

## CISCO IOS SOFTWARE RELEASE 12.2(18)SXD SECURITY FEATURES

### 1. CISCO IOS SOFTWARE RELEASE 12.2S INTRODUCTION

Cisco IOS<sup>®</sup> Software Release 12.2S is designed for Enterprise campus and Service Provider edge networks that require world-class IP and Multiprotocol Label Switching (MPLS) services. The Cisco Catalyst<sup>®</sup> Switches and high-end routers in Release 12.2S provide secure, converged network services in the most demanding Enterprise and Service Provider environments, from the wiring closet and data center to the WAN aggregation edge.

The infrastructure innovation and technology leadership in Release 12.2S enable advanced Ethernet LAN switching, Metro Ethernet, and Broadband Aggregation services through enhancements in High Availability, Security, MPLS, VPNs, and IP Routing and Services.

Releases 12.2(22)S, 12.2(20)S, 12.2(18)S, and 12.2(14)S are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, refer to Release 12.2S New Features and Hardware Support, Product Bulletin No. 2216.

Derived from Release 12.2(14)S, Release 12.2SX provides Release 12.2S functionality and new features and hardware support for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

In addition to Release 12.2(18)SXD, Releases 12.2(17d)SXB, 12.2(17b)SXA, 12.2(17a)SX, and 12.2(14)SX are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, please visit:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletins_list.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletins_list.html)

#### 1.1 Release 12.2SX Ordering Information, Feature Sets, and Image Names

Refer to the “Feature Sets” section of the Release 12.2SX release notes for information about Release 12.2SX orderable product numbers, feature sets, and image names.

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_release\\_note09186a00801c8339.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_release\\_note09186a008019e1e9.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a008019e1e9.html)

#### 1.2 Additional Information

- Cisco IOS Software Release 12.2S

<http://www.cisco.com/go/release122s/>

- Cisco IOS Software Release feedback and questions

<http://www.cisco.com/warp/public/732/feedback/release/>

- Cisco IOS Software Product Lifecycle Dates & Milestones

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_bulletin09186a00801a1349.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin09186a00801a1349.html)

## 2 RELEASE 12.2(18)SXD SECURITY FEATURES

### 2.1 Control Plane Policing

Even the most robust software implementations and hardware architectures are vulnerable to Denial of Service (DoS) attacks. DoS attacks are malicious acts designed to cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the control plane processor. By involving hundreds of sources, distributed DoS attacks multiply the amount of worthless IP traffic, sometimes by as much as many gigabytes per second. These IP streams contain packets that are destined for processing by the control plane of Cisco route processors. Based on the high rate of rogue packets presented to the route processor, the control plane must spend an inordinate amount of time processing and discarding the DoS traffic.

Control Plane Policing provides users with a mechanism to control the type and rate of traffic that hits the control-plane of the device, and thereby helps to maintain packet forwarding and protocol states while the router is under attack. Control Plane Policing leverages Modular Quality of Service (QoS) CLI (MQC) to provide a programmable policing functionality on routers that filter and rate limit (or police) traffic destined to the control plane. This policing functionality can be used in conjunction with Cisco IOS QoS classification mechanisms to identify and limit certain traffic types completely, or to target only those that exceed a specified threshold level.

#### Benefits

- Streamlines incoming rate of traffic destined to the control plane
- Protects against attacks targeted towards the network infrastructure
- Easily defines global policy commands to address the aforementioned security goals using the Cisco MQC infrastructure

#### Hardware

Routers	Cisco 7600 Series Router
Switches	Cisco Catalyst 6500 Series Switch

#### Additional Information

<http://www.cisco.com/go/autosecure/>

#### Product Management Contact

IOS-Security-PM@cisco.com

### 2.2 Secure Copy

#### Description

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files.

#### Benefits

SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the copy command. An authorized administrator may also perform this action from a workstation.

## Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst Series, Supervisor Engine 720, Supervisor Engine 2

## Additional Information

[://www.cisco.com/go/iossecurity/](http://www.cisco.com/go/iossecurity/)

## Product Management Contact

[ios-security-pm@cisco.com](mailto:ios-security-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.  
168 Robinson Road  
#28-01 Capital Tower  
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 • 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

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo 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.  
(0403R) 204068\_ETMG\_SH\_08.04