

# Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E for Cisco Catalyst 2960C, 2960S, 3560C, 3560-X, 3750-X, 4500E, 4500-X, and 4900 Series Switches

PB729400

## Overview

This product bulletin describes the primary hardware and software features supported by Cisco IOS® XE Software Release 3.5.0E/15.2(1)E for the following products:

- Cisco® Catalyst® 4500E Series Supervisor Engine 7-E and Supervisor Engine 7L-E running Cisco IOS XE Software Release 3.5.0E
- Cisco Catalyst 4500-X Series Switch running Cisco IOS XE Software Release 3.5.0E
- Cisco Catalyst 4500E Series Supervisor Engine 6-E and Supervisor Engine 6L-E running Cisco IOS Software Release 15.2(1)E
- Cisco Catalyst 4900M, 4948E, and 4948E-F Switches running Cisco IOS Software Release 15.2(1)E
- Cisco Catalyst 3560C, 3560-X, and 3750-X Series running Cisco IOS Software Release 15.2(1)E
- Cisco Catalyst 2960C and 2960S Series running Cisco IOS Software Release 15.2(1)E

For detailed information about the features and hardware supported in Standard Maintenance Release Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E, refer to the release notes and support documentation at:

- Cisco IOS XE Software 3.5.0E release notes for:
  - [Cisco Catalyst 4500E \(with Supervisor Engine 7-E/7L-E\)](#)
  - [Cisco Catalyst 4500-X](#)
- Cisco IOS Software 15.2(1)E release notes for:
  - [Cisco Catalyst 2960S, 2960C and 3560C](#)
  - [Cisco Catalyst 3750-X and 3560-X](#)
  - [Cisco Catalyst 4500E \(with Supervisor Engine 6-E/6L-E\)](#)
  - [4900M, 4948E, and 4948E-F](#)

## Primary Hardware and Software Service Innovations Delivered in Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E

Cisco IOS XE Software Release 3.5.0E/15.2(1)E is part of the new software releases on Cisco Catalyst 2960C, 2960S, 3560C, 3560-X, 3750-X, 4500E, and 4500-X Series Switches and Cisco Catalyst 4900M and 4948E/E-F Switches. These releases deliver new software and hardware innovations in campus access and aggregation deployments that span across application experience, BYOD, security, virtualization, operational simplicity, lower TCO, and resiliency. Each technology is covered in more detail in this product bulletin.

## Software Features

### Application Experience

#### Medianet Enhancements: Support for Metadata and Media Services Proxy

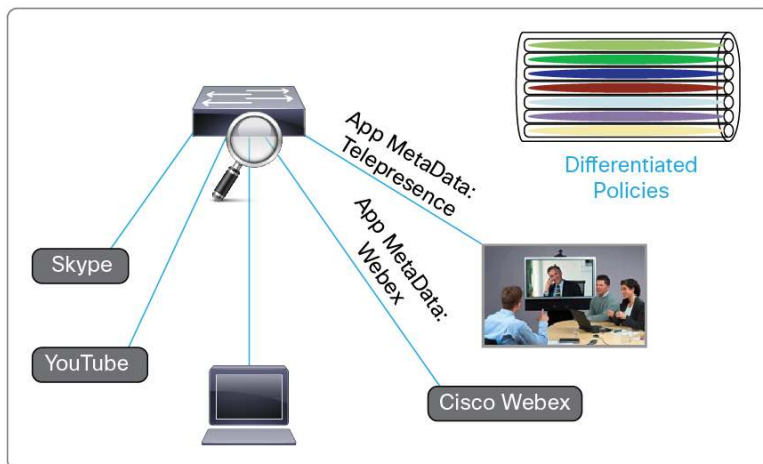
The growing use of video requires a change in how networks are built, operate, and function. While the demand for video grows, so does the need for more collaboration, requiring a network that is optimized for rich media (that is, not only voice and video but also the mixing together of video, documents, webpages, text, and many other forms of media).

Different types of devices that provide collaboration services (media endpoints) connect to a Cisco Catalyst switch. Some of them are legacy, and some might be MSI (Media Services Interface) aware. It is essential that the intervening network to be able to recognize the endpoint and provide relevant media service and the best performance on the network to these end devices. This capability sometimes needs the network to generate synthetic traffic to evaluate the capability of the underlying network to support such media. In light of this, two sets of needs are supported in the Cisco IOS XE Software 3.5.0/15.2(1)E release on the Cisco Catalyst 3750-X switch:

- Per-port metadata
- MSI proxy support

Figure 1 shows media-aware optimization and intelligent policy deployment using Medianet.

**Figure 1.** Media-Aware Optimization and Intelligent Policy Deployment Using Medianet



The per-port metadata and MSI proxy support enables the switch to snoop and to identify the legacy device and flow information (based on the protocols) for these devices. Based on the device/flow identification, the switch could then take action to provide the appropriate services such as quality-of-service (QoS) configuration and flow metadata signaling for network services. Metadata is now enabled on a per-port, per-flow basis, providing the relevant network services as required by the media endpoint.

**Flexible NetFlow IPFIX:** This feature, an IETF protocol based on RFC 5101, RFC 5102 and RFC 5103 is the only standards based protocol for flow information export. This is in addition to the existing v9 and v5 export protocol.

---

## BYOD and Security

### IPv6 First Hop Security (FHS)

With enterprises realizing the futuristic role that IPv6 will play, transition from IPv4 to IPv6 in campus access is gaining momentum. The transition to IPv6, although IPv6 is not directly compatible with its predecessor, poses many of the same security risks associated with IPv4.

Introduced on the Extended Maintenance Releases of 15.0(2)SE (Cisco Catalyst 3750 and 3560 products) and 15.1(2)SG (Cisco Catalyst 4500 products), IPv6 FHS provides effective countermeasures at the first hop (the switch) level, protecting the IPv6 network. Cisco IOS XE Software 3.5.0/15.2(1)E comprehensively covers all aspects of the IPv6 FHS, covering the entire spectrum of Cisco Catalyst switch platforms. This Cisco IOS Software release now provides for:

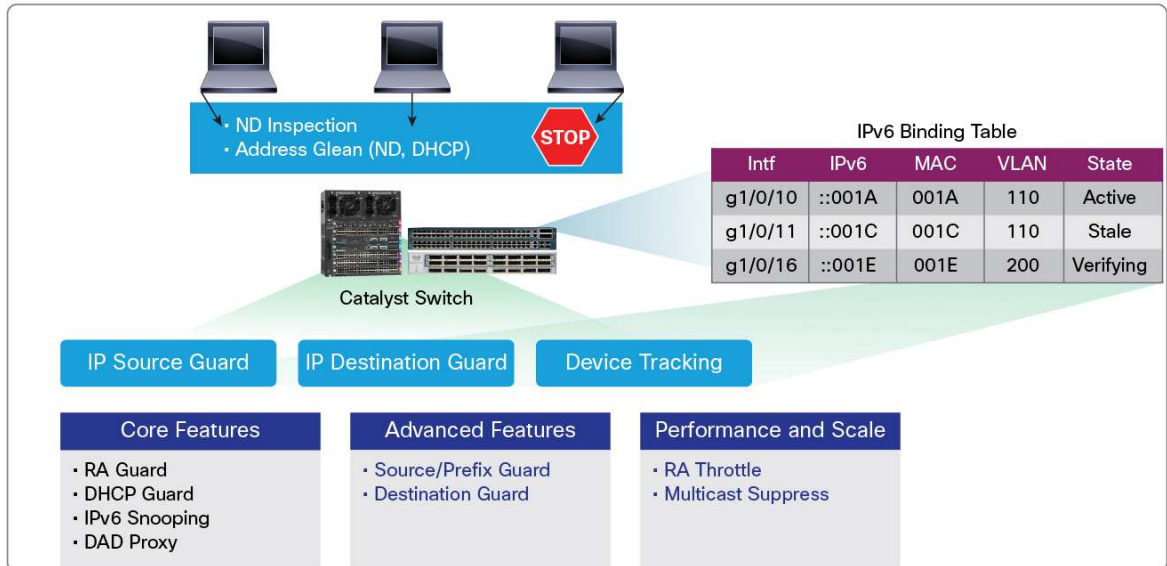
- **Source and Prefix Guard:** IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses Dynamic Host Configuration Protocol (DHCP) snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. This support is now available on Cisco Catalyst 4500E, 4500-X, and 4900M/4948E/E-F platforms.
- **Destination Guard:** The switch maintains "incomplete" entries for unresolved addresses in its binding table. Excessive scanning for large address resolution can cause denial of service, leading to binding table exhaustion. Destination Guard prevents against this. This support is now available on the Cisco Catalyst 3750-X and the 3560-X.

Networks with large numbers of devices face a number of scale challenges, such as effective and efficient address resolution. For example, in wireless Layer 2 domains, bandwidth might be constrained, and the amount of control traffic generated by protocols such as IPv6 Neighbor Discovery (ND) or Multicast Listener Discovery (MLD) can quickly become prohibitive. IPv6 FHS provides for features that help control performance and scale on such low-bandwidth networks. These features include:

- **RA Throttler:** This feature throttles the number of multicast RAs circulating on low-bandwidth networks.
- **Neighbor Discovery (ND) Multicast Suppress:** This feature stops as many multicast neighbor solicitations (NSs) as possible circulating on low-bandwidth networks.
- **Lightweight DHCPv6 Relay Agent (LDRA):** This feature allows relay agent information to be inserted by an access switch that performs a link-layer bridging (nonrouting) function. This is used to insert relay agent options in DHCPv6 message exchanges primarily to identify client-facing interfaces. LDRA functionality can be enabled on an interface and on a VLAN.

Figure 2 shows IPv6 FHS support of Cisco Catalyst switches.

**Figure 2.** IPv6 FHS Support on Cisco Catalyst Switches



IPv6 First Hop Security – Support in Catalyst 3K-X, 4500E/X, 49xx Switches

Feature	Catalyst 4500E (Sup 6/7), 4500X	4900M, 4948E, and 4948E-F	Catalyst 3K-X	2960S/SF, 2960CG*, 3560CG, (LAN-Base only)
RA Guard	✓	✓	✓	✓
DHCPv6 Guard	✓	✓	✓	✓
IPv6 Snooping	✓	✓	✓	✓
Source Guard	⊙	⊙	✓	x
Destination Guard	✓	✓	⊙	x
DHCPv6 LDRA	✓	✓	⊙	x
DAD Proxy	✓	✓	⊙	x
Prefix Guard	⊙	⊙	⊙	x

\* 2K, Compact LAN-Lite license levels & Compact 10/100 SKUs do not support IPv6 FHS

⊙ : New in XE-3.5.0E/15.2(1)E    ✓ : Already Supported    x : Unsupported

## Cisco TrustSec

### SGT/SGACL

Cisco TrustSec® is an intelligent access control solution mitigating security risks by providing comprehensive visibility into who and what are connecting across the entire network infrastructure. A combination of SGT (tagging) and SGACL (access control) lists provide role-based rather than IP subnet-based access control. In addition to SGT/SGACL, the release also provides for SGT eXchange Protocol (SXP).

---

SGT/SGACL has been supported on the Cisco Catalyst 3750 and 3560 platform since the Cisco IOS Software 15.0(2)SE release. Now the Cisco IOS XE Software 3.5.0E release brings SGT/SGACL support to the Cisco Catalyst 4500E. In addition to the basic features and functionality of SGT/SGACL, the release also introduces the following features that enhance the capability:

- **Cisco TrustSec VLAN to SGT mapping** to co-relate source SGT with source VLAN in VLAN-based environments
- **IP address to SGT mapping** to co-relate source SGT with source IP address enforcing appropriate SGACL
- **Port to SGT mapping** to tag all traffic from a specific interface/port

#### **MACSec Encryption on Cisco Catalyst 4500-X**

Cisco MACSec makes sure of data confidentiality and integrity of all wired network traffic, whereas the "hop by hop" nature of MACSec preserves traffic visibility and allows NetFlow, QoS, and other Layer 2 technologies to work alongside the network encryption. Cisco IOS XE Software 3.5.0E will provide support for following MACSec features:

- IEEE 802.1ae MACSec Layer 2 encryption
- IEEE 802.1ae MACSec encryption on user-facing ports
- IEEE 802.1ae MACSec encryption between switch-to-switch links using Cisco Security Association Protocol (SAP)

#### **MAC Authentication Bypass (MAB): Configurable User Name and Password**

This feature allows the user to configure the format of the MAC address used in the username and password fields in the RADIUS access-request packet for MAB authentication. This allows easy interoperability with RADIUS servers or MAC databases that expect the MAC address in a different format than provided by the switch as default.

#### **Virtualization**

##### **VRF-Aware Support for EIGRPv6, OSPFv3, and BGPv6**

With networks beginning to migrate to IPv6, the Cisco IOS XE Software 3.5.0/15.2(1)E release now extends IPv6 VRF-Lite capability for EIGRPv6, OSPFv3, and BGPv6 routing protocols on Cisco Catalyst 4500E, 4500-X, 3750-X, and 3560-X platforms.

This feature allows configuration of multiple VRFs and simplifies the management and troubleshooting of traffic belonging to a specific VRF. VRF-Lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Physical Ethernet ports or logical interfaces such as VLAN SVIs are supported.

##### **Bidirectional Forwarding Detection (BFD) Support for Routing Protocols**

In enterprise networks, the convergence of business-critical applications is dependent upon the ability of individual network devices to quickly detect failures and reroute traffic to an alternate path. Bidirectional Forwarding Detection (BFD) provides rapid failure detection times, while maintaining low overhead. BFD may be used on many different underlying transport mechanisms and layers and operates independently of all of these.

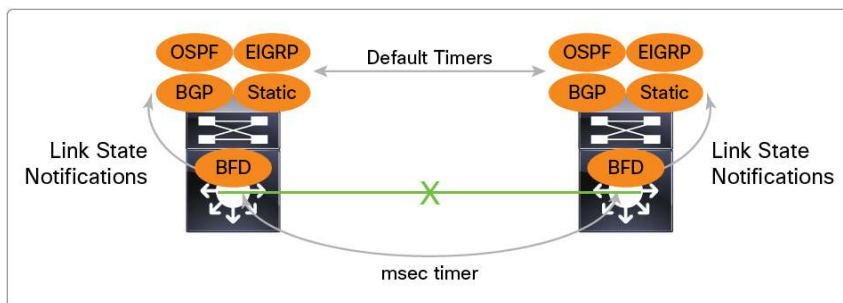
The Cisco IOS XE Software 3.5.0E and 15.2(1)E release now provides IPv4- and IPv6-based BFD support for static routes and for dynamic routing protocols encompassing BGP, EIGRP, and OSPF. BFD provides short-duration detection of failures in the forwarding path between two adjacent routing instances, leading to subsecond link-failure detection. The Cisco BFD implementation supports the BFD asynchronous mode using echo and control packets, allowing it to detect and react to media or protocol failures in ~100 milliseconds.

BFD is supported on directly connected routed, SVI, and port-channel interfaces, including MACSec encrypted links.

**Note:** IPv4 and IPv6 BFD support for Cisco Catalyst 4900M, 4948E, and 4948E-F was introduced in the Cisco IOS XE Software 3.3.0SG release.

Figure 3 shows BFD for routing protocols.

**Figure 3.** BFD for Routing Protocols



## Operational Simplicity and Lower Total Cost of Ownership

### Smart Install with Configuration-Only Deployment and Smooth Upgrade

When added to the network, new Smart Install clients download an image and configuration. In many customer networks, downloading and installing an image are not required and unnecessarily add time to the deployment process.

Currently, Smart Install mandates that the image and configuration be provided during zero-touch upgrade, necessitating the switch to be rebooted with both the configuration and image. However, sometimes the customer only prefers the configuration to be updated. Additionally, in a Smart Install on-demand action, the user might want to revert to a previous or default configuration in the event that the image or configuration upgrade fails for any reason.

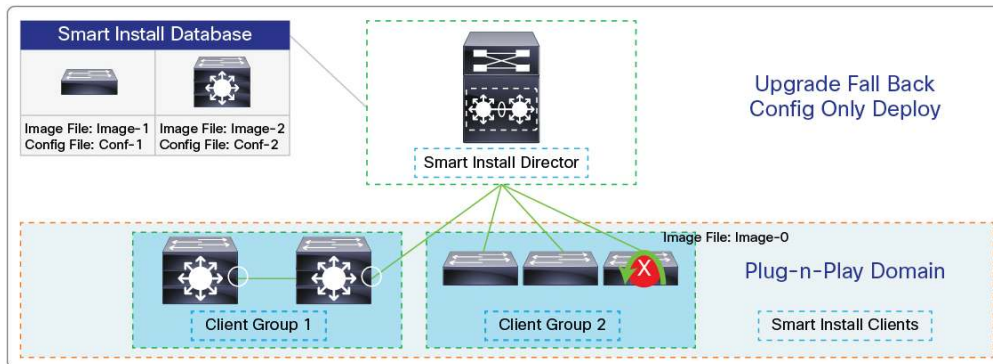
This release expands Smart Install to provide for a mode that allows for configuration-only deployment. This mode is configured on the director as an alternative to specifying a specific image file. Clients in a configuration-only group will download and apply a configuration file, but will not download an image. This release further provides the option for the client to use a previous or default configuration (based on Smart Install group), allowing the client to notify the director of such a reversal.

Together these features dramatically reduce deployment times for Smart Install, either in the case of an upgrade or when the user wants to revert back to an earlier image (for example, when an upgrade fails).



Figure 4 illustrates a Smart Install upgrade fallback and configuration-only deployment.

**Figure 4.** Smart Install Upgrade Fallback and Configuration-Only Deployment



### Cisco Service Discovery Gateway

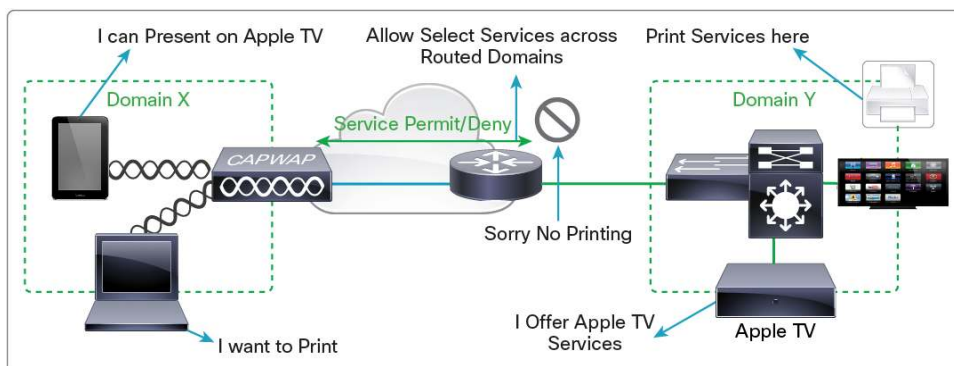
With the emergence of wireless LANs, a modern campus network can expect to have devices removed and added frequently, resulting in the need for increasingly dynamic and automatic configuration. Zero configuration provides a set of means and technologies that do not require manual intervention or special configuration servers.

A common example of zero-configuration networking is Apple Bonjour, which uses the mDNS capability to locate devices and the services that they offer, allowing users to set up a network without any configuration. The issue with practically all zero-configuration networking approaches is that they offer such services only across a single L2 domain. That restricts use of the resource-advertising service to only that one network domain, which doesn't work when users are highly mobile.

The Cisco Service Discovery Gateway feature on the Cisco Catalyst 3750-X/3560-X and the 4500E (Supervisor Engine 7E/LE) and 4500-X helps overcome this issue. The Cisco Service Discovery Gateway solution listens to service announcements on all configured network segments and builds a cache of services and corresponding addresses. Then, it can be configured to proxy these requests to other segments and apply filters based on various service attributes. These filters can limit which services will be seen or allowed to be advertised.

Figure 5 illustrates zero configuration and Cisco Service Discovery Gateway implementation.

**Figure 5.** Zero Configuration and Cisco Service Discovery Gateway Implementation



The Cisco Service Discovery Gateway allows for transparent integration of devices that offer services with those that use services, even if they are not connected to the same broadcast domain. Administrators can easily manage which services are to be advertised, or withdrawn, on a particular segment by applying filters.

Specifically, the Service Discovery Gateway feature provides:

- The ability to filter services based on criteria such as:
  - Service type
  - Instance name
  - Message type
- Granular application on either a global or per-interface basis
- IPv4 and IPv6 support

### **Multicast VLAN Registration (MVR) for Cisco Catalyst 4500E**

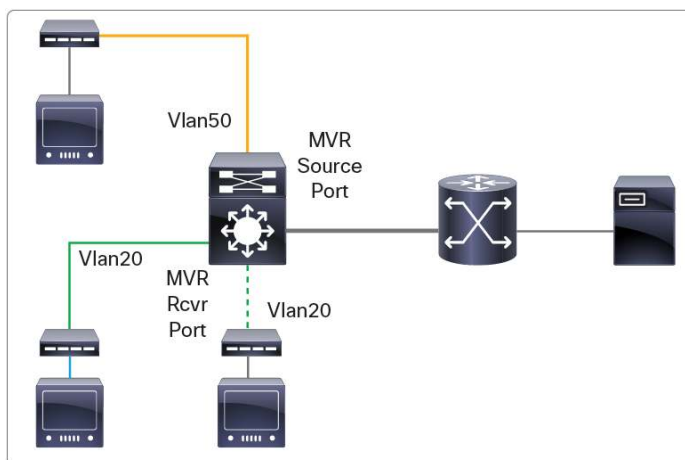
With increasing use of video on the network, multicast traffic has seen a dramatic rise on the LAN. With content-based (for example, triple play) providers, this service is now extensively seen over the last-mile networks of service providers. With networks expanding across VLAN, even the use of IGMP snooping does not provide any benefits because the switch multicasts traffic to all VLANs.

MVR is a protocol for Layer 2 (IP) networks that enables multicast traffic from a source VLAN to be shared with subscriber VLANs. MVR follows the same principle as that of IGMP snooping, but operates with hosts on different VLANs in a Layer 2 network to selectively deliver multicast traffic to requesting hosts, thereby reducing the amount of bandwidth needed to forward multicast traffic.

The Cisco IOS XE Software 3.5.0E/15.2(1)E release provides support for MVR across the 4500E (with Supervisor Engines 6 and 7) and the Cisco Catalyst 4500-X platform complementing the current support on the Cisco Catalyst 3750-X.

Figure 6 illustrates MVR on the Cisco Catalyst 4500E.

**Figure 6.** MVR on Cisco Catalyst 4500E





PIM routers in a domain must be able to map each multicast group to the correct rendezvous point (RP) address. The BSR protocol for PIM sparse mode (PIM SM) provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected, and the mapping tables will be modified so that the unreachable RP is no longer used and new tables will be rapidly distributed throughout the domain.

The BSR Scoped Zone Support feature enhances IPv6 BSR, allowing for distributing group to RP mappings in networks using administratively scoped multicast. It allows the operator to configure candidate BSRs and a set of candidate RPs for each administratively scoped region in a domain.

**Right-to-use (RTU) software licensing:** Cisco IOS XE Software Release 3.5.0E/15.2(1)E now simplifies software licensing with the introduction of right-to-use (RTU) licensing that allows the user to order and activate a specific license type and level and then manage license usage on switches.

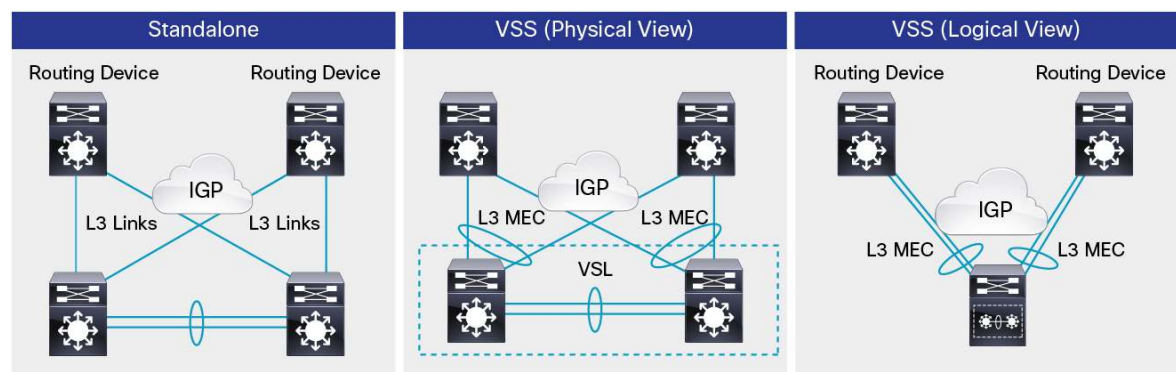
## Resiliency

### Enhancing Virtual Switching System (VSS) Support on Cisco Catalyst 4500E (Supervisor Engine 7-E and 7L-E) and 4500-X Series Switches

The Cisco IOS XE Software release 3.4.0SG introduced support for VSS on the Cisco Catalyst 4500E and Cisco Catalyst 4500-X. The Cisco IOS XE Software 3.5.0E release enhances the VSS support by providing the following features:

- **Support for L3-MEC:** VSS with Layer 3 Multichassis EtherChannel (MEC) at the aggregation layer simplifies the managing, tuning, and troubleshooting of routing protocols by reducing the neighbor counts and routing table entries. This greatly reduces CPU load. The physical and logical views of VSS with support for L3-MEC are presented in Figure 7.

**Figure 7.** VSS Physical View Showing Physical Connectivity



**Classic line-card support:** Beginning with the Cisco IOS XE Software 3.5.0 E/15.2(1)E release, the Cisco Catalyst 4500E VSS now provides support for classic line cards (earlier generation), leading to complete investment protection, and significantly reduces capital expenditures (CapEx). The line cards listed in Table 1 are supported with the Cisco Catalyst 4500E VSS with Supervisor Engine 7 or Supervisor Engine 6 (for example, if an upgrade failed).

**Table 1.** Classic Line Cards Supported on VSS System

WS-X4306-GB	WS-X4548-RJ45V+
WS-X4232-L3	WS-X4448-GB-SFP
WS-X4248-RJ45V	WS-X4248-FE-SFP
WS-X4148-FX-MT	WS-X4148-RJ

**Note:** The preceding line-card ports cannot be configured as part of VSL.

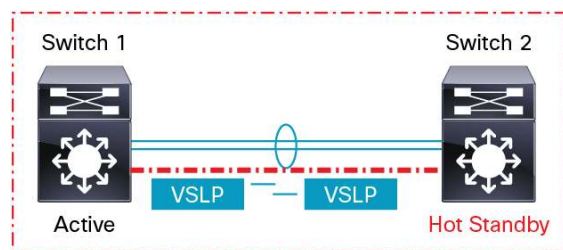
- **Support for asymmetric chassis:** Now Cisco Catalyst 4500E VSS can be formed between chassis that have different numbers of slots (for example, VSS can be formed between a 3-slot and 6-slot chassis). This feature still requires that the supervisor engines on both chassis should be the same to meet SSO requirements.

**Note:** This feature is not supported on the Cisco Catalyst 4500-X (VSS cannot be formed between 16-port and 32-port 4500-X fixed switches).

- **Support for VSLP Fast Hello:** With the VSLP Fast Hello feature, the Cisco Catalyst 4500-E or 4500-X VSS can be connected to access switches that do not support ePAgP protocol. This helps in achieving subsecond failover time.

Figure 8 illustrates subsecond convergence with VSLP Fast Hello.

**Figure 8.** Subsecond Convergence with VSLP Fast Hello



In addition to the preceding features, Release 3.5.0E/15.2(1)E now provides support for Smart Install Director capability in conjunction with VSS, leading to zero-touch installation without any convergence downtime.

## Compliance and Certifications

Different organizations across the world have standards for compliance: some related to security, some related to IPv6, and so on. These include USGv6, JITC, Common Criteria, and FIPS140-2, to name a few. Among a number of enhancements that are available as a part of the Cisco IOS XE Software 3.5.0E/15.2(1)E release, the following points help with compliance to one or more standards:

- **Hop-hop extensions filtering and throttling:** As per the IPv6 protocol definition, the Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. For traffic with a chain of extension headers going through a Layer 3 interface that has packet filtering (access lists) applied to it, the router must hop from one extension header to the other until it gets to it, and this can be used by a malicious user to slow forwarding performance of such a switch.

---

The IPv6 ACL Extensions for hop-by-hop filtering feature allows the user to control IPv6 traffic that might contain hop-by-hop extension headers. One can configure an access-control list (ACL) or a class map to throttle or deny all hop-by-hop traffic or to selectively permit traffic based on protocol.

- **Common Criteria and FIPS140-2 Evaluation:** The Common Criteria (CC) is an international standard for computer security certification in which products are evaluated at a level that is commensurate with the target environment for use (based on appropriate protection profiles).

Through this release, the Cisco Catalyst 4500E (Supervisor Engine 7E/LE) and the Cisco Catalyst 4500-X are evaluated for the network device protection profile (ND\_PP\_V1) at level EAL 3 as also compliant to the FIPS140-2 requirements.

Other capabilities that are introduced to support the compliance needs for different standards include support for:

- ICMP RFCs 4291, 4443, 3484, 2526, 4861, 4862, 5095, 4007, and 3513
- UDP MIB (RFC 4113) and TCP MIB (RFC 4022)
- IPv6 support for IP MIB (RFC 4292) and IP forwarding MIB (RFC 4293)
- IPv6 MIB for Diffserv
- IPv6 tunnel over IPv4

## Packaging Changes

To provide consistency of packaging across Cisco Catalyst 3K and 4K platforms, the following packaging changes have been added in the release:

- Support for IPv4 PIM routing (full) has been extended from Enterprise Services to IP Base feature set for Cisco Catalyst 3K platforms.
- Support for IPv4 and IPv6 PIM routing have been extended from Enterprise Services to IP Base feature set for Cisco Catalyst 3K and 4K platforms.
- Support for IPv4 PBR support has been extended from Enterprise Services to IP Base feature set for Cisco Catalyst 3K and 4K platforms.
- Support for IPv6 EIGRP stub routing support has been introduced with IP Base feature set for Cisco Catalyst 4K and 3K platforms.
- Number of routes supported with OSPF routed access in IP Base feature set has been increased from 200 to 1000, it is applicable for both Cisco Catalyst 3K and 4K platforms.

## Other Features

Some other new feature additions include:

- Support for EIGRP wide metrics
- SXP loop detection
- DHCP glean for device sensor
- EIGRP features:
  - EIGRP IPv6 NSF/GR
  - EIGRP MIB
  - EIGRP IPv6 MIBs

- Route Tag Enhancements
- Generate SNMP trap when EIGRP neighbor is down
- Disable IPX in EIGRP
- EIGRP add-path
- EIGRP wide metrics
- OSPFv3 features:
  - OSPFv3 BFD
  - OSPFv3 Graceful Shutdown
  - OSPFv2 NSSA
  - OSPFv3 NSSA Option
  - OSPFv3 External Path Preference
  - OSPFv3 Router Max metric Router LSA
  - OSPFv3 Retransmission Limit
  - OSPFv3 MIB
  - OSPFv3 Prefix Suppression
  - Area Filter/DC Ignore
- HSRP-aware PIM
- IPv6 Global entries for unsolicited NA
- IPv6 ND cache expire
- Option to configure exponential back-off for NS timer used in NUD
- IPv6 support for TFTP
- DNS over IPv6
- BGP features:
  - BGP support for malformed attribute error handling
  - BGP support for Cisco-BGP-MIBv2
  - BGP support for graceful shutdown
  - BGP support for Add-Path
  - BGP support for VRF dynamic route leaking (for VRF lite)
- ISISv6 on 3K-X
- BGPv6 on 3K-X
- Configurable TCP Keep Alive timer
- Hop by Hop EH ACL Throttling
- CISCO-EMBEDDED-EVENT-MGR-MIB
- SNMP-COMMUNITY-MIB
- OSPF MIB
- Cisco Dynamic Arp Inspection MIB
- Digital Optical Monitoring (DOM) MIB

## Hardware Features

### Support for Cisco SFP+ Modules on the Cisco Catalyst Switches

This release enables the support of the following modules across the Cisco Catalyst switching platforms as below.

**Table 2.** Matrix of Supported SFP+ Modules on Cisco Catalyst Switches in XE 3.5.0E/15.2(1)E

SFP+ Modules vs Platforms	2960-S	2960-C	3560-X/3750-X	3560-C	4500 (Sup7E/LE) & 4500-X	4500E (Sup6E/LE)
<b>GLC-T</b>	Yes	Yes	Yes	Yes	Already Supported**	Already Supported
<b>GLC-GE-100FX</b>	Yes	Yes	Yes*	Yes	Yes**	NA
<b>DWDM SFP+</b>	Yes	NA	Yes	NA	Already Supported	Already Supported
<b>SFP+ ZR</b>	Yes	NA	Yes	NA	Already Supported	Already supported

\* 3K-X: Not Supported on C3KX-SM-10G aka WallE Modules

\*\* 4500X: Support only on 1000Mbps ports

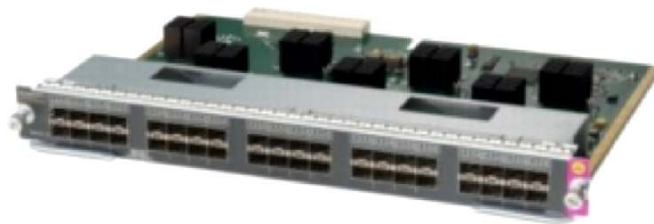
### Digital Optical Monitoring (DOM) Support for SFP and SFP+ Modules

All Cisco Catalyst switches support DOM as per the standard SFF-8724 multisource agreement (MSA). This feature is also known as digital optical monitoring (DOM). Modules with this capability give the end user the ability to monitor parameters of the SFP in real time, such as optical output power and optical input power, among others. These parameters are monitored against the threshold values that allow the user to view the threshold violation messages.

### Support for WS-X4640-CSFP-E on 10-Slot 4500E Chassis

The Cisco IOS XE Software 3.5.0E/15.2(1)E release enables the support of the following WS-X4640-CSFP-E on the Cisco Catalyst 4500E 10-slot chassis. (See Figure 9 and Table 3.) The support is enabled with Supervisor Engine 6E/LE and 7E/LE. The WS-X4640-CSFP-E provides up to 40 SFP ports into which customers can mix and match Gigabit SFP and compact SFP modules, providing point-to-point fiber to the home (FTTH) or building (FTTB) for residential and business applications or fiber to the desktop (FTTD).

**Figure 9.** WS-X4640-CSFP-E Module Support on 10-Slot Cisco Catalyst 4500E



**Table 3.** Matrix of Supported Features

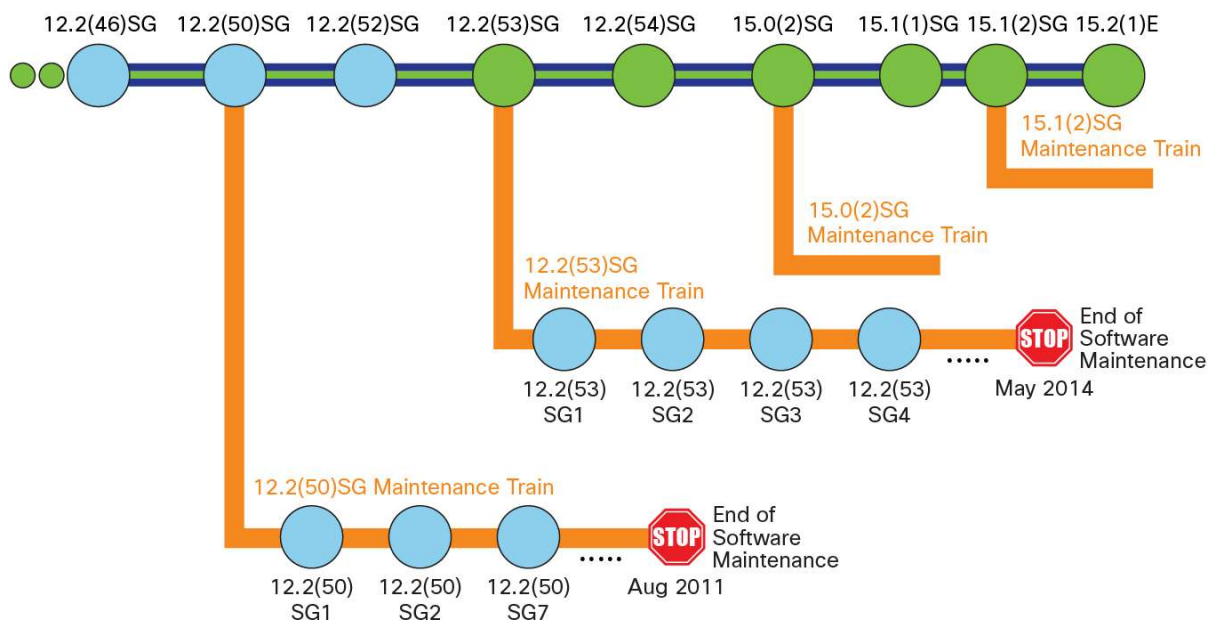
Feature	Platform					
	Cisco Catalyst 3750-X/3560-X	Cisco Catalyst 4500E (Supervisor Engine 7E and 7L-E)	Cisco Catalyst 4500E (Supervisor Engine 6E and 6L-E)	Cisco Catalyst 4500-X	Cisco Catalyst 4948E/4948E-F	Cisco Catalyst 4900M
<b>Cisco VSS Phase II</b>	NA	7E (IP Base) Supervisor Engine 7L-E (Ent Svcs)	NA	IP Base	NA	NA

Feature	Platform					
	Cisco Catalyst 3750-X/3560-X	Cisco Catalyst 4500E (Supervisor Engine 7E and 7L-E)	Cisco Catalyst 4500E (Supervisor Engine 6E and 6L-E)	Cisco Catalyst 4500-X	Cisco Catalyst 4948E/4948E-F	Cisco Catalyst 4900M
IPv6 First Hop Security II	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base
Smart Install Enhancements	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base
VRF-Lite for IPv6 on OSPF/BGP/EIGRP	IP Services	Enterprise Services	Enterprise Services	Enterprise Services	Enterprise Services	Enterprise Services
IPv6/v4 BFD with OSPF/BGP/EIGRP and Static	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base
Cisco TrustSec SGT/SGA Support	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base
Medianet (MSP and Metadata)	IP Services	Enterprise Services	Enterprise Services	Enterprise Services	Enterprise Services	Enterprise Services
Cisco Service Discovery Gateway Support	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base	LAN Base

## Cisco IOS Software Release Trains for Cisco Catalyst 4500 Series Switches

Cisco IOS Software Release 15.2(1)E and Cisco IOS XE Software Release 3.5.0E are part of a scheduled time-based release containing new hardware and software features as shown in Figures 10 and 11.

**Figure 10.** Cisco IOS Software Release Trains for Cisco IOS Software Release 15.2(1)E



**Figure 11.** Cisco IOS Software Release Trains for Cisco IOS XE Software Release 3.5.0E



For configuration details and information about the new features in Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E, refer to the release notes at:

- Cisco IOS XE Software 3.5.0E release notes for:
  - [Cisco Catalyst 4500E \(with Supervisor Engine 7-E/7L-E\)](#)
  - [Cisco Catalyst 4500-X](#)
- Cisco IOS Software 15.2(1)E release notes for:
  - [Cisco Catalyst 2960S](#)
  - [Cisco Catalyst 3750-X and 3560-X](#)
  - [Cisco Catalyst 4500E \(with Supervisor Engine 6-E/6L-E\)](#)
  - [4900M, 4948E, and 4948E-F](#)

## Support

Support for Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E follows the standard Cisco support policy, available at [http://www.cisco.com/en/US/products/products\\_end-of-life\\_policy.html](http://www.cisco.com/en/US/products/products_end-of-life_policy.html).

For more information about the Cisco Catalyst 4500E Series, visit <http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>.

For more information about the Cisco Catalyst 4500-X Series, visit <http://www.cisco.com/en/US/products/ps12332/index.html>.

For more information about the Cisco Catalyst 4900M Series, visit <http://www.cisco.com/en/US/products/ps9310/index.html>.

For more information about the Cisco Catalyst 2960-X, 3750-X and 3650-X Series, visit <http://www.cisco.com/en/US/products/ps12995/index.html>.  
<http://www.cisco.com/en/US/products/ps10745/index.html>.  
<http://www.cisco.com/en/US/products/ps10744/index.html>.

For more information about the Cisco Catalyst C2960 and C3650 Series, visit [http://www.cisco.com/en/US/products/ps11527/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps11527/Products_Sub_Category_Home.html).



## Ordering Information

Tables 4 through 7 provide product numbers and ordering information for Cisco IOS XE Software Release 3.5.0E and Cisco IOS Software Release 15.2(1)E.

**Table 4.** Cisco IOS XE Software Release 3.5.0E Product Numbers and Images for Cisco Catalyst 4500E Series Switches with Supervisor Engine 7-E/7L-E

Product Number	Description	Image
<b>S45EU-35-1521E</b>	Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E universal image	cat4500e-universal.SPA.03.05.00.E.152-1.E.bin
<b>S45EUK9-35-1521E</b>	Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E universal crypto image	cat4500e-universalk9.SPA.03.05.00.E.152-1.E.bin
<b>S45EUN-35-1521E</b>	Cisco Catalyst 4500E Supervisor Engine 7-E and Supervisor Engine 7L-E universal no MACSec image	cat4500e- cat4500e-universalk9npe.SPA.03.05.00.E.152-1.E.bin

**Table 5.** Cisco IOS Software Release 15.2(1)E Product Numbers and Images for Cisco Catalyst 4500E Series Switches with Supervisor Engine 6E/6L-E

Product Number	Description	Image
<b>S45ELB-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E (LAN Base image)	cat4500e-lanbase-mz.152-1.E.bin
<b>S45ELBK9-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E (LAN Base image with 3DES)	cat4500e-lanbasek9-mz.152-1.E.bin
<b>S45EIPB-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500 Supervisor Engine 6-E and Supervisor Engine 6L-E (IP Base image)	cat4500e-ipbase-mz.152-1.E.bin
<b>S45EIPBK9-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500E Supervisor Engine 6-E and Supervisor Engine 6L-E (IP Base image with 3DES)	cat4500e-ipbasek9-mz.152-1.E.bin
<b>S45EES-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500E Supervisor Engine 6-E and Supervisor Engine 6L-E (Enterprise Services image)	cat4500e-entservices-mz.152-1.E.bin
<b>S45EESK9-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500E Supervisor Engine 6-E and Supervisor Engine 6L-E (Enterprise Services image with 3DES)	cat4500e-entservicesk9-mz.152-1.E.bin
<b>S45EESU-15201E(=)</b>	Cisco IOS Software Enterprise image upgrade from LAN Base for the Supervisor Engine 6-E and Supervisor Engine 6L-E	cat4500e-entservices-mz.152-1.E.bin
<b>S45EESUK9-15201E(=)</b>	Cisco IOS Software Enterprise with 3DES upgrade from LAN Base for the Supervisor Engine 6-E and Supervisor Engine 6L-E	cat4500e-entservicesk9-mz.152-1.E.bin
<b>S45EIPBU-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500E Series Supervisor Engine 6-E and Supervisor Engine 6L-E, Cisco Catalyst 4948E Cisco IOS Software IP Base upgrade	cat4500e-ipbase-mz.152-1.E.bin
<b>S45EIBUK9-15201E(=)</b>	Cisco IOS Software for the Cisco Catalyst 4500E Series Supervisor Engine 6-E and Supervisor Engine 6L-E, Cisco Catalyst 4948E Cisco IOS Software IP Base upgrade SSH	cat4500e-ipbasek9-mz.152-1.E.bin

**Table 6.** Cisco IOS XE Software Release 3.5.0E Product Numbers and Images for Cisco Catalyst 4500-X Series Switches

Product Number	Description	Image
<b>S45XU-35-1521E</b>	Cisco Catalyst 4500-X universal image	cat4500e-universal.SPA.03.05.00.E.152-1.E.bin
<b>S45XUK9-35-1521E</b>	Cisco Catalyst 4500-X universal crypto image	cat4500e-universalk9.SPA.03.05.00.E.152-1.E.bin

**Table 7.** Cisco IOS Software Release 15.2(1)E Product Numbers and Images for Cisco Catalyst 4900 Series Switches

Product Number	Description	Image
<b>S49EES-15201E(=)</b>	Cisco CAT4900 IOS ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz.152-1.E.bin
<b>S49MES-15201E(=)</b>	Cisco CAT4900M IOS ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz.152-1.E.bin
<b>S49EESK9-15201E(=)</b>	Cisco CAT4900 IOS ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz.152-1.E.bin

Product Number	Description	Image
<b>S49MESK9-15201E(=)</b>	Cisco CAT4900M IOS ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz.152-1.E.bin
<b>S49EIPB-15201E(=)</b>	Cisco CAT4900 IOS IP BASE W/O CRYPTO	cat4500e-ipbase-mz.152-1.E.bin
<b>S49MIPB-15201E(=)</b>	Cisco CAT4900M IOS IP BASE W/O CRYPTO	cat4500e-ipbase-mz.152-1.E.bin
<b>S49EIPBK9-15201E(=)</b>	Cisco CAT4900 IOS IP BASE SSH	cat4500e-ipbasek9-mz.152-1.E.bin
<b>S49MIPBK9-15201E(=)</b>	Cisco CAT4900M IOS IP BASE SSH	cat4500e-ipbasek9-mz.152-1.E.bin
<b>S49ELB-15201E(=)</b>	Cisco CAT4900 IOS LAN BASE W/O CRYPTO	cat4500e-lanbase-mz.152-1.E.bin
<b>S49ELBK9-15201E(=)</b>	Cisco CAT4900 IOS LAN BASE SSH	cat4500e-lanbasek9-mz.152-1.E.bin

**Table 8.** Cisco IOS Software Release 15.2(1)E Product Numbers and Images for Cisco Catalyst C2960 and C3560 Series Switches

Product Number	Description	Image
<b>S29CVK9T-15201E(=)</b>	CAT 2960C405 IOS UNIVERSAL WITH WEB BASED DEV MGR	c2960c405-universalk9-tar.152-1.E.tar
<b>S296VK9T-15201E(=)</b>	CAT 2960C405EX IOS UNIVERSAL WITH WEB BASED DEV MGR	c2960c405ex-universalk9-tar.152-1.E.tar
<b>S35CVK9T-15201E(=)</b>	CAT 3560C405 IOS UNIVERSAL WITH WEB BASED DEV MGR	c3560c405-universalk9-tar.152-1.E.tar
<b>S35CVK9TN-15201E(=)</b>	CAT 3560C405 IOS UNIVERSAL WITH WEB BASED DEV MGR	c3560c405-universalk9npe-tar.152-1.E.tar

**Table 9.** Cisco IOS Software Release 15.2(1)E Product Numbers and Images for Cisco Catalyst 3750-X and 3560-X Series Switches

Product Number	Description	Image
<b>S356XVK9T-15201E</b>	CAT 3560X IOS UNIVERSAL WITH WEB BASED DEV MGR	c3560e-universalk9-tar.152-1.E.tar
<b>S356XVK9TN-15201E</b>	CAT 3560X IOS UNIVERSAL NO MACSEC WITH WEB BASED DEV MGR	c3560e-universalk9npe-tar.152-1.E.tar
<b>S375XVK9T-15201E</b>	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	c3750e-universalk9-tar.152-1.E.tar
<b>S375XVK9TN-15201E</b>	CAT 3750X IOS UNIVERSAL NO MACSEC WITH WEB BASED DEV MGR	c3750e-universalk9npe-tar.152-1.E.tar
<b>S356XSMK9T-15201E</b>	CAT 3560X IOS SOFTWARE IMAGE FOR SERVICE MODULE C3KX-SM-10G	c3kx-sm10g-tar.152-1.E.tar
<b>S375XSMK9T-15201E</b>	CAT 3750X IOS SOFTWARE IMAGE FOR SERVICE MODULE C3KX-SM-10G	c3kx-sm10g-tar.152-1.E.tar



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](http://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](http://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)