



# Cisco IOS Software Release 12.2(14)SX for Supervisor Engine 720 of the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router

Use this publication if you plan to implement the Cisco Supervisor Engine 720 for the Cisco Catalyst® 6500 Series Switch or the Cisco 7600 Series Internet Router.

Cisco IOS® Software Release 12.2(14)SX is supported only on the Supervisor Engine 720.

## Hardware Features

The Cisco IOS Software Release 12.2(14)SX supports all modules that the Cisco IOS Software Release 12.1(13)E2 supported, with the following exceptions. No support is provided for:

- Optical Services Modules (OSM)
- Service Modules
- Cisco Catalyst 6500 Series Supervisor Engine 1A or Supervisor Engine 2
- Switch fabric module (SFM) or SFM2 (the Supervisor Engine 720 has an integrated 720-Gbps switch fabric)

Table 1 lists the new hardware modules supported in Cisco IOS Software Release 12.2(14)SX.

Table 1 Cisco IOS Software Release 12.2(14)SX New Hardware

Hardware	Description
<b>WS-SUP720 (Supervisor Engine 720)</b>	This is the new Cisco Supervisor Engine 720 and third-generation policy feature card (PFC3a) with integrated Multilayer Switch Feature Card 3 (MSFC3). The Supervisor Engine 720 helps enable enterprise and service provider customers to enhance their network infrastructures with advanced IP services delivered in hardware such as IPv6 and Multiprotocol Label Switching (MPLS), while fully integrating the switch fabric to deliver increased density and performance. This scalable architecture provides increased bandwidth, network control, and secure converged services from the wiring closet through the core to the data center and WAN edge, delivering an 8- to 10-year product life cycle.
<b>WS-X6516A-GBIC</b>	This cost-reduced, 16-port Gigabit Ethernet module offers crossbar switching fabric connectivity.
<b>WS-F6K-DFC3</b>	This is the dial feature card 3a (DFC3a) for Cisco Express Forwarding and distributed Cisco Express Forwarding 256 modules. This daughter module is field replaceable and is required for distributed forwarding functions when used in conjunction with a Cisco Supervisor Engine 720.
<b>PA-A6-T3</b>	1-Port ATM T3 Port Adapter, Enhanced
<b>PA-A6-E3</b>	1-Port ATM E3 Port Adapter, Enhanced
<b>PA-A6-OC3MM</b>	1-Port ATM OC-3 Multi Mode Port Adapter, Enhanced
<b>PA-A6-OC3SMI</b>	1-Port ATM OC-3 Single Mode Intermediate Reach Port Adapter, Enhanced
<b>PA-A6-OC3SML</b>	1-Port ATM OC-3 Single Mode Long Reach Port Adapter, Enhanced



## Software Features

Software features in this release are specific to the Cisco Supervisor Engine 720.

The Cisco IOS Software Release 12.2(14)SX supports all software features previously supported by the Cisco IOS Software Release 12.1(13)E2 for the Cisco Catalyst 6500 and Cisco 7600 supervisor engines, with the following exceptions. These features will be supported on the Cisco Supervisor Engine 720 in future releases.

- Web Cache Control Protocol (WCCP)
- VLAN ACL (VACL) capture
- Cisco IOS server load balancing (SLB)
- Network-based application recognition (NBAR)

The Cisco Supervisor Engine 720 supports the following features (described later in the document) in Cisco IOS Software Release 12.2(14)SX:

- Virtual Router Redundancy Protocol (VRRP)
- Bidirectional Protocol Independent Multicast (PIM) in hardware
- Interior Border Gateway Protocol (IBGP) multipath
- IP-in-IP and generic routing encapsulation (GRE) tunneling—hardware based
- User-based rate limiting
- Internet Group Management Protocol Version 3 (IGMPv3) snooping
- Multiple-path Unicast Reverse Path Forwarding (uRPF) enhancements in hardware
- Hardware-assisted Network Address Translation (NAT)
- Egress rate limiting

The FlexWAN Module supports the following new features (described later in this document) in Cisco IOS Software Release 12.2(14)SX.

- Compressed Real-time Protocol (cRTP)
- Distributed Link Fragmentation and Interleaving (dLFI)
- FRF.12
- FRF.11 Voice over Frame Relay
- MLPPP with Quality of Service (QoS)
- 8000 Virtual Circuits on FlexWAN with ATM Port Adapters.

## VRRP

VRRP provides functions equivalent to the Cisco Hot Standby Router Protocol (HSRP), but is supported by multiple vendors. It is designed to eliminate a single point of failure that is unavoidable in static default routing environments. The advantage of both HSRP and VRRP is a highly available default gateway redundancy for end stations.

Statically configuring default routers on clients creates a single point of failure. VRRP is designed to solve the static configuration resiliency problem by enabling a group of routers to form a single virtual router. The clients can then be configured with the virtual-router IP address as their default gateway.



Each router that participates in a group to form a virtual router is referred to as a VRRP router. Thus a virtual router comprises one or more VRRP routers. The VRRP router currently controlling the virtual-router IP address is referred to as the master and is responsible for forwarding packets sent to this virtual IP address. The other VRRP routers in the group act as backup. If the master fails, an election process takes place and one of the backup routers becomes the new master.

The VRRP implementation also supports multiple VRRP groups on the same interface, acting as master for one group and backup for one or more other groups. This capability allows the routers to load share as well as provide redundancy. With Cisco IOS Software Release 12.2(14)SX, the Cisco Supervisor Engine 720 supports up to 255 VRRP (or HSRP) group IDs.

#### Bidirectional PIM in Hardware

PIM is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. With Cisco IOS Software Release 12.2(14)SX, PIM now supports bidirectional mode, in addition to dense mode, sparse mode, and source-specific multicast mode.

Bidirectional PIM creates a two-way forwarding tree, which allows the efficient transmission of low-bandwidth many-to-many communication; for example, for use in a financial trading application or IP telephony application. Multicast groups in bidirectional mode can scale to an arbitrary number of multicast sources without incurring the otherwise expected overhead due to that number of sources.

The routing state of bidirectional shared trees is bidirectional, meaning that packets can flow up the tree toward the route processor and down the tree away from the route processor, depending on the location of the source. Also, in bidirectional PIM, packets are shared by all sources to the group. This scenario is in contrast to "unidirectional shared trees" built by PIM sparse mode (PIM-SM). Bidirectional PIM is much more scalable than PIM-SM implementations because it uses a single (\*,G) forwarding entry for all hosts sending to the same group G, as opposed to PIM-SM, which would create a new (S,G) entry for each source S. This contributes to decreased memory and CPU utilization on the Cisco Supervisor Engine 720.

To use bidirectional PIM in Cisco IOS Software Release 12.2(14)SX, all routers must be capable of supporting the feature. Also, bidirectional PIM does not support IGMPv3 snooping because it cannot recognize the source entry in the (S,G) states.

#### IBGP Multipath

Prior to Cisco IOS Software Release 12.2(14)SX, when a BGP speaking router A with no local policy configured received multiple network layer reachability information from an internal BGP for the same destination, router A chose one internal BGP path as the best path. The best path was then installed in the IP routing table of router A. For example, imagine that three paths are available to reach an autonomous system X. Router A determined that one of the paths to autonomous system X was the best path and used this path only to reach autonomous system X. The internal BGP multipath load-sharing feature enables the BGP speaking router A to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of router A. So, if three paths exist to reach autonomous system X from router A, and they are configured as multipaths, all three paths can equally load share and can be used to reach autonomous system X.



## IP-in-IP and GRE Tunneling—Hardware Based for Increased Performance

Tunneling provides a means for transporting an arbitrary data packet across a network through the addition of a tunnel header that the transport network supports.

The GRE implementation in the Cisco Supervisor Engine 720 in Cisco IOS Software Release 12.2(14)SX is a tunneling protocol that encapsulates IP protocol packet types inside IP tunnels, creating a virtual point-to-point link to routers at remote points in an IP network. By connecting IP subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

IP-in-IP tunneling can be thought of as a special case of GRE where only IP packets are encapsulated in IP headers, primarily to reduce the overhead associated with the generic nature of GRE.

In Cisco IOS Software Release 12.2(14)SX, the Supervisor Engine 720 with PFC3 offers hardware-based encapsulation and decapsulation of IP-in-IP and GRE tunneling for increased tunneling performance. Only unicast IPv4 packets as the encapsulated payload are supported in this release.

## User-Based Rate Limiting

User-based rate limiting is a function of the microflow-policing feature of the Cisco Catalyst 6500 Series. Microflow policing allows dynamically learned, unique flows to be policed to specified rates. Unique flows are determined by flow masks, which both specify how a flow is identified and create entries in the NetFlow table.

The Cisco Supervisor Engine 720 enhances the microflow-policing capabilities by first allowing multiple flow masks to exist at the same time within the system. Based on the user configuration, the flow mask is dynamically determined from the ingress access-control-list (ACL) and quality-of-service (QoS) lookup results for each flow.

Secondly, the Cisco Supervisor Engine 720 with the PFC3 supports two additional flow masks:

- Source only
- Destination only

By supporting these flow masks, customers can configure user-based rate limiting, based on a user's identity or IP address, the network administrator can rate limit their traffic to the configured rate. The rate limiting can be done from the user (source only) or to the user (destination only).

Use Case:

As an example, consider the case in a university dorm room setting. The network administrator wishes to grant Internet access to 10,000 users in the network. User-based rate limiting rate limits users (based on individual IP address) to a particular speed by dynamically learning all 10,000 source-IP addresses as they flow through the switch.

## IGMPv3 Snooping

IGMPv3 snooping enables the Cisco Catalyst 6500 Series Switch to make multicast forwarding decisions in a Layer 2 bridged network. It constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it. Without snooping functions, the switch would flood multicast traffic out every port regardless of whether a user is requesting it.

IGMPv3, which runs on a multicast router, generates Layer 3 IGMPv3 queries in subnets where the multicast traffic needs to be routed. With IGMPv3, hosts can signal (and the switch constrains) multicast group membership on a per-source basis. IGMPv3 snooping monitors, or sniffs, the IGMPv3 traffic as it traverses the switch. The switch then



records the Media Access Control (MAC) addresses and the port that requested to be a part of a multicast group. Because the switch becomes an integral part of the process of IGMPv3, the router forwards status messages to the switch and the switch forwards them out the appropriate ports.

Different from IGMP snooping, IGMPv3 snooping can monitor IGMPv3 traffic.

#### Multiple-Path uRPF Enhancements in Hardware

uRPF mitigates security threats that are caused by the introduction of forged (spoofed) source IP addresses into a network by discarding IP packets that lack a verifiable source IP address. It does this by forwarding only packets that have source addresses that are valid and consistent with the current IP routing table.

On the Cisco Supervisor Engine 720 coupled with Cisco IOS Software Release 12.2(14)SX, uRPF is enhanced to support multiple-path RPF checks in hardware. This is compared to the Catalyst 6500 Series Supervisor Engine 2, which supports only one path in hardware. The multiple paths include two paths for all prefixes in the Forwarding Information Base (FIB) table, and up to six paths for prefixes reached through any of four configurable uRPF interface groups.

#### Hardware-Assisted NAT

Prior to Cisco IOS Software Release 12.2(14)SX, the NAT function on the Cisco Catalyst 6500 Series Switch was performed in software and bound to the capacity of the route processor. With the Cisco Supervisor 720 and PFC3, coupled with Cisco IOS Software 12.2(14)SX, the NAT function is now hardware assisted for increased performance and scalability.

NAT is beneficial to users for many reasons. First, it helps to solve the shortage of Internet IP address space. As its name implies, NAT translates IP addresses within private "internal" networks to "public" IP addresses for transport over public (external) networks (such as the Internet). Thus, NAT allows an organization with unregistered private addresses to connect to the Internet by translating those addresses into globally registered IP addresses.

NAT also increases network privacy by hiding internal IP addresses from external networks but maintains network flexibility. For example, static NAT maps an unregistered address to a registered address in a one-to-one mapping. This setup not only hides the internal IP address but also is very useful when devices need to be accessible from outside the network, and it maintains security.

With Software Release 12.2(14)SX on the Cisco Catalyst Supervisor Engine 720 with integrated PFC3, NAT is hardware assisted for unicast traffic only; thus performance effects are minimized when NAT functions are executed.

#### Egress Rate Limiting

In addition to ingress rate-limiting functions, the Cisco Supervisor Engine 720 for the Catalyst 6500 Series switches supports egress policing and marking on router ports or Layer 2 virtual LANs (VLANs). This feature offers a different logical point for rate limiting.

Note: Only aggregate and shared aggregate policers are available for egress policing. Egress policing is enforced at ingress forwarding engines (PFC or DFCs) of traffic flows.



### Compressed Real-time Protocol (cRTP)

cRTP, RFC1889, provides bandwidth efficiencies over low-speed links by compressing the UDP/RTP/IP header when transporting voice. With cRTP, the header for voice-over-IP traffic can be reduced from 40 bytes to approximately 2 to 5 bytes offering substantial bandwidth efficiencies for low-speed links. cRTP is supported over Frame Relay, ATM, PPP, MLPPP, and HDLC encapsulated interfaces.

### Distributed Link Fragmentation and Interleaving (dLFI)

dLFI provides support for real-time voice traffic while transporting other non real-time data traffic that is not in real time. Large data packets not transported in real time are fragmented and interleaved between voice packets, thereby minimizing end-to-end latency and jitter for voice traffic. On the receiving end, the fragmented packets are reassembled. dLFI is supported over Frame Relay, ATM, and PPP/MLPPP/HDLC links.

### FRF.12

FRF.12 is standards-based link fragmentation and interleaving over Frame Relay links. FRF.12 supports real-time voice over Frame Relay links by fragmenting large data packets and interleaving fragmented data packets with voice packets, thereby minimizing end-to-end latency and jitter. On the receiving end, the fragmented packets are reassembled.

### FRF.11 Voice over Frame Relay

FRF.11 is a Frame Relay standard that defines encapsulation and transport of voice and data across a Frame Relay link. Voice and data are carried across sub-channels on a Frame Relay link. This feature enables the Cisco 7600 and Catalyst 6500 Series to function as a Frame Relay tandem switch for voice and data.

### MLPPP with Quality of Service (QoS)

MLPPP allows multiple T1/E1 links to be bundled together to offer bandwidth greater than multiple T1s/E1s but less than a T3/E3. MLPPP with QoS supports CBWFQ/LLQ, enabling MLPPP to carry voice and data on the same MLPPP bundle.

### 8000 Virtual Circuits on FlexWAN with ATM Port Adapters

A total of 8000 virtual circuits will be supported per FlexWAN module for all the following ATM port adapters:

- PA-A3-OC3MM
- PA-A3-OC3SMI
- PA-A3-OC3SML
- PA-A3-T3
- PA-A3-E3
- PA-A6-OC3MM
- PA-A6-OC3SMI
- PA-A6-OC3SML
- PA-A6-T3
- PA-A6-E3



## Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the Cisco Supervisor Engine 720 for the Cisco Catalyst 6500 Switch. Cisco IOS Software runs on the DFC to provide distributed Cisco Express Forwarding support. This image is bundled as part of the sup720 image and is not released separately.

*Caution:* Always back up the switch configuration file to a Trivial File Transfer Protocol (TFTP) server or Flash device before upgrading or downgrading the switch software to avoid losing all or part of the configuration stored in NVRAM. When downgrading switch software, the configuration will be lost.

Table 2 Software Versions and Ordering Information

Product Number	Description	Image
<b>S7-33AK9-12214SX</b>	C6500/C7600 S720/MSFC3/PFC3 IOS ENTERPRISE W/VIP SSH 3DES	s72033-jk9sv-mz.122-14.SX
<b>S7-33AK9-12214SX=</b>	Spare; requires appropriate feature license(s)	
<b>S7-33ZV-12214SX h</b>	C6500/C7600 S720/MSFC3/PFC3 IOS SERVICE PROVIDER W/VIP	s72033-psv-mz.122-14.SX
<b>S7-33ZV-12214SX=</b>	Spare; requires appropriate feature license(s)	
<b>S7-33ZK9-12214SX</b>	C6500/C7600 S720/MSFC3/PFC3 IOS SP W/VIP SSH 3DES	s72033-pk9sv-mz.122-14.SX
<b>S7-33ZK9-12214SX=</b>	Spare; requires appropriate feature license(s)	
<b>S7-33ALK9-12214SX</b>	C6500/C7600 S720/MSFC3/PFC3 IOS ENTERPRISE SSH 3DES LAN ONLY	s72033-jk9s-mz.122-14.SX
<b>S7-33ALK9-12214SX=</b>	Spare; requires appropriate feature license(s)	
<b>S7-33ZLV-12214SX</b>	C6500/C7600 S720/MSFC3/PFC3 IOS SERVICE PROVIDER LAN ONLY	s72033-ps-mz.122-14.SX
<b>S7-33ZLV-12214SX=</b>	Spare; requires appropriate feature license(s)	
<b>S7-33ZLK9-12214SX</b>	C6500/C7600 S720/MSFC3/PFC3 IOS SP SSH 3DES LAN ONLY	s72033-pk9s-mz.122-14.SX
<b>S7-33ZLK9-12214SX=</b>	Spare; requires appropriate feature license(s)	

## Additional Information

More information about Cisco IOS Software Release 12.2(14)SX is available in the Cisco Catalyst 6500 Series and Cisco 7600 Series Release Notes at:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/>

Cisco Catalyst 6500 Series documentation is available at:

<http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/>

and

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/>

Cisco 7600 Series documentation is available at:

<http://www.cisco.com/warp/public/cc/pd/rt/7600osr/>



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 Systems, Cisco IOS, the Cisco Systems logo, Cisco Unity, and EtherSwitch are registered trademarks or 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.  
(0303R) 203070/ETMG 06/03