Product Bulletin No. 3257

Cisco IOS Software Release 12.2(31)SG for Cisco Catalyst 4900 Series Switches

This product bulletin describes the hardware and software features supported by Cisco IOS® Software Release 12.2(31)SG for the Cisco® Catalyst® 4900 Series switches.

KEY FEATURE BENEFITS

- **Control Plane Policing (CoPP):** Protects the supervisor CPU by rate limiting and filtering out malicious traffic in hardware.
  - Ensures network stability and availability and predictable network performance by controlling the traffic to the supervisor CPU
- **Web Content Communication Protocol (WCCPv2) Layer 2 Redirection:** Transparently redirects content requests to directly connected content engines via a L2/MAC address rewrite.
  - Improves user response time and content availability by serving content locally on the LAN instead of the WAN
- **Network Admission Control (NAC) and 802.1x Enhancements** (MAC Authentication Bypass, 802.1x Inaccessible Authentication Bypass, 802.1x Unidirectional Controlled Port): Helps ensure that endpoints comply with security policies to protect networks against worms and viruses.
  - Increases flexibility of NAC and 802.1x deployments

NEW SOFTWARE FEATURES

Control Plane Policing

Control plane policing provides a unified solution to rate limit the CPU-bound control plane traffic in hardware. It enables users to install systemwide control plane access-control lists (ACLs) to protect the CPU by rate limiting or filtering out malicious denial-of-service (DoS) attacks. Control plane policing helps ensure network stability, availability, and packet forwarding. It prevents network outages such as loss of protocol updates, despite an attack or heavy load on the switch. Hardware-based control plane policing is available for Cisco Catalyst 4900 switches. It supports various Layer 2 and Layer 3 control protocols, such as Cisco Discovery Protocol (CDP), Extensible Authentication Protocol over LAN (EAPOL), Spanning Tree Protocol, Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), Internet Control Message Protocol (ICMP), Cisco Group Management Protocol (CGMP), Internet Group Management Protocol (IGMP), Dynamic Host Configuration Protocol (DHCP), Routing Information Protocol Version 2 (RIPv2), Open Shortest Pat First (OSPF), Protocol Independent Multicast (PIM), Telnet, Simple Network Management Protocol (SNMP), HTTP, and packets destined to 224.0.0.* multicast link local addresses. Predefined system policies or user-configurable policies can be applied to those control protocols. A staged approach is recommended for implementing the control plane policing by first understanding the traffic profile in the networks.

WCCPv2 L2 Redirection

Web Content Communication Protocol (WCCP) Version 2 Layer 2 redirection enables a Cisco Catalyst 4900 to transparently redirect content requests to the directly connected content engines using a Layer 2/MAC address rewrite. The WCCPv2 Layer 2 redirection is accelerated in the switching hardware and thus is more efficient than Layer 3 redirection using Generic Routing Encapsulation (GRE). The content engines in a cache cluster transparently store frequently accessed content and then fulfill successive requests for the same content, eliminating repetitive transmissions of identical content from the original content servers. It supports the transparent redirection of HTTP and non-HTTP traffic with well-known ports or dynamic services, such as Web caching, HTTPS caching, File Transfer Protocol (FTP) caching, proxy caching, media caching, and streaming services. WCCPv2 Layer 2 redirection is typically deployed for transparent caching at the network edge, such as regional or branch sites. WCCPv2

Layer 2 redirection cannot be enabled on the same input interface with Policy-Based Routing (PBR) or Virtual Route Forwarding (VRF)-lite. ACL-based classification for Layer 2 redirection is not supported.

MAC Authentication Bypass

MAC authentication bypass is an enhancement to Cisco Network Admission Control (NAC 2.0) Layer 2 802.1x. It provides network access to agentless devices without 802.1x supplicant capabilities, such as printers. Upon detecting a new MAC address on a switch port, the switch will proxy an 802.1x authentication request based on the device's MAC address. A database of MAC addresses is maintained by the RADIUS server for such devices. The device's network access is either granted or denied by the RADIUS server and is enforced by the switch. Per-port reauthentication of MAC addresses is also supported. MAC authentication bypass is typically deployed on switch ports connected to managed agentless devices without the 802.1x supplicant functionality.

802.1x Inaccessible Authentication Bypass

802.1x inaccessible authentication bypass is an enhancement to Cisco NAC 2.0 Layer 2 802.1x. In the event that the authentication, authorization, and accounting (AAA) servers are unreachable or nonresponsive, 802.1x user authentication typically fails with the port closed, and the user is denied access. 802.1x inaccessible authentication bypass provides a configurable alternative on the switch to grant a critical port network access in a locally specified VLAN. After the AAA servers become reachable again, those ports will either remain critically authorized or be reinitialized. 802.1x inaccessible authentication bypass can be enabled on a per-port basis for access ports, private VLAN host ports, or routed ports. 802.1x inaccessible authentication bypass is typically enabled on ports connected to critical devices, minimizing business impact for the duration of the AAA server outage.

802.1x Unidirectional Controlled Port

802.1x unidirectional controlled port allows the Wake-on-LAN (WoL) magic packets to reach a workstation attached to an unauthorized 802.1x switch port. WoL is typically used to push out OSs or software updates from a central server to workstations at night. When a workstation is powered down at night, the 802.1x switch port is not authenticated. The 802.1x unidirectional controlled port feature enables the one-way WoL magic packets to power on the sleeping workstation for the 802.1x authentication. It expands the WoL operations to workstations attached to 802.1x switch ports.

Private VLAN Promiscuous Trunk

Private VLANs (PVLANs) are an effective means of conserving IP address space while isolating Layer 2 traffic for devices residing within the same subnet. A promiscuous port in a PVLAN is an upstream port, carrying traffic between the upstream device in a primary VLAN and the downstream devices in secondary VLANs. Private VLAN promiscuous trunk extends the promiscuous port to a 802.1Q trunk port, carrying multiple primary VLANs (hence multiple subnets). Private VLAN promiscuous trunk is typically used to offer different services or content on different primary VLANs to isolated subscribers. Secondary VLANs cannot be carried over the private VLAN promiscuous trunk.

MAC Address Notification

MAC address notification monitors the MAC addresses that are learned by, aged out, or removed from the switch. Notifications are sent out or retrieved using the CISCO-MAC-NOTIFICATION MIB. It is typically used by a central network management application to collect such MAC address notification events for host moves. User-configurable MAC table utilization thresholds can be defined to notify any potential DoS or man-in-the-middle attack.

Voice VLAN Sticky Port Security

Port security restricts the MAC addresses allowed or the maximum number of MAC addresses on a switch port. Sticky port security extends port security by saving the dynamically learned MAC addresses in the running configuration to survive port link down and switch reset. Voice VLAN

sticky port security further extends the sticky port security to the voice-over-IP deployment. It locks a port and blocks access from a station with a MAC address different from the IP phone and the workstation behind the IP phone.

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is a standard-based first-hop redundancy protocol. With VRRP, a group of routers functions as one virtual router by sharing one virtual IP address and one virtual MAC address. The master router performs packet forwarding, while the backup routers stay idle. VRRP is typically used in a multivendor first-hop gateway redundancy deployment.

Secure Copy Protocol

Secure Copy Protocol (SCP) provides a secure and authenticated way to transfer files between a switch and a network management station. It uses the Secure Shell (SSH) Protocol as a transport mechanism for file copy operations. SCP is typically used for secure transfer of switch configurations and images. Both client side and server side of SCP are supported.

CISCO IOS SOFTWARE PACKAGING FOR THE CISCO CATALYST 4900 SERIES

A new Cisco IOS Software package for the Cisco Catalyst 4900 Series switches was introduced in Cisco IOS Software Release 12.2(25)SG. It is a new foundation for features and functionality and provides consistency across all Cisco Catalyst switches. The new Cisco IOS Software release train is designated as 12.2SG.

Prior Cisco IOS Software images for the Cisco Catalyst 4900 Series, formally known as “Basic Layer 3” and “Enhanced Layer 3” images, now map to “IP Base” and “Enterprise Services,” respectively. Border Gateway Protocol (BGP) is now included in the “Enterprise Services” image. Unless otherwise specified, all currently shipping Cisco Catalyst 4900 software features based on Cisco IOS Software are supported in the IP Base image of Release 12.2(31)SG, with a few exceptions:

The IP Base image does not support any enhanced routing related features (including BGP, EIGRP, OSPF, Intermediate System–to–Intermediate System (IS-IS) Protocol, Internetwork Packet Exchange [IPX] Protocol, AppleTalk, VRF-lite, and PBR).

The IP Base image supports EIGRP-Stub for limited routing on Cisco Catalyst 4900 Series switches. For more information about EIGRP-Stub functionality, go to http://www.cisco.com/en/US/technologies/tk648/tk365/technologies_white_paper0900aecd8023df6f.shtml

The Enterprise Services image supports all Cisco Catalyst 4900 Series software features based on Cisco IOS Software, including enhanced routing. BGP capability is included in the Enterprises Services package. Table 1 shows a more detailed description of the feature differences between the IP Base and Enterprise Services (ES) images as they relate to the Cisco Catalyst 4900 Series switches.

Table 1. Feature Comparison for Cisco IOS Software Release 12.2(31)SG IP Base and Enterprise Services

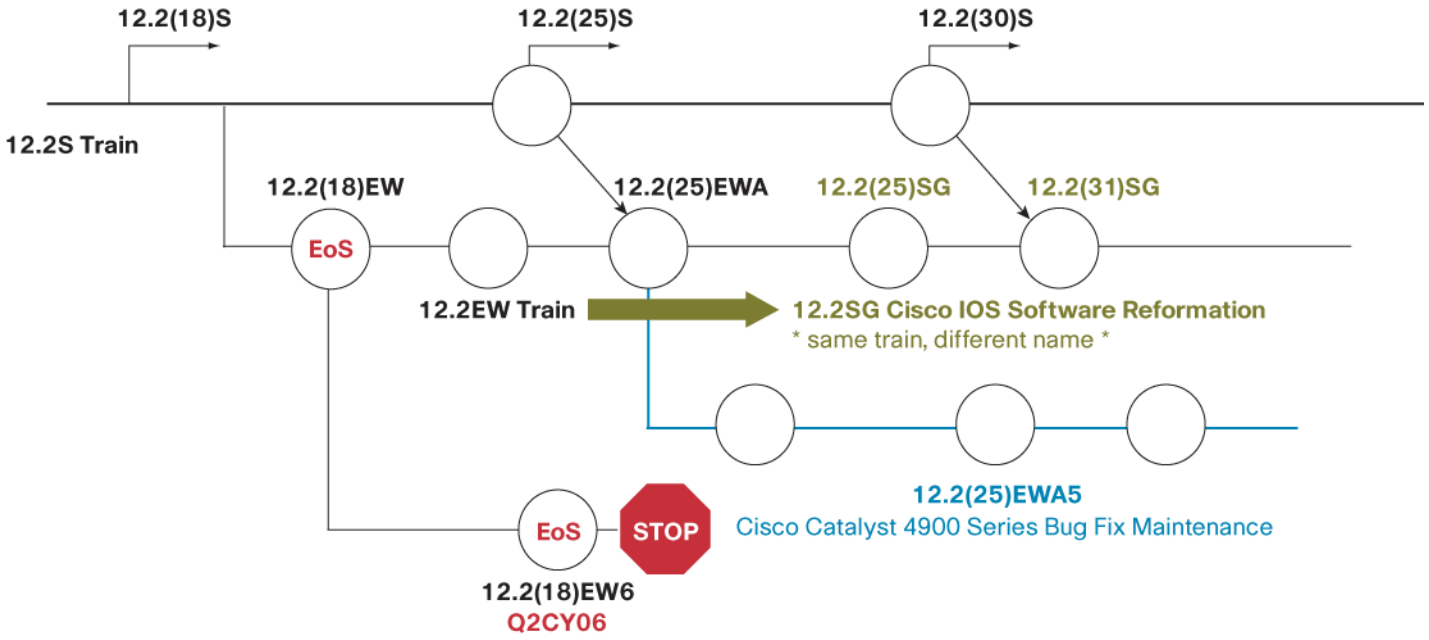
Feature	IP Base Image	Enterprise Services Image
NACv2.0	Yes	Yes
RIP and Static Route	Yes	Yes
NSF-aware	No	Yes
EIGRP	No	Yes
EIGRP-Stub	Yes	Yes
NSF-aware EIGRP-stub	Yes	Yes
OSPF/IS-IS	No	Yes
BGP	No	Yes

Feature	IP Base Image	Enterprise Services Image
VRF-lite	No	Yes
AppleTalk	No	Yes
IPX	No	Yes
PBR	No	Yes

CISCO CATALYST 4900 IOS SOFTWARE MIGRATION GUIDE

Figure 1 displays the Cisco IOS Software Release 12.2(31)SG plan relative to the 12.2S release train and identifies the recommended migration path.

Figure 1. Cisco IOS Software Release Plan for the Cisco Catalyst 4900 Series



* EoS: end of sale.

Summary of migration plan:

- Customers requiring the latest Cisco Catalyst 4900 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(31)SG.
- Cisco IOS Software Release 12.2(25)EWA will continue offering maintenance releases.

SUPPORT

Support for Cisco IOS Software Release 12.2(31)SG follows the standard Cisco Systems® support policy, available at http://www.cisco.com/en/US/products/products_end-of-life_policy.html.

For more information about the Cisco Catalyst 4900 Series, visit http://www.cisco.com/en/US/products/ps6021/index.html.

ORDERING INFORMATION

Tables 2 and 3 provide product numbers and ordering information for Cisco IOS Software Release 12.2(31)SG and supporting hardware.

Table 2. Cisco IOS Software Release 12.2(31)SG Product Numbers and Images

Product Number	Description	Image
S49IPB-12231SG	Cisco IOS Software for Cisco Catalyst 4900 Series switches (IP Base image)	cat4500-ipbase-mz
S49IPBK9-12231SG	Cisco IOS Software for Cisco Catalyst 4900 Series switches (IP Base image with Triple Data Encryption Standard [3DES])	cat4500-ipbasek9-mz
S49ES-12231SG	Cisco IOS Software for Cisco Catalyst 4900 Series switches (Enterprise Services image with BGP support)	cat4500-entservices-mz
S49ESK9-12231SG	Cisco IOS Software for Cisco Catalyst 4900 Series switches (Enterprise Services image with 3DES and BGP support)	cat4500-entservicesk9-mz

Table 3. Cisco IOS Software Release 12.2(31)SG Hardware Support

Product Number	Description
WS-C4948	Cisco Catalyst 4948 Switch, optional software image, optional power supplies, fan tray
WS-C4948-S	Cisco Catalyst 4948 Switch, IP Base Image, one AC power supply, fan tray
WS-C4948-E	Cisco Catalyst 4948 Switch, Enterprise Services Image, one AC power supply, fan tray
WS-C4948-10GE	Cisco Catalyst 4948-10GE Switch, optional software image, optional power supplies, fan tray
WS-C4948-10GE-S	Cisco Catalyst 4948-10GE Switch, IP Base Image, one AC power supply, fan tray
WS-C4948-10GE-E	Cisco Catalyst 4948-10GE Switch, Enterprise Services Image, one AC power supply, fan tray

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C25-338868-00 03/06