SUP SSO Overview



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- **Hot Standby Router Protocol (HSRP)-aware PIM:** PIM has no inherent redundancy capabilities, and its operation is completely independent of HSRP group states. As a result, IP multicast traffic is forwarded not necessarily by the same device as is elected by HSRP. The HSRP-aware PIM feature provides consistent IP multicast forwarding in a redundant network with virtual routing groups enabled.

  HSRP-aware PIM enables multicast traffic to be forwarded through the HSRP active router, allowing PIM to use HSRP redundancy, avoid potential duplicate traffic, and enable failover, depending on the HSRP states in the device. The PIM designated router runs on the same gateway as the HSRP active router and maintains mroute states. This vastly improves multicast performance when used with HSRP.

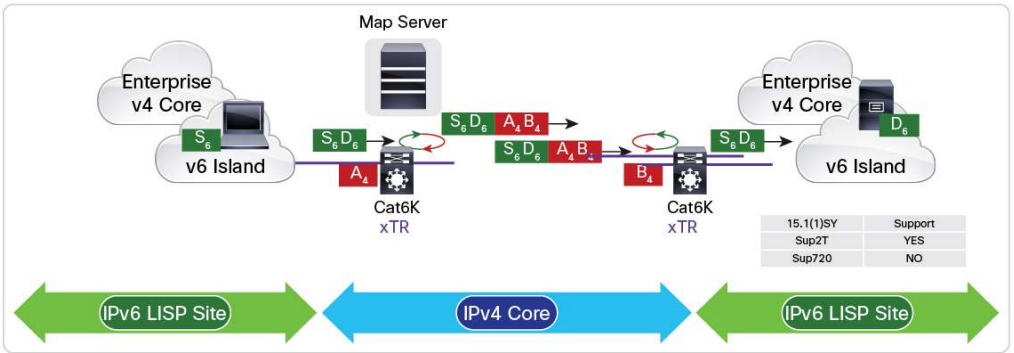
Routing and Switching

- **LISP:** LISP is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:
  - Endpoint identifiers (EIDs): assigned to end hosts.
  - Routing locators (RLOCs): assigned to devices (primarily routers and switches) that make up the global routing system.

  Splitting EID and RLOC functions yields several advantages, including improved routing system scalability and improved multihoming efficiency and ingress traffic engineering.

  The Ingress Tunnel Router (ITR) encapsulates data from a LISP site to another LISP site, and the Egress Tunnel Router (ETR) decapsulates packet coming in from a LISP site. Similarly, the Proxy ITR (PITR) encapsulates the data from a non-LISP site to a LISP site. The Proxy ETR (PETR) decapsulates data from a LISP site and natively forwards packets to the non-LISP site. The Cisco Catalyst 6500 switch with Sup 2T and 6904/6908 line cards can function as ITR or ETR (xTR) in the campus networks. LISP map server and map resolver can be configured on the Cisco Catalyst 6500 switch:
  - **LISP shared virtualization support:** LISP shared model virtualized EID space is created by binding VRFs associated with an EID space to instance IDs. A common shared locator space is used by all virtualized EIDs.
  - **LISP for IPv4 to IPv6 transition:** Since LISP allows both IPv4 and IPv6 EIDs to be encapsulated in IPv4 RLOCS, it can be used to connect IPv6 LISP sites separated by an IPv4 network. It can therefore be used to transition islands into IPv6 and connect them over IPv4 networks. (See Figure 2.)

Figure 2. LISP on Catalyst 6500



Base LISP (xTR, PxTR), Map-Server
Multitenant (MS/MR/xTR) Shared Mode
Supported with Supervisor 2T, 6904, 6908 Modules

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- **VPLS PIM and IGMP snooping:** With Release 15.1(1)SY1, IGMP snooping and PIM snooping constrain VPLS multicast traffic, except with hierarchical VPLS or integrated routing and bridging (IRB). IGMP snooping is commonly deployed to make sure multicast traffic is not forwarded on ports without IGMP receivers. PIM snooping procedures are important to restrict multicast traffic to only the switches interested in receiving such traffic. This feature improves IP multicast bandwidth usage in the VPLS core by making sure traffic is replicated only to Provider Edge (PE) with member sites.
- **MPLS TE bundled interface support:** The MPLS TE bundled interface support feature enables MPLS TE tunnels over the bundle interfaces such as EtherChannel and Multilink Point-to-Point Protocol (MLPPP) for Sup 720. With this feature Resource Reservation Protocol (RSVP) notifies TE about bandwidth changes that occur when member links status changes or when links become active or inactive. TE notifies other nodes in the network using Interior Gateway Protocol (IGP) flooding. The fast reroute (FRR) feature is now supported on the bundled interfaces and gets activated when the interface goes down.
- **DHCPv6 relay chaining for prefix delegation:** The DHCPv6 relay agent notification for prefix delegation allows the switch working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 reply packet that is transmitted by the relay agent to the client. When a prefix delegation option is found, the relay agent extracts the information about the prefix that is being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent.

Security and Virtualization

- **Cisco TrustSec on 1 Gig interfaces:** Support for 802.1AE MACsec encryption on 1 Gig interfaces is added for end-to-end Cisco TrustSec on Cisco Catalyst platforms. The 6904 line card with 4X Small Form-Factor Pluggable/Small Form-Factor Pluggable Plus (SFP/SFP+) adapter will support this feature.
- **SGT name export in NetFlow:** This feature allows flexible NetFlow to export Cisco TrustSec environmental data tables that map SGTs to security group names (SGNs).
- **SGACL monitor mode:** During the pre deployment phase of Cisco TrustSec, an administrator would use the monitor mode to test security policies without enforcing them to make sure the policies are what were originally intended. If there is something wrong with the security policy, the monitor mode provides a convenient way to roll back before enforcing it. This feature enables administrators to have increased visibility to the outcome of the policy actions before enforcement and confirmation that the subject policy meets the security need (deny access to resources if the individuals are not authorized). This feature also reduces the eventual deployment time for a Cisco TrustSec system.
- **Cisco TrustSec diagnostic toolkits: packet trace:** This feature brings in end-to-end debug ability in the campus network with the packet tracing utility turned on for SGT packets traversing the Cisco Catalyst 6500 Series Switch.
- **SGA syslog messages:** This feature converts existing SGA debug messages to formatted syslogs. This makes sure that critical messages during the authentication and negotiation are captured for subsequent debugging. New syslogs have been defined, and they also provide Simple Network Management Protocol (SNMP) support to trap syslogs.
- **Conditional debugging:** This feature allows users to define a debug condition and then turn on Cisco TrustSec debug, so that only debugs that meet the defined condition will be displayed. Currently there is no Cisco TrustSec conditional debug, and therefore Cisco TrustSec requires turning on all debug. This could adversely affect the network and is only to be turned on during a maintenance window. The conditional debugging takes away that restriction.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Application Visibility and Control

- **WCCPv2 IPv6 support:** This functionality enables customers to take advantage of WAN optimization for web security appliances that support IPv6. Multiple routers can use WCCPv2 to service a content engine cluster.

  WCCP provides client local caching of content accessed using HTTP in order to:

  - Accelerate access to HTTP-based content
  - Conserve WAN bandwidth consumption by HTTP-based applications
  - Operate transparently to clients and servers
- **Egress microflow destination-only policing:** This feature provides additional capabilities in the per-interface microflow policer. The mask dest-only keywords can be applied on the base flow identification (only on destination addresses), which applies the microflow policer to all traffic to each source address. Policy Feature Card (PFC) QoS supports the mask dest-only keywords for both IP traffic and MAC traffic.
- **QoS policer rate increase to 256G:** The maximum for the valid range of values for the peak rate: **pir** *bits_per_second* parameter is now increased to 256 gigabits per second.
- **Global QoS policy:** Global protocol packet policing is now supported with this feature, and protocol packet policing mechanism effectively protects the supervisor CPU against attacks such as line-rate Address Resolution Protocol (ARP) attacks. It polices both routing protocols and ARP packets to the switch and also polices traffic through the switch with less granularity than Control plane policy (CoPP)**.**
- **Interfaces MIB: SNMP context-based access:** The SNMP support over VPNs context-based access control feature provides the infrastructure for multiple SNMP context support in Cisco software and VPN-aware MIB infrastructure using the multiple SNMP context support infrastructure. The SNMP notification support over VPNs feature allows the sending and receiving of SNMP notifications (traps and informs) using VPN routing and forwarding (VRF) instance tables. This feature extends the capabilities of the SNMP notification support for VPNs feature and enables SNMP to differentiate between incoming packets from different VPNs.

Supervisor Support

Table 1 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)SY1 is where parity for both supervisors for certain features is achieved.

Table 1. 15.1(1)SY1 Feature and Supervisor Support

Feature	Supervisor Support
Quad-supervisor VSS (VS4O)	Sup 2T
HSRP-aware PIM	Sup 720, Sup 2T
Cisco TrustSec: per session change of authorization	Sup 720, Sup 2T
SGT name export in NetFlow	Sup 720, Sup 2T
Cisco TrustSec diagnostic toolkits: packet trace	Sup 720, Sup 2T
SGACL monitor mode (dry run)	Sup 720, Sup 2T
Cisco TrustSec conditional debugging	Sup 720, Sup 2T
Cisco TrustSec SGA syslog messages	Sup 720, Sup 2T
LISP	Sup 2T

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Feature	Supervisor Support
PIM and IGMP snooping for VPLS	Sup 2T
MPLS TE bundled interface support	Sup 720, Sup 2T
DHCPv6 relay chaining for prefix delegation	Sup 720, Sup 2T
WCCPv2 IPv6 support	Sup 720, Sup 2T
Egress microflow destination-only policing	Sup 720, Sup 2T
QoS policer rate increase to 256G	Sup 720, Sup 2T
Global QoS policy	Sup 720, Sup 2T
Interfaces MIB SNMP context-based access	Sup 720, Sup 2T

Ordering Information

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center. Table 2 lists ordering information for Cisco IOS Software Release 15.1(1)SY.

Table 2. Cisco IOS Software Release 15.1(1)SY Ordering Information

Product Name	Part Number
Cisco CAT6000-VS-S2T IOS ADV ENT SERV FULL ENCRYPT	S2TAEK9-15101SY
Cisco CAT6000-VS-S2T IOS ADVANCED ENTERPRISE SERVICES NPE	S2TAEK9N-15101SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES FULL ENCRYPT	S2TAIK9-15101SY
Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES NPE	S2TAIK9N-15101SY
Cisco CAT6000-VS-S2T IOS IP SERV FULL ENCRYPT	S2TISK9-15101SY
Cisco CAT6000-VS-S2T IOS IP SERV NPE	S2TISK9N-15101SY
Cisco CAT6000-VS-S2T IOS IP BASE FULL ENCRYPT	S2TIBK9-15101SY
Cisco CAT6000-VS-S2T IOS IP BASE NPE	S2TIBK9N-15101SY
Cisco CAT6000-VS-S2T IOS UPD IOS ADV IP 2 ADV ENT ENCRYPT	S2TAIAE9-15101SY=
Cisco CAT6000-VS-S2T IOS UPD IOS IP SRV 2 ADV ENT ENCRYPT	S2TIAE9-15101SY=
Cisco CAT6000-VS-S2T IOS UPD IOS ADV IP 2 ADV ENT NPE	S2TAAE9N-15101SY=
Cisco CAT6000-VS-S2T IOS UPD IOS IP SRV 2 ADV ENT NPE	S2TIAE9N-15101SY=
Cisco CAT6000-VS-S2T IOS UPD IP SRV 2 ADV IP ENCRYPT	S2TIAI9-15101SY=
Cisco CAT6000-VS-S2T IOS UPD IP SRV 2 ADV IP NPE	S2TIAI9N-15101SY=

Product Management Contacts

For more information, contact the Cisco Catalyst 6500 Marketing Team at cco-6500-external@cisco.com.

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.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 make sure 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C25-728597-00 06/13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.