

# Cisco IOS Software Release 12.1(19)EW for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, III, and IV

This product bulletin lists the hardware and software features that are supported in Cisco® IOS® Software Release 12.1(19)EW for the Cisco Catalyst® 4500 Series Supervisor Engines II-Plus, III, and IV. Cisco IOS Software Release 12.1(19)EW is derived from the Cisco IOS Software 12.1E train. Release 12.1(19)EW is not supported on the Cisco Catalyst 4000 Series Supervisor Engine I or II, or any other Cisco switching or routing platforms.

Cisco IOS Software Release 12.1(19)EW New Hardware Support

## New Hardware Features

### Cisco Catalyst 4500 Series Supervisor Engine II-Plus (WS-X4013+)

The Cisco Catalyst 4500 Series Supervisor Engine II-Plus is a Cisco IOS based supervisor engine that meets the needs of value-conscious customers seeking a flexible and scalable LAN solution. Optimized for wiring closets for medium-sized enterprises, education customers, or small enterprise/branch offices, the Cisco Catalyst 4500 Series Supervisor Engine II-Plus provides resiliency and control for converged data, voice and video networks.

The Cisco Catalyst 4500 Series Supervisor Engine II-Plus delivers non-blocking Layer 2 switching with Layer 3/4 intelligent services to power resilient, multilayer switching solutions for converged data, voice, and video networks. The Cisco Catalyst 4500 Series Supervisor Engine II-Plus allows customers to deploy network-wide intelligent services, such as advanced quality of service (QoS),

comprehensive security, and management with optimal control and resiliency. Compatible with the widely deployed Cisco Catalyst 4503, 4506, 4507R, and 4006 chassis, and with existing Cisco Catalyst 4500 Series line cards, the Supervisor Engine II-Plus helps to ensure an extended window of deployment of the modular Cisco Catalyst 4500 Series.

### Cisco Catalyst 4500 Series 48-Port 10/100/1000 RJ-45 Line Card (WS-X4548-GB-RJ45=)

The Cisco Catalyst 4500 Series 48-Port 10/100/1000 RJ-45 module has efficient power draw.

### Catalyst 4500 Series 2-Port Gigabit Ethernet Line Card (WS-X4302-GB=)

The Cisco Catalyst 4500 Series 2-Port Gigabit Ethernet module is a two-port, wire-speed GBIC line card. It offers additional uplinks for any Cisco Catalyst 4000 or 4500 series chassis.



### Cisco DWDM GBICs (DWDM-GBIC-xx.yy)

Cisco Dense Wavelength Division Multiplexing (DWDM) GBICs support an ITU 100 GHz grid with 32 different fixed wavelengths. They can be used and interchanged on numerous Cisco products and can be intermixed in combinations of 1000BASE-SX, 1000BASE-LX/LH, or 1000BASE-ZX on a port-by-port basis.

### Cisco Receive-Only 1000BASE-WDM GBIC (WDM-GBIC-REC)

The Cisco receive-only 1000BASE-WDM GBIC does not have a laser. It interoperates with any Cisco coarse WDM (CWDM) or Cisco DWDM GBIC at the other end of the link.

Cisco IOS Software Release 12.1(19)EW Software Support

### **New Software Features**

- Dynamic Address Resolution Protocol (ARP) Inspection
- IP source guard
- 802.1x with virtual LAN (VLAN) assignment
- 802.1x with guest VLAN
- Port ACL (PACL)
- Port flood blocking
- Per-VLAN Rapid Spanning-Tree Plus (PVRST+)
- Storm control (broadcast suppression)
- Internet Group Management Protocol Version 3 (IGMPv3 snooping)
- Auto-QoS
- Trusted boundary
- Inline power pre-allocation
- Switched Port Analyzer (SPAN) destination inpkts option
- SPAN CPU source
- SPAN packet type filtering
- NetFlow Version 8
- Show interface capabilities
- IfIndex persistence
- Unidirectional link routing (UDLR)
- Enhanced SNMP Management Information Base (MIB) support

### Dynamic ARP Inspection

ARP does not have any authentication. It is quite simple for a malicious user to poison ARP tables of other hosts on the same VLAN. In a typical attack, a malicious user can send unsolicited ARP replies (gratuitous ARP packets) to other hosts on the subnet with the attacker's MAC address and the default gateway's IP address. Such ARP poisoning leads to various "man-in-the-middle" attacks, posing a security threat in the network. Dynamic ARP Inspection intercepts all ARP requests and replies on the untrusted ports. Each intercepted packet is verified for valid IP-to-MAC bindings. The Dynamic Host Control Protocol (DHCP) snooping feature is typically used to maintain IP-to-MAC



bindings. Dynamic ARP Inspection helps prevent the man-in-the-middle attacks by not relaying invalid ARP replies out to other ports in the same VLAN. It is a solution with no change to the end user or host configurations. Denied ARP packets are logged by the switch for auditing. Incoming ARP packets on the trusted ports or isolated private VLAN (PVLAN) trunks are not inspected.

### IP Source Guard

IP source guard provides per-port IP traffic filtering of the assigned source IP addresses at wire speed. It is a unique Cisco Catalyst 4500 Series IOS Software feature that helps mitigate IP spoofing. It dynamically maintains per-port VLAN ACLs (VACLs) based on IP to MAC to switch port bindings. The binding table is populated either by the DHCP snooping feature or through static configuration of entries. IP source guard prevents a malicious host from attacking the network by hijacking its neighbor's IP address. IP source guard is typically deployed for untrusted switch ports in the access layer.

### 802.1x with VLAN Assignment

The 802.1x with VLAN assignment feature authorizes a user for an associated VLAN. This is achieved by maintaining a username-to-VLAN mapping database on the Remote Authentication Dial-In User Service (RADIUS) server. Following successful 802.1x authentication, the RADIUS server sends the VLAN name to the switch for that particular user, and the switch configures the authenticated port for the specified VLAN.

### 802.1x with Guest VLAN

When 802.1x is enabled on an access port, a user without an 802.1x client is typically denied access to the network. The 802.1x with guest VLAN feature offers limited network access through a guest VLAN to those users. It is usually deployed in a lobby or in customer briefing areas.

### PACL

PACL is a security ACL feature applied to Layer 2 switch ports. PACL filters traffic to and from Layer 2 switch ports with permit and deny actions, based on Layer 3 and 4 header information or non-IP Layer 2 information. By default, PACL actions override VLAN-based ACLs. Both input and output PACLs are supported. PACLs can be configured on physical ports and channel ports. PACLs are typically used to limit IP address use per customer on access ports, by restricting a port to one IP address. PACLs can be deployed along with PVLANS to separate users from each other on the same subnet.

### Port Flood Blocking

By default, a switch floods packets with unknown destination MAC addresses to all Ethernet ports. In certain configurations, such flooding is neither needed nor desired. For example, a port with only manually assigned address or only one connected host has no unknown destination. Flooding serves no purpose for such a port. Port flood blocking allows a user to disable the flooding of unicast and multicast packets on a per-port basis.



## PVRST+

Rapid Spanning-Tree Protocol (RSTP) as specified in IEEE 802.1w provides rapid recovery of connectivity following the failure of a bridge, bridge port, or LAN. Cisco Per-VLAN Spanning Tree Plus (PVST+) applies RSTP convergence with 802.1d on a per-VLAN basis. Per-VLAN Rapid Spanning-Tree (PVRST+) is the implementation of 802.1w on a per-VLAN basis. It is the same as PVST+ with respect to Spanning-Tree Protocol mode and runs RSTP based on 802.1w.

## Storm Control (Broadcast Suppression)

Broadcast suppression is used to prevent LANs from being disrupted by a broadcast storm. A broadcast storm occurs when broadcast packets flood the LAN, creating excessive traffic and degrading network performance. Broadcast suppression measures how much broadcast traffic traverses a port, and compares the broadcast traffic bandwidth with some configurable threshold value within a specific time interval. If the amount of broadcast traffic reaches the threshold during this interval, broadcast frames are dropped, and optionally the port is shut down. Simple Network Management Protocol (SNMP) traps can be generated by the switch when broadcast suppression is activated. Broadcast suppression can be enabled or disabled on a per-port basis. For nonblocking Gigabit Ethernet ports, broadcast suppression is achieved in hardware. In all other cases, broadcast suppression is implemented in software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus, III, and IV.

## IGMPv3 Snooping

The IGMPv3 snooping feature provides constrained flooding of multicast traffic in the presence of IGMPv3 hosts or routers. IGMPv3 snooping listens to IGMPv3 query and membership report messages to maintain host-to-multicast group associations. IGMPv3 snooping enables a switch to propagate multicast data only to ports that need them. The IGMPv3 snooping feature is fully interoperable with IGMPv1 and v2.

## Auto-QoS

Auto-QoS is a set of new Cisco IOS Software macros that simplify the voice over IP (VoIP) deployment of Cisco QoS features. It enables a user to consistently deploy appropriate QoS in the network for IP telephony. The same macros are used across Cisco IOS platforms for effective QoS configurations in the network.

## Trusted Boundary

In a typical network supporting IP telephony, traffic sent from Cisco IP phones to a switch is usually marked with a tag in 802.1Q header. The header contains the VLAN information and a three-bit class of service (CoS) field, which determines the priority of the packet. In most IP telephony configurations, the traffic sent from a Cisco IP phone to the switch is trusted to help ensure that voice traffic is properly prioritized over other types of traffic in the network. If a user bypasses the Cisco IP phone and connects the PC directly to the switch, the trusted CoS labels generated by the PC can cause misuse of high-priority queues. The trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue, if a Cisco IP phone is not detected.



### Inline Power Pre-Allocation

An inline power port can be configured with option “static” to gain a higher priority than the “auto” option. A configurable amount of inline power is pre-allocated for the static port regardless of whether a device is connected to it. Such static ports no longer need to participate in the current first-come-first-served model, even when inline power is oversubscribed in the system. In the event of insufficient inline power due to partial power supply failure, auto ports are shut down before static ports.

### SPAN Destination Inpkts Option

SPAN allows a user to configure a set of source ports or VLANs as SPAN sources. Packets either received at or transmitted from SPAN sources are copied to a destination port. A SPAN destination port is used to transmit the sniffed traffic of the SPAN source ports. All ingress traffic to the SPAN destination port is usually dropped. The SPAN destination inpkts option allows the SPAN destination port to receive and switch normal incoming traffic. This feature is typically used by an intrusion detection system (IDS) to send a reset or notification signal into the network through the SPAN destination port.

### SPAN CPU Source

SPAN CPU source allows a user to specify the CPU (or a subset of CPU queues) as a SPAN source. Traffic going to or from the CPU via one of the specified queues is mirrored and sent to the SPAN destination port. This traffic includes both control packets and regular data packets that are sent to or from the CPU (due to software forwarding, for example). This feature is typically used for troubleshooting.

### SPAN Packet Type Filtering

SPAN packet type filtering allows a user to apply packet filters to SPAN sources for ingress and egress traffic. Ingress traffic may be filtered by unicast, multicast, broadcast, good, or error packets. Egress traffic may be filtered by unicast, multicast, or broadcast. This feature is typically used to simplify network traffic monitoring.

### NetFlow Version 8

NetFlow statistics collection and export are supported by the NetFlow Services Card on the Cisco Catalyst 4500 Series Supervisor Engine IV. NetFlow statistics enable flow-level monitoring of all IPv4 routed traffic through the switch. NetFlow Version 8 adds router-based aggregation schemes. By maintaining aggregation caches, NetFlow Version 8 enables aggregation of NetFlow data export streams. Additional NetFlow Version 5 fields are also supported in this release, such as input and output interface, Autonomous System (AS) info, and next-hop router.

### Show Interface Capabilities

The show interface capabilities command allows a user to quickly determine available options that can be configured on an interface or a module. It does not provide the current operating configurations of an interface. It is only supported on all physical Layer 2 and Layer 3 interfaces.

### IfIndex Persistence

The ifIndex persistence feature allows the ifIndex value for any interface to remain the same after a system reboot. The SNMP ifIndex value is a unique identifier for a physical or logical interface on a switch. This feature simplifies many SNMP-based network management applications.



## UDLR

UDLR enables a router to emulate the behavior of a bidirectional link for IP operations over two unidirectional links. The feature is normally used for asymmetric links (such as in video transport networks) where the downstream link requires a much higher bandwidth than the upstream link.

## Enhanced SNMP MIB Support

Additional SNMP MIBs are supported in this release. They are:

- CISCO-IF-EXTENSION-MIB
- ETHERLIKE-MIB

## Support

Cisco IOS Software Release 12.1(19)EW follows the standard Cisco support policy, which is available at:

[www.cisco.com/warp/public/437/27.html](http://www.cisco.com/warp/public/437/27.html)

For more information on the Cisco Catalyst 4500 Series, visit:

[www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm)

## Product Numbers

Table 1 Cisco IOS Software Release 12.1(19)EW Feature Sets, Images, and Software Licenses

Product Number	Description	Image
S4KL3-12119EW	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus, III, and IV Basic Layer 3 and voice software image, including Routing Information Protocol (RIP) v1 and v2, static routes, AppleTalk, and Internetwork Packet Exchange (IPX) software routing	cat4000-i9s-mz.121-19.EW
S4KL3E-12119EW	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine III and IV Enhanced Layer 3 and voice software image, including Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), and Enhanced IGRP (EIGRP)	cat4000-i5s-mz.121-19.EW



Table 1 Cisco IOS Software Release 12.1(19)EW Feature Sets, Images, and Software Licenses

Product Number	Description	Image
S4KL3K2-12119EW	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus, III, and IV with Triple Data Encryption Standard (3DES) strong encryption Basic Layer 3 and voice software image, including Secure Shell (SSH) Protocol Version 1 and Version 2, RIPv1, RIPv2, static routes, AppleTalk, and IPX software routing	cat4000-i9k2s-mz.121-19.EW
S4KL3EK2-12119EW	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine III and IV with 3DES strong encryption Enhanced Layer 3 and voice software image, including OSPF, IS-IS, IGRP, and EIGRP	cat4000-i5k2s-mz.121-19.EW
FR-IRC4	Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine III and IV Interdomain routing feature license including Border Gateway Protocol Version 4 (BGP4)	N/A

Table 2 Cisco IOS Software Release 12.1(19)EW Hardware Support

Product Number	Description
WS-X4014	Cisco Catalyst 4500 Series Supervisor Engine III
WS-X4515	Cisco Catalyst 4500 Series Supervisor Engine IV
WS-X4515/2	Cisco Catalyst 4507R Series Redundant Supervisor Engine IV
WS-X4013+	Cisco Catalyst 4500 Series Supervisor Engine II-Plus
WS-C4503	Cisco Catalyst 4503 chassis
WS-C4506	Cisco Catalyst 4506 chassis
WS-C4507R	Cisco Catalyst 4507R chassis
WS-C4006-S3	Cisco Catalyst 4006 chassis, with Supervisor Engine III and 2 AC power supplies
WS-C4006-S3-DC	Cisco Catalyst 4006 chassis, with Supervisor Engine III and 2 DC power supplies
WS-C4006-S4	Cisco Catalyst 4006 chassis, with Supervisor Engine IV and 2 AC power supplies
WS-C4006-S4-DC	Cisco Catalyst 4006 chassis, with Supervisor Engine IV and 2 DC power supplies
WS-C4006-S2+	Cisco Catalyst 4006 chassis, with Supervisor Engine II-Plus and 2 AC power supplies
WS-C4006-S2+-DC	Cisco Catalyst 4006 chassis, with Supervisor Engine II-Plus and 2 DC power supplies
WS-X4124-FX-MT (=)	Cisco Catalyst 4000 Series Fast Ethernet switching module, 24-100FX multimode fiber (MMF) (MT-RJ)
WS-X4148-FX-MT (=)	Cisco Catalyst 4000 Series Fast Ethernet switching module, 48-100FX MMF (MT-RJ)



Table 2 Cisco IOS Software Release 12.1(19)EW Hardware Support

Product Number	Description
WS-X4148-FE-LX-MT(=)	Cisco Catalyst 4000 Series Fast Ethernet switching module, 48-port 100BASE-LX10 single-mode fiber (SMF) (MT-RJ)
WS-X4148-RJ (=)	Cisco Catalyst 4000 Series 10/100 module, 48 ports (RJ-45)
WS-X4148-RJ21 (=)	Cisco Catalyst 4000 Series 10/100 module, 48 ports telco (4xRJ-21)
WS-X4148-RJ45V (=)	Cisco Catalyst 4000 Series inline power 10/100, 48-ports (RJ-45)
WS-X4232-GB-RJ (=)	Cisco Catalyst 4000 Series 32-10/100 (RJ-45), 2-Gigabit Ethernet (GBIC) module
WS-X4232-RJ-XX (=)	Cisco Catalyst 4000 Series 32-10/100 (RJ-45) with modular uplink slot
WS-X4424-GB-RJ45 (=)	Cisco Catalyst 4000 Series 24-port 10/100/1000 module (RJ-45)
WS-X4306-GB (=)	Cisco Catalyst 4000 Series Gigabit Ethernet Module, 6 ports (GBIC)
WS-X4412-2GB-T (=)	Cisco Catalyst 4000 Series Gigabit Ethernet module, 12-1000T(RJ-45) with 2 1000X GBICs
WS-X4418-GB (=)	Cisco Catalyst 4000 Series Gigabit Ethernet module, server switching 18-port (GBIC)
WS-X4448-GB-LX (=)	Cisco Catalyst 4000 Series 48-port 1000BASE-LX (small form-factor pluggable [SFP])
WS-X4448-GB-RJ45 (=)	Cisco Catalyst 4000 Series 48-port 10/100/1000 module (RJ-45)
WS-U4504-FX-MT (=)	Cisco Catalyst 4000 Series uplink daughter card, 4-port 100FX (MT-RJ)
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 4000 Series Compact Flash, 64-MB option
MEM-C4K-FLD128M (=)	Cisco Catalyst 4000 Series Compact Flash, 128-MB option
WS-X4095-PEM (=)	Cisco Catalyst 4000 Series DC power entry module (PEM)
PWR-C45-2800ACV	2800W AC power supply for Cisco Catalyst 4503, 4506, and 4507R chassis
PWR-C45-1400DC-P	Cisco Catalyst 4500 Series 1400W DC power supply with integrated PEM
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
CWDM-GBIC-xxxx	Cisco 1000BASE-CWDM xxxx nm GBIC, where xxxx is the number 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610
WS-F4531 (=)	NetFlow Services Card on Cisco Catalyst 4500 Series Supervisor Engine IV
<b>New Hardware supported by</b>	<b>Cisco IOS Software Release 12.1(19)EW</b>
WS-X4013+ (=)	Cisco Catalyst 4500 Series Supervisor Engine II-Plus

Table 2 Cisco IOS Software Release 12.1(19)EW Hardware Support Table 2 Cisco IOS Software Release 12.1(19)EW Hardware Support

Product Number	Description	Product Number	Description
WS-X4548-GB-RJ45 (=)	Cisco Catalyst 4500 Series 48-port 10/100/1000-Mbps GBIC	DWDM-GBIC-REC=	Cisco receive-only 1000BASE-WDM GBIC
WS-X4302-GB (=)	Cisco Catalyst 4500 Series 2-port Gigabit Ethernet line card (GBIC)		
DWDM-GBIC-xx.yy	Cisco 1000BASE-DWDM ITU 100-GHz grid 15xx.yy nm GBIC		

For additional information about this release, send e-mail to: ask\_c4000\_pm@cisco.com



Corporate Headquarters  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://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](http://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](http://www.cisco.com)  
 Tel: 408 526-7660  
 Fax: 408 527-0883

Asia Pacific Headquarters  
 Cisco Systems, Inc.  
 Capital Tower  
 168 Robinson Road  
 #22-01 to #29-01  
 Singapore 068912  
[www.cisco.com](http://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 Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R) EL/LW4715 06/03