



Product Bulletin No. 3256

Cisco IOS Software Release 12.2(31)SG for Cisco Catalyst 4500 Series Supervisor Engines

This product bulletin describes the hardware and software features supported by Cisco IOS® Software Release 12.2(31)SG for the Cisco® Catalyst® 4500 Series Supervisor Engine II-Plus, II-Plus-TS, II-Plus-10GE, IV, V and V-10GE. The Cisco Catalyst 4500 Series Supervisor Engine III is not supported in this software release.

KEY FEATURE BENEFITS

- **Nonstop Forwarding with Stateful Switchover (NSF/SSO):** Ensures continuous packet forwarding in a Layer 3 routing environment during supervisor engine switchover.
 - Nonstop traffic forwarding, transparent to users, such as voice over IP (VoIP) and mission-critical applications
- **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

Nonstop Forwarding with Stateful Switchover

Nonstop forwarding with stateful switchover (NSF/SSO) offers continuous packet forwarding in a Layer 3 routing environment during supervisor engine switchover. It further extends reliability and availability offered by the Cisco Catalyst 4500's SSO and NSF-aware to the Layer 3 networks. During supervisor engine switchover, NSF/SSO continues forwarding data packets along known routes while the routing protocol information is recovered and validated gracefully, avoiding unnecessary route flaps and network instability. With NSF/SSO, IP phone calls do not drop. NSF/SSO is supported for Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate Systems (IS-IS) Protocol, and Cisco Express Forwarding. NSF/SSO is typically deployed in the most critical parts of an enterprise or service provider network, such as Layer 3 aggregation/core or a resilient Layer 3 wiring closet design. It is an essential component of single chassis deployment for mission-critical applications.

SSO-Aware Hot Standby Router Protocol

SSO-aware Hot Standby Router Protocol (HSRP) offers continuous packet forwarding during a supervisor engine switchover without a path change to the standby HSRP router. During supervisor engine switchover, NSF/SSO continues forwarding data packets along known routes using the HSRP virtual IP address. When both supervisor engines fail on the active HSRP router, the standby HSRP router takes over as the active HSRP router. It further extends reliability and availability offered by the Cisco Catalyst 4500's NSF/SSO to the Layer 3 aggregation with redundant chassis.

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 all shipping Cisco Catalyst 4500 supervisor engines. 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), 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.

Web Content Communication Protocol Version 2 Layer 2 Redirection

Web Content Communication Protocol (WCCP) Version 2 Layer 2 redirection enables a Cisco Catalyst 4500 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 an 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.

Combined Mode Power Resiliency

Combined Mode Power Resiliency is an extension of the traditional combined mode power supply behavior; it is only applicable to the 4200W power supply. Each 4200W power supply contains two smaller power supplies (called a subunit). In Combined Mode Power Resiliency the system only relies on power from three out of four power supply sub - units. When using 200V AC, this feature ensures that 5500W of power is available while the switch is protected against a single input power failure or sub - unit component failure. When using four 110V AC, Combined Mode Power Resiliency provides up to 2,728 Watts.

VRRP

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 the 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 4500 SERIES

A new Cisco IOS Software package for Cisco Catalyst 4500 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 4500 Series, formally known as “Basic Layer 3” and “Enhanced Layer 3” images, now map to “IP Base” and “Enterprise Services,” respectively. BGP is now included in the “Enterprise Services” image. Unless otherwise specified, all currently shipping Cisco Catalyst 4500 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 NSF/SSO, BGP, EIGRP, OSPF, IS-IS, Internetwork Packet Exchange [IPX] protocol, AppleTalk, VRF-lite, and PBR).

The IP Base image supports EIGRP-Stub for limited routing on Cisco Catalyst 4500 Series supervisor engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE. For more information on 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 4500 Series software features based on Cisco IOS Software, including enhanced routing. Customers planning to enable BGP for supervisor engines IV, V, or V-10GE will no longer need to purchase a separate BGP license (FR-IRC4); BGP capability is included in the Enterprises Services package. The Enterprise Services image is not available for supervisor engine II-Plus, II-Plus-TS and II-Plus-10GE. 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 4500 Series supervisor engines.

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

Feature	Supervisor Engine II-Plus (II-Plus-TS and II-Plus-10GE): IP Base	Supervisor Engine IV: IP Base	Supervisor Engine IV: ES	Supervisor Engine V: IP Base	Supervisor Engine V: ES	Supervisor Engine V-10GE: IP Base	Supervisor Engine V-10GE: ES
NACv2.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP and Static Route	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetFlow v1, v5, and v8	No	Yes	Yes	Yes	Yes	Yes	Yes
EIGRP	No	No	Yes	No	Yes	No	Yes
EIGRP-Stub	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF/IS-IS	No	No	Yes	No	Yes	No	Yes
BGP	No	No	Yes	No	Yes	No	Yes
NSF-Aware	No	No	Yes	No	Yes	No	Yes
NSF-Aware EIGRP-Stub	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NSF/SSO	No	No	Yes	No	Yes	No	Yes
SSO Aware HSRP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VRF-Lite	No	No	Yes	No	Yes	No	Yes
AppleTalk	No	No	Yes	No	Yes	No	Yes

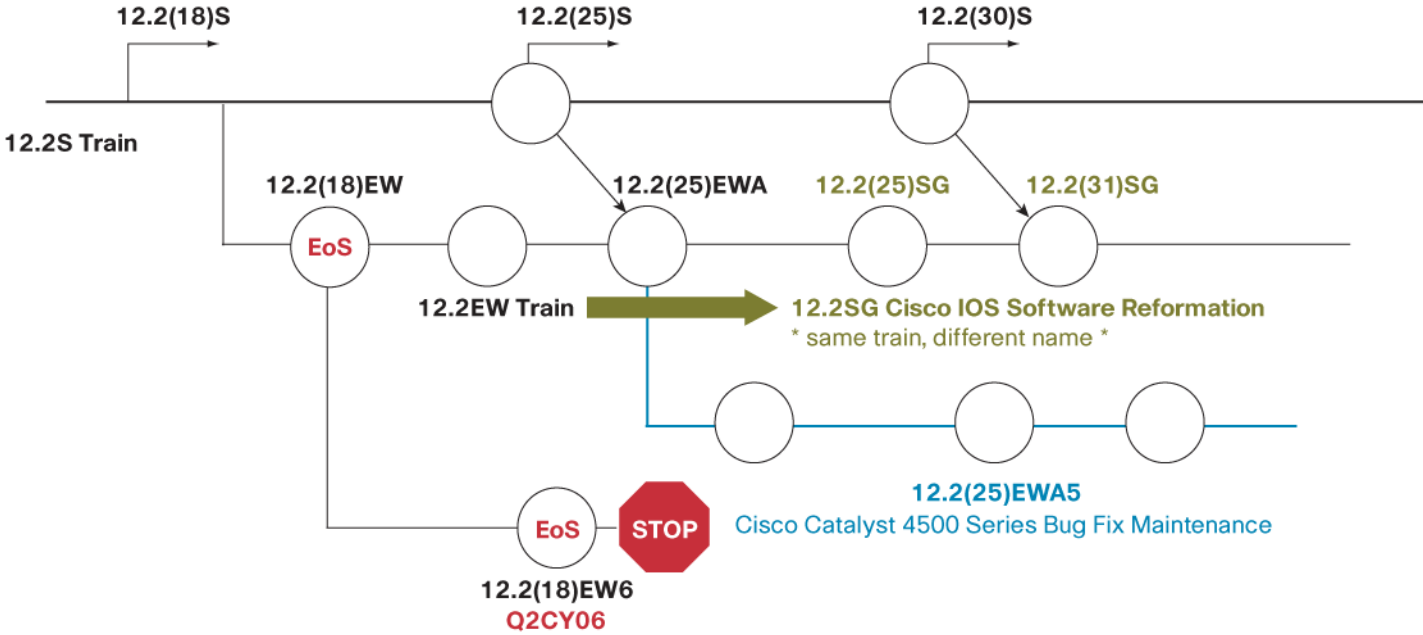
Feature	Supervisor Engine II-Plus (II-Plus-TS and II-Plus-10GE): IP Base	Supervisor Engine IV: IP Base	Supervisor Engine IV: ES	Supervisor Engine V: IP Base	Supervisor Engine V: ES	Supervisor Engine V-10GE: IP Base	Supervisor Engine V-10GE: ES
IPX	No	No	Yes	No	Yes	No	Yes
PBR	No	No	Yes	No	Yes	No	Yes

Please note that the Cisco Catalyst 4500 Series Supervisor Engine III is not supported in Cisco IOS Software Release 12.2(31)SG.

CISCO CATALYST 4500 CISCO 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 4500 Series



* EoS: end of sale.

Summary of migration plan:

- Customers requiring the latest Cisco Catalyst 4500 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(31)SG.
- Cisco IOS Software Release 12.2(18)EW6 will be the last 12.2(18)EW maintenance release.
- 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 support policy, available at http://www.cisco.com/en/US/products/products_end-of-life_policy.html.

For more information about the Cisco Catalyst 4500 Series, visit <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm>.

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
S45IPB-12231SG	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image)	cat4500-ipbase-mz
S45IPBK9-12231SG	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard [3DES])	cat4500-ipbasek9-mz
S45ES-12231SG	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support)	cat4500-entservices-mz
S45ESK9-12231SG	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (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-X4013+	Cisco Catalyst 4500 Series Supervisor Engine II-Plus
WS-X4013+/2	Cisco Catalyst 4500 Series Redundant Supervisor Engine II-Plus
WS-X4013+TS	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-TS
WS-X4013+10GE	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE
WS-X4013+10GE/2	Cisco Catalyst 4500 Series Redundant Supervisor Engine II-Plus-10GE
WS-X4515	Cisco Catalyst 4500 Series Supervisor Engine IV
WS-X4515/2	Cisco Catalyst 4500 Series Redundant Supervisor Engine IV
WS-X4516	Cisco Catalyst 4500 Series Supervisor Engine V
WS-X4516/2	Cisco Catalyst 4500 Series Redundant Supervisor Engine V
WS-X4516-10GE	Cisco Catalyst 4500 Series Supervisor Engine V-10GE
WS-X4516-10GE/2	Cisco Catalyst 4500 Series Redundant Supervisor Engine V-10GE
WS-C4503	Cisco Catalyst 4503 Switch chassis
WS-C4506	Cisco Catalyst 4506 Switch chassis
WS-C4507R	Cisco Catalyst 4507R Switch chassis
WS-C4510R	Cisco Catalyst 4510R Switch chassis
WS-X4124-FX-MT(=)	Cisco Catalyst 4500 Series 24-port Fast Ethernet switching module, 100BASE-FX multimode fiber (MMF), MTRJ
WS-X4124-RJ45(=)	Cisco Catalyst 4500 Series 24-port 10/100 module (RJ-45)
WS-X4148-FX-MT(=)	Cisco Catalyst 4500 Series 48-port Fast Ethernet switching module, 100BASE-FX, MMF, MTRJ
WS-X4148-FE-LX-MT(=)	Cisco Catalyst 4500 Series 48-port Fast Ethernet switching module, 100BASE-LX10 single-mode fiber, MTRJ
WS-X4148-RJ(=)	Cisco Catalyst 4500 Series 48-port 10/100 module (RJ-45)
WS-X4148-RJ21(=)	Cisco Catalyst 4500 Series 48-port 10/100 module, telco (4xRJ-21)
WS-X4148-RJ45V(=)	Cisco Catalyst 4500 Series 48-port inline power 10/100 module (RJ-45)
WS-X4148-FE-BD-LC(=)	Cisco Catalyst 4500 Series 48-port 100BASE-BX10-D line card

Product Number	Description
WS-X4224-RJ45V(=)	Cisco Catalyst 4500 Series 24-port Power over Ethernet (PoE) 10/100 module (RJ-45)
WS-X4232-GB-RJ(=)	Cisco Catalyst 4500 Series 32-port 10/100 (RJ-45), 2-port Gigabit Ethernet module (GBIC)
WS-X4232-RJ-XX(=)	Cisco Catalyst 4500 Series 32-port 10/100 (RJ-45) with modular uplink slot
WS-X4248-FE-SFP(=)	Cisco Catalyst 4500 Series 48-port 100BASE-X (SFP optics optional)
WS-X4248-RJ45V(=)	Cisco Catalyst 4500 Series 48-port PoE 10/100 (RJ-45)
WS-X4248-RJ21V(=)	Cisco Catalyst 4500 Series 48-port PoE 10/100, telco (4xRJ-21)
WS-X4424-GB-RJ45(=)	Cisco Catalyst 4500 Series 24-port 10/100/1000 module (RJ-45)
WS-X4306-GB (=)	Cisco Catalyst 4500 Series 6-port Gigabit Ethernet module (GBIC)
WS-X4302-GB (=)	Cisco Catalyst 4500 Series 2-port Gigabit Ethernet line card (GBIC)
WS-X4412-2GB-T (=)	Cisco Catalyst 4500 Series 12-port Gigabit Ethernet module, 1000BASE-T (RJ-45) with two 1000BASE-X GBICs
WS-X4418-GB (=)	Cisco Catalyst 4500 Series 18-port Gigabit Ethernet module, server switching (GBIC)
WS-X4448-GB-RJ45 (=)	Cisco Catalyst 4500 Series 48-port 10/100/1000 module (RJ45)
WS-X4448-GB-SFP (=)	Cisco Catalyst 4500 Series 48-port 1000BASE-X (SFP optics optional)
WS-X4506-GB-T (=)	Cisco Catalyst 4500 Series 6-port alternatively wired 10/100/1000 PoE or 1000BASE-X, SFP optics
WS-X4524-GB-RJ45V (=)	Cisco Catalyst 4500 Series 24-port PoE 10/100/1000 line card (RJ-45)
WS-X4548-GB-RJ45 (=)	Cisco Catalyst 4500 Series 48-port 10/100/1000 line card (RJ45)
WS-X4548-GB-RJ45V (=)	Cisco Catalyst 4500 Series 48-port PoE 10/100/1000 line card (RJ45)
WS-U4504-FX-MT (=)	Cisco Catalyst 4500 Series 4-port uplink daughter card 100BASE-FX (MTRJ)
WS-G5483=	1000BASE-T GBIC
WS-G5484 (=)	1000BASE-SX short-wavelength GBIC (multimode only)
WS-G5486 (=)	1000BASE-LX/LH long-haul GBIC (single-mode or multimode)
WS-G5487 (=)	1000BASE-ZX extended-reach GBIC (single-mode)
MEM-C4K-FLD64M (=)	Cisco Catalyst 4500 Series Compact Flash, 64-MB option
MEM-C4K-FLD128M (=)	Cisco Catalyst 4500 Series Compact Flash, 128-MB option
PWR-C45-4200ACV	Cisco Catalyst 4500 4200W AC dual input power supply (data + PoE)
PWR-C45-2800ACV	2800W AC power supply for Cisco Catalyst 4503, 4506, and 4507R chassis
PWR-C45-1400DC	Cisco Catalyst 4500 Series 1400W DC power supply
PWR-C45-1400DC-P	Cisco Catalyst 4500 Series 1400W DC power supply with integrated PEM
PWR-C45-1400AC	Cisco Catalyst 4500 Series 1400W AC power supply (data only)
PWR-C45-1300ACV	1300W AC power supply for Cisco Catalyst 4503, 4506, and 4507R chassis
PWR-C45-1000AC	1000W AC power supply for Cisco Catalyst 4503, 4506, and 4507R chassis (data only)
CWDM-GBIC-xxxx	Cisco 1000BASE coarse wavelength-division multiplexing (CWDM) xxxx nm GBIC, where xxxx is the number 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610
DWDM-GBIC-xx.yy	Cisco 1000BASE dense wavelength-division multiplexing (DWDM) ITU 100-GHz grid 15xx.yy nm GBIC
WDM-GBIC-REC=	Cisco receive-only 1000BASE-WDM GBIC
WS-F4531(=)	NetFlow Services Card for Cisco Catalyst 4500 Series Supervisor Engines IV and V

**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

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

