



Cisco IOS Release 12.0(22)S Consolidates the 12.0S and 12.0ST Images

Introduction

This Product Bulletin describes the content and delivery information concerning Cisco IOS™ software release 12.0(22)S. 12.0(22)S is the consolidated image of 12.0S and 12.0ST and the preferred train for the C7200, C7500, C10000, C10720, and C12000 product families.

The 12.0S train was introduced in July 1999 to provide unique services to providers operating core networks built primarily around the C12000 and C7200/7500 series routers. One year later the first 12.0ST image was shipped for a select set of customers to pioneer advanced MPLS features including LDP, VPNs, COS, FRR, and MPBGP.

12.0ST was derived from the 12.0S code and has been a super set of the 12.0S train, inclusive of all 12.0S features and bug fixes. Regular synchronization of the two images has been maintained with the objective of consolidation, once the 12.0ST image had reached the stability and quality of the 12.0S train.

12.0(22)S is the result of the consolidation of 12.0S and 12.0ST. Along with the consolidation, a number of additional features have been introduced, which are summarized in the tables below.

Support Plans for 12.0ST

All feature support required by customers running the 12.0ST image will continue to be available in the 12.0S train. Any new features and hardware will go into the single consolidated image going forward. The end of sales, end of engineering, and end of life for the content of the 12.0ST image will be deferred until such plans are developed for 12.0S. However, the following schedule is relevant for the orderable product codes containing 12.0ST nomenclature.

- EOS - End of Sales for the 12.0ST image will occur on January 31, 2003.
- EOE - End of engineering support for the 12.0ST image will occur on March 31, 2003. The image shipped by this date will be the last 12.0(21)ST image incorporating bug fixes.
- EOL - End of life for the 12.0ST image will correspond with the end of support by the TAC. This will occur on January 31, 2008.

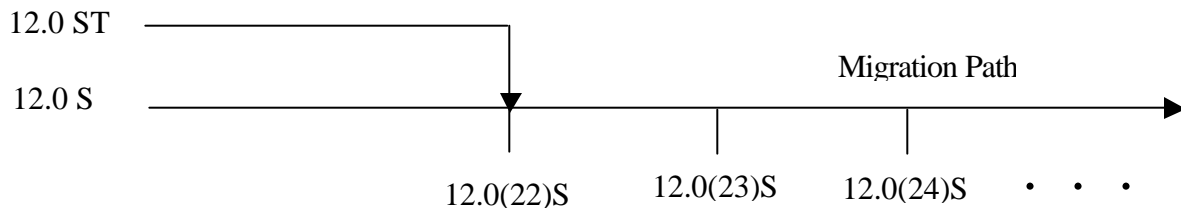


Special Diagnostic Image for 12.0(22)S

A separate image has been created for those customers wishing to run board level diagnostics on the C12000 routers. Board level diagnostics allow for troubleshooting in the event of a suspected hardware failure. This image had been previously bundled in the 12.0S code. It was removed to allow customers the option of continuing with the 20MB flash disk storage on the GRP or migrating to a 64MB flash disk, and allow for flexibility in always using the latest version of field diagnostics. The new field diagnostic image can be stored on a separate 20MB flash disk, on a TFTP server, or along with the 12.0(22)S image using a 64MB flash disk. The field diagnostic image is available on the Cisco Connection Online under the name c12k-fdiagsbflc-mz.

Migration Guide

The diagram below displays Cisco 12.0(22)S release functionality relative to the 12.0S and 12.0ST releases. 12.0 S is the migration path going forward with 12.0(22)S as the first release on the consolidated path.



New Features in 12.0(22)S

The following tables summarize the new features added to the 12.0(22)S release including new hardware additions to the platforms along with software features. These features are in addition to those supported previously in the 12.0(21)S and 12.0(21)ST images.



New Hardware Support Introduced in 12.0(22)S

New Hardware introduced in 12.0(22)S	Cisco 7XXX	Cisco 10720	Cisco 10XXX	Cisco 12XXX
PA-MC-8TE1+ Port Adapter	X			
RSP16	X			
VIP6	X			
Console/Auxiliary Module		X		
4-Port Gigabit Ethernet 8-Port 10/100 BASE-TX Access Card		X		
24-Port E1 Line Card			X	
4-port OC-3c/STM-1c POS/SDH ISE				X
8-port OC-3c/STM-1c POS/SDH ISE				X
8-Port OC-3 STM-1 ATM Line Card				X
Performance Route Processor (PRP-1)				X

Table 1. Cisco IOS Release 12.0(22)S New Hardware

New Software Support Introduced in 12.0(22)S

New Software Features introduced in 12.0(22)S	Cisco 7XXX	Cisco 10720	Cisco 10XXX	Cisco 12XXX
ARP Optimization	X			X
Auto Install		X		
Automatic Protection Switching on 2-Port Channelized OC-3/STM-1 (DS1/E1)				X
Auto-Shutdown Feature Changes			X	
BGP Hybrid CLI	X		X	X
BGP Increased Support of Numbered AS-path Access Lists to 500	X		X	X
BGP Policy Accounting Support			X	
BGP Policy Accounting on Engine 4 Plus Line Cards				X
BGP Prefix-Based Outbound Route Filtering	X		X	X
BGP Restart Session After Max-prefix Limit	X		X	X
BGP Route-map Policy List Support	X		X	X
BGP Update Packing	X		X	X
Cisco Nonstop Forwarding with Stateful Switchover	X		X	X
Facility-alarm Command			X	
Frame Relay Fast Restart	X		X	
HSRP Support for MPLS-VPNs			X	
IP Event Dampening	X		X	X
IP Receive ACL				X
IP Source Tracker Supported on the 7500 Series Routers	X			



New Software Features introduced in 12.0(22)S	Cisco 7XXX	Cisco 10720	Cisco 10XXX	Cisco 12XXX
Ipv6 Enhancements				X
IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements	X	X		X
MIB Additions and Enhancements			X	X
MPLS AToM—Ethernet over MPLS in Cisco 10720 Internet Routers		X		
MPLS layer 3 VPN enhancements – Inter AS and Carrier Supporting Carrier		X		X
MPLS Traffic Engineering (TE)—Interarea Tunnels			X	
MPLS Traffic Engineering (TE)—Link and Node Protection	X			X
MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE)				X
MPLS VPN - VRF Selection Based on Source IP Address				X
Multicast Forwarding on IP Service Engine Line Cards				X
Multi-VPN Routing and Forwarding Tables		X		
Nested Policies			X	
OSPF Sham-Link Support for MPLS VPN			X	
Parser Cache	X	X	X	X
Policy-Based Routing on Engine 4 Plus Line Cards				X
Privilege Command Enhancements				X
Reserve Memory for Console Access	X			X
Routing Table Improvements			X	
Tunnel mpls traffic-eng autoroute announce Command			X	
Unicast Reverse Path Forwarding Checking			X	X

Table 1. Cisco IOS Release 12.0(22)S Software Features

Detailed Information

ARP Optimization

In previous versions of Cisco IOS, the ARP table was organized for easy searching on an entry based on the IP address. However, there are cases such as interface flapping on the router and a topology change in the network in which all related ARP entries need to be refreshed for correct forwarding. This situation could consume a significant amount of CPU time in the ARP process to search and clean up all the entries. The ARP Optimization feature improves ARP performance by reducing the ARP searching time by using an improved data structure.

Auto Install on the 10720 Internet Routers

The AutoInstall feature allows you to configure a new Cisco 10720 Internet router automatically and dynamically. The AutoInstall procedure involves connecting a new router to a network in which an existing router is preconfigured, turning on the new router, and enabling it with a configuration file that is automatically downloaded from a TFTP server, reachable through the dynamic packet transport (DPT) /Spatial Reuse Protocol (SRP) uplink interface on the Cisco 10720 Internet router. If no startup configuration has already been saved in the router, the AutoInstall procedure is invoked when the router starts.



Automatic Protection Switching on 2-Port Channelized OC-3/STM-1 (DS1/E1) Line Cards

This feature allows switchover of Packet-over-SONET (POS) circuits in the event of circuit failure and is often required when connecting SONET equipment to telco equipment. APS refers to the mechanism of using a "protect" POS interface in the SONET network as the backup for the "working" POS interface. When the working interface fails, the protect interface quickly assumes its traffic load. The protection mechanism used for this feature has "1+1, architecture" as described in the Bellcore publication TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3. The connection may be bidirectional or unidirectional, and revertive or nonrevertive.

Auto-Shutdown Feature Changes

In Cisco IOS Release 12.0(22)S, the following changes have been made to the Auto-Shutdown feature for the Cisco 10000 series edge services routers (ESR):

- Fan events no longer cause an auto-shutdown of the ESR. This behavior differs from the behavior noted on the fan tray labels.
- By default, the ESR no longer shuts down automatically when a critical temperature threshold is exceeded. Now, you must enable auto-shutdown by issuing the facility-alarm command with critical exceed-action shutdown keyword. Then, if the core temperature exceeds its critical threshold (85°C) for 2 minutes, or the intake temperature exceeds its critical threshold (67°C) for 2 minutes, the ESR shuts down automatically.

BGP Hybrid CLI

The BGP Hybrid CLI feature simplifies the migration of Border Gateway Protocol (BGP) networks and existing configurations from the Network Layer Reachability Information (NLRI) format to the address-family identifier (AFI) format. This new functionality allows the network operator to configure commands in the AFI format and save these command configurations to existing NLRI formatted configurations. The feature provides the network operator with the capability to take advantage of new features and provides support for migration from the NLRI format to the AFI format. The BGP Hybrid CLI feature is present in Cisco IOS Release 12.0(22)S and later software releases and does not require the network operator to perform any specific configuration tasks.

BGP Increased Support of Numbered AS-path Access Lists to 500

The BGP Increased Support of Numbered AS-path Access Lists to 500 feature is an enhancement for Border Gateway Protocol (BGP) autonomous system accesslists. This enhancement increases the maximum number autonomous system access lists from 199 to 500.

BGP Policy Accounting Support

The BGP Policy Accounting feature allows you to account for IP traffic differentially by assigning counters based on community-list, autonomous system (AS) number, and AS-path on a per the input interface basis. For the policy accounting feature to work, you must enable BGP and Cisco Express Forwarding/distributed Cisco Express Forwarding (CEF/dCEF) on the router. Using BGP policy accounting, you can account for traffic (and apply billing) according to the route it traverses. For example, you can account for traffic that is routed domestic, international, terrestrial, or satellite. In this way, you can identify and account for all traffic on a per-customer basis.



Support for BGP Policy Accounting in 12.0(22)S has been added for the following products:

- Cisco 10000 series ESR
- 1-port OC-192c/STM-64c POS/SDH (Cisco 12000 series Engine 4 Plus line card)
- 1-port OC-192c/STM-64c POS/SDH (Cisco 12000 series Engine 4 Plus line card)

BGP Prefix-Based Outbound Route Filtering

The BGP Prefix-Based Outbound Route Filtering feature uses Border Gateway Protocol (BGP) outbound route filter (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between peer routers. Configuration of this feature can help reduce the amount of resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.

BGP Restart Session After Max-prefix Limit

The BGP Restart Session After Max-prefix Limit feature enhances the capabilities of the neighbor maximum-prefix command with the introduction of the restart keyword. This enhancement allows the network operator to configure the time interval at which a peering session is reestablished by a router when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. The restart keyword has a configurable timer argument that is specified in minutes. The time range of the timer argument is from 1 to 65535.

BGP Route-map Policy List Support

The BGP Route-map Policy List Support feature introduces new functionality to Border Gateway Protocol (BGP) route maps. This feature adds the capability for a network operator to group route-map match clauses into a named list called a policy list. A policy list functions like a macro within a route map. When the policy list is referenced within a route map with the match policy-list command, all match statements in the policy list are executed. Policy lists can be used for all applications of a route map and for redistribution between routing protocols. Policy lists can coexist with configured match and set clauses within the same subblock. Policy lists, however, do not support set statements, and policy lists are not supported by IP routing policy.

BGP Update Packing

The BGP Update Packing feature introduces a new caching mechanism to reduce the amount of time that is required for Border Gateway Protocol (BGP) convergence. Neighbor update messages are stored in a cache until the update message is the maximum size and then the update is forwarded to neighbors. Updates are cached and forwarded based on peer groups and per-individual neighbors.)

Cisco 10000 ESR MIB Enhancements

MIB enhancements in Cisco IOS Release 12.0(22)S provide enhanced management features that enable the Cisco 10000 series edge services routers (ESR) to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to do the following:

- Use SNMP set and get requests to access information in ESR MIBs.



- Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers.

Cisco Nonstop Forwarding with Stateful Switchover

Cisco Nonstop Forwarding (NSF) is a complementary feature to the Stateful Switchover (SSO) feature in Cisco IOS software. NSF always runs together with SSO and works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability. NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the Standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the Active RP is key to NSF operation.

Stateful Switchover is particularly useful at the network edge. Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with dual route processors (RPs) that represent a single point of failure in the network design, and at which point an outage might result in loss of service for customers. In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them. A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Facility-alarm Command

A new keyword (critical exceed-action shutdown) allows you to enable or disable the auto-shutdown feature on the Edge Services Router (ESR). Previously, auto-shutdown was enabled by default. When auto-shutdown is enabled, the ESR shuts down automatically when its core or intake temperature exceeds the critical temperature threshold for 2 minutes.

Frame Relay Fast Restart

The Frame Relay Fast Restart feature increases network availability by reducing recovery time from Route Processor (RP) failures on Cisco routers in Frame Relay networks. This feature reduces recovery time by accelerating the transition from primary RP to standby RP after a hardware or software failure. When a switchover from primary RP to standby RP occurs on a router that has been configured for Frame Relay encapsulation, the router must implement an initialization procedure to bring permanent virtual circuits (PVCs) back up and to reestablish dynamic mappings. While this procedure is under way, the Frame Relay interface is unavailable for traffic forwarding. Before the introduction of this feature, the initialization



procedure took from 30 to 90 seconds to complete on each Frame Relay interface. The Frame Relay Fast Restart feature reduces interface restart time to 10 to 15 seconds.

HSRP Support for MPLS VPNs

Hot Standby Router Protocol (HSRP) support on a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) interface is useful when an Ethernet is disconnected between two provider edges (PEs) with either of the following:

- A customer edge (CE) with a default route to the HSRP virtual IP address
- One or more hosts with the HSRP virtual IP address configured as the default gateway

Each VPN is associated with one or more VPN routing/forwarding (VRF) instances. A VRF consists of the following:

- IP routing table
- Cisco Express Forwarding (CEF) table
- Set of interfaces that use the CEF forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a router within the VPN. HSRP currently adds Address Resolution Protocol (ARP) entries and IP hash table entries (aliases) using the default routing table instance. However, a different routing table instance is used when VRF forwarding is configured on an interface, causing ARP and Internet Control Message Protocol (ICMP) echo requests for the HSRP virtual IP address to fail.

The HSRP Support for MPLS VPNs feature ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table. Session Idle Timeout Timer (configurable per APN) GGSN support for radius attributes for session/ idle timeout on a per session basis. In GGSN 1.4 the idle timer granularity is at the GGSN level. Idling PDP contexts are delete when the timer expires GGSN 3.0 provides a per session idle timer. The timer value can be configured:

- per APN
- based on RADIUS attribute
- per GGSN

IP Event Dampening

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events to the routing protocols and the routing table. This feature allows the network operator to configure a router to identify and dampen flapping interfaces, thereby reducing the utilization of system processing resources and improving network stability.



IP Receive ACL

The IP Receive ACL feature provides basic filtering capability for traffic that is destined for the router; that is, the router can protect high priority routing protocol traffic from an attack because the filtering occurs after any input access control list (ACL) on the ingress interface. This feature may be implemented in a security solution to protect a router from remote intrusions. Access to the router can be restricted to known, trusted sources and expected traffic profiles.

IP Source Tracker Supported on the 7500 Series Routers

The IP Source Tracker feature allows you to gather information about the traffic flowing to a host that is suspected to be under attack. This feature also allows you to easily trace an attack back to its entry point into the network. After you identify the destination being attacked, you can enable tracking for the destination address on the router by entering the ip source-track command. Each line card or port adapter creates a special Cisco Express Forwarding (CEF) entry for the destination address being tracked. For line cards or port adapters that use specialized application specific integrated circuits (ASICs) to do packet switching, the CEF entry is used to punt packets to the CPU of the line card or the CPU of the port adapter. These CPUs collect information about the traffic flow to the tracked destination.

IPv6 Phase2

The following IPv6 enhancements have been added to the C12000:

- **CEFv6/dCEFv6—Cisco Express Forwarding:** Cisco Express Forwarding for IPv6 (CEFv6) is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed CEF for IPv6 (dCEFv6) performs the same functions as CEFv6 but for distributed architecture platforms such as the Cisco 12000 series Internet routers. dCEFv6 and CEFv6 function the same and offer the same benefits as dCEFv4 and CEFv4.
- **IPv6 Provider Edge Router over MPLS:** The IPv6 Provider Edge Router over MPLS feature (also referred to as Cisco 6PE) enables IPv6 sites to communicate over a Multiprotocol Label Switching (MPLS) IPv4 network with no software or hardware upgrades in the core MPLS infrastructure and with no disruption to existing customer services.
- **IPv6 RIP Enhancements:** The IPv6 RIP Enhancements feature adds support for a separate IPv6 Routing Information Protocol (RIP) routing table, the ability to delete routes from the IPv6 RIP routing table, and the ability to set route tags. The holddown timer default is now set to zero, and a maximum number of parallel routes can be configured.
- **Secure Shell (SSH) over an IPv6 Transport:** Secure Shell (SSH) in IP version 6 (IPv6) functions the same and offers the same benefits as SSH in IPv4—the SSH Server feature enables an SSH client to make a secure, encrypted connection to a Cisco router and the SSH Client feature enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running an SSH server. IPv6 enhancements to SSH consist of support for IPv6 addresses that enable a Cisco router to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.



IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

This feature provides two IS-IS mechanisms to exclude IP prefixes of connected networks from label-switched path (LSP) advertisements, thereby reducing IS-IS convergence time.

MIB Enhancements and Additions

The following MIB additions have been added to provide support on the Cisco 12000 routers:

- **SNMP Support for Class Based QoS on Cisco 12000 Series Line Cards**: This feature adds Simple Network Management Protocol (SNMP) monitoring support to the Engine 2, Engine 3, Engine 4, and Engine 4plus (E4+) Cisco 12000 series line cards for Quality of Service (QoS). QoS is configured on Cisco devices using the Modular QoS CLI (MQC). E4+ line cards now support MQC configuration. The managed objects for QoS are defined in the Cisco Class-Based Quality of Service MIB (CISCO-CLASS-BASED-QOS-MIB.my). This MIB provides read access to QoS configurations and provides QoS statistics information based on the Modular QoS CLI (MQC), including information regarding class map and policy map parameters.
- **CISCO-APS-MIB**: The Cisco SONET Linear Automatic Protection Switching (APS) MIB module supports the configuration and management of SONET linear APS groups. The definitions and descriptions that are used in this MIB are derived from SONET Transport Systems: Common Generic Criteria, GR-253-CORE Revision 2, section 5.3. The MIB is also consistent with the Multiplex Section Protection (MSP) protocol as specified in ITU-T Recommendation G.783, Characteristics of synchronous digital hierarchy (SDH) equipment function blocks, Annex A and B. Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers.
- **CISCO-ENHANCED-WRED-MIB**: The Cisco Enhanced WRED MIB (CISCO-ENHANCED-WRED-MIB) provides WRED packet configuration and packet filtering information. This MIB provides the WRED information about the transmit (Tx) side and receive (Rx) side of the modules, for the managed systems that support WRED on both the transmit side and the receive side.
- **SNMPv3 Community MIB Support**: The SNMPv3 Community MIB Support feature implements support for the SNMP Community MIB (SNMP-COMMUNITY-MIB) module, defined in RFC 2576, in Cisco IOS software.
- **SNMP Notification Logging**: This feature implements support for the Notification Log MIB (defined in RFC 3014) in Cisco IOS software. Systems that support SNMP often need a mechanism for recording notification information as a hedge against lost notifications, whether those are traps or informs that exceed retransmission limits. The Notification Log MIB provides a common infrastructure for other MIBs in the form of a local logging function. The SNMP Notification Logging feature adds Cisco IOS Command Line Interface (CLI) commands to change the size of the notification log, to set the global ageout value for the log, and to display logging summaries at the command line.

MIB enhancements in Cisco IOS Release 12.0(22)S provide enhanced management features that enable the Cisco 10000 series edge services routers (ESR) to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to do the following:

- Use SNMP set and get requests to access information in ESR MIBs.



- Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers.

MPLS AToM—Ethernet over MPLS in Cisco 10720 Internet Routers

The MPLS AToM—Ethernet over MPLS feature, part of the Any Transport over Multiprotocol Label Switching (MPLS) (AToM) product set, is now supported on the Cisco 10720 Internet routers. This feature allows you to connect two VLAN networks that are in different locations, without using expensive bridges, routers, or switches at the VLAN locations. You enable the MPLS backbone network to accept Layer 2 VLAN traffic by configuring the label edge routers (LERs) at both ends of the MPLS backbone. The Cisco 10720 Internet router also supports the VLAN ID Rewrite feature for Ethernet over MPLS (EoMPLS) connections. The egress side of an EoMPLS connection that is mapped to a VLAN rewrites the VLAN ID in outgoing packets to the ID of the local VLAN. This feature allows you to use VLAN interfaces with different VLAN IDs at either end of the MPLS backbone.

MPLS layer 3 VPN enhancements – Inter AS and Carrier Supporting Carrier

- Carrier supporting carrier is a term used to describe a situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier. The Carrier Supporting Carrier (CsC) feature enables an MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network.
- The MPLS VPN—Inter-Autonomous System Support feature allows a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) to span service providers and autonomous systems. As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. Also, some VPNs need to extend across multiple service providers (overlapping VPNs). Regardless of the complexity and location of the VPNs, the connection between autonomous systems must be seamless to the customer. The MPLS VPN—Inter-Autonomous System Support feature provides that seamless integration of autonomous systems and service providers. Separate autonomous systems from different service providers can communicate by exchanging IPv4 network layer reachability information (NLRI) in the form of VPN-IPv4 addresses.

MPLS Traffic Engineering (TE)—Interarea Tunnels

The MPLS Traffic Engineering (TE)—Interarea Tunnels feature allows you to establish Multiprotocol Label Switching (MPLS) TE tunnels that span multiple Interior Gateway Protocol (IGP) areas and levels, removing the restriction that had required that the tunnel headend and tailend routers both be in the same area. The IGP can be either Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

MPLS Traffic Engineering (TE)—Link and Node Protection, with RSVP Hellos Support

Fast ReRoute (FRR) is a mechanism for protecting Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) label-switched paths (LSPs) from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on the LSPs while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR



locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes. Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the next hop of the LSP's path. FRR provides node protection for LSPs with backup tunnels that bypass next-hop nodes along LSP paths. Such tunnels are called next-next-hop (NNH) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of Resource Reservation Protocol (RSVP) Hellos to accelerate the detection of node failures. NHOP backup tunnels also provide protection from link failures because they bypass the failed link as well as the node.

MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE)

The MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature provides the Enhanced Interior Gateway Routing Protocol (EIGRP) with the capability to redistribute routes through a Border Gateway Protocol (BGP) Virtual Private Network (VPN) cloud. This feature is configured only on PE routers, requiring no upgrade or configuration changes to customer equipment. This feature also introduces EIGRP support for Multiprotocol Label Switching (MPLS) and BGP extended community attributes.

MPLS VPN—VRF Selection Based on Source IP Address

The VRF Selection feature allows packets that arrive on an interface to be switched into the appropriate Virtual Private Network (VPN) routing/forwarding (VRF) Selection table based upon the source IP address of the packets. Once the packets have been "selected" into the correct VRF Selection routing table, they are processed normally based upon the destination address and forwarded through the rest of the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

Multicast Forwarding on IP Service Engine Line Cards

Cisco IOS Release 12.0(22)S introduces hardware engine-based multicast forwarding on the following Cisco 12000 series IP Service Engine (ISE) line cards (also referred to as Engine 3 line cards):

- 1-port Channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c) POS/SDH, OC-12c/STM-4c
- 4-port OC-12c/STM-4c POS/SDH
- 4-port Channelized OC-12/STM-4 (DS3/E3, OC-3c/STM-1c) POS/SDH
- 16-port OC-3c/STM-1c POS/SDH
- 16-port Channelized OC-3/STM-1 (DS3/E3) POS/SDH

Multi-VPN Routing and Forwarding Tables

The Multi-VPN Routing and Forwarding Tables feature (also referred to as the Multi-VRF feature) extends limited provider edge (PE) router functionality to a customer edge (CE) router in an Multiprotocol Label Switching (MPLS) virtual private



network (VPN) configuration. When used as a CE router, the Cisco 10720 Internet router can now maintain separate VPN routing and forwarding (VRF) tables in order to extend the privacy and security of an MPLS VPN down to a branch office instead of only to the PE router node. The Cisco 10720 Internet router supports up to:

- 999 VRF entries for static routes
- 200 VRF entries that use the Border Gateway Protocol (BGP) to distribute VPN routing information
- 30 VRF entries that use the Open Shortest Path First (OSPF) protocol to distribute VPN routing information

Nested Policies

The Cisco 1000 now provides for nested policies. A nested policy allows multiple classes and subclasses of IP traffic to be shaped at a single rate. This feature provides the following benefits:

- Allows traffic from multiple queues to be shaped at a single rate, which provides a way to implement fair queues on virtual circuits.
- Enables you to shape the aggregate traffic of fair queues on a physical interface (for example, to provide a 10-Mbps service on a 100-Mbps physical interface).
- Enables you to specify the maximum transmission rate for traffic that is queued separately.
- Enables a single class of traffic to be divided into one or more subclasses.
- Can be applied to physical interfaces and to logical interfaces such as Frame Relay or VLAN interfaces.

OSPF Sham-Link Support for MPLS VPN on C10000

In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configuration, the Open Shortest Path First (OSPF) protocol is one way you can connect customer edge (CE) routers to service provider edge (PE) routers in the VPN backbone. OSPF is often used by customers that run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone.

Parser Cache

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files. The Parser Cache feature can rapidly recognize and translate configuration lines that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on) by dynamically creating, caching, and reusing simplified parse graphs. This improvement is especially useful for configuration files that repeat similar commands hundreds or thousands of times, such as when thousands of virtual circuits must be configured for subinterfaces or when hundreds of access lists must be configured. Cisco testing indicates an improvement to load time of up to 36 percent for large configuration files when using the Parser Cache feature. Performance will increase the most for those files in which the same



commands are used repeatedly but the numerical arguments change from command to command. The Parser Cache feature is enabled by default.

Policy Based Routing

Policy-based routing is supported on Cisco 12000 series Engine 4 Plus line cards, including the following:

- 4-port OC-48c/STM-16c POS/SDH
- 1-port OC-192c/STM-64c POS/SDH

By using policy-based routing, you can implement policies that selectively cause packets to take different paths.

On Cisco 12000 series Engine 4 Plus line cards, policy routing with committed access rate (CAR) provides a mechanism to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques enabled through the Cisco IOS software. These queuing techniques provide an extremely powerful, simple, and flexible tool for network managers who implement routing policies in their networks.

Privilege Command Enhancements

This feature simplifies the configuration of privilege levels for specific commands through the enhancement of the "privilege level" global configuration command. A privilege level can now be specified for all keyword options of a command with a single command-line interface (CLI) command. Previously, separate "privilege level" commands were required for each keyword combination of a command. This enhancement can significantly reduce the number of commands needed to configure user privilege levels and correspondingly reduce the size of configuration files.

Reserve Memory for Console Access

When a router is low on memory or heavily fragmented, console access is not allowed. This feature implements memory reserve sufficient to allow login via the console. This gives administrators the ability to log in to the router in any situation and perform administrative tasks and troubleshooting even when the router is running low on memory.

Routing Table Improvements

Cisco IOS Release 12.0(22)S increases the number of routes allowed in the routing table of the Cisco 10000 series edge services (ESR) router to the following approximate values:

- 450,000 global routes
- 230,000 MPLS/VPN routes

It is hard to specify the exact number of routes allowed in the routing table because the distribution of IP addresses affects the routing table storage capacity. Routes are stored in the Mtrie structure, which is part of the IP lookup algorithm used in Cisco Express Forwarding (CEF). Routes with a similar IP address (those that share an IP address prefix) take up less space in the Mtrie structure than routes with dissimilar addresses. This means that the structure can hold more routes if the routes share a similar IP address.



Unicast Reverse Path Forwarding Checking

The Cisco 10000 series edge services router (ESR) supports enhancements to the ip verify unicast command to allow Unicast Reverse Path Forwarding (uRPF) checks to be made in strict or loose mode:

- Loose mode—Checks that a packet's source IP address is reachable over any interface on the ESR.
- Strict mode—Checks that a packet's source IP address is reachable over the interface on which the packet was received.

The forwarding application specific integrated circuit (ASIC) on Cisco 12000 series Engine 4 Plus (E4+) line cards is designed to support the enhanced "loose check" version of unicast Reverse Path Forwarding (uRPF) on the following line cards in Cisco 12000 series Internet routers:

- 4-port OC-48c/STM-16c POS/SDH
- 1-port OC-192c/STM-64c POS/SDH

For more detailed information about the platforms and features being delivered in 12.0(22)S, please reference the following documents:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/relnote/12000ser/index.htm>

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

Support

Cisco IOS software release 12.0(22)S follows the standard Cisco support policy as indicated in the following link:

<http://www.cisco.com/warp/public/437/37.html>

Product Numbers

Cisco IOS Release 12.0(22)S Feature Sets, Images, and Memory Recommendations



Platform	Software Feature Set	Product Code	Image	Flash	DRAM
12000	Cisco 12000 Series IOS SERVICE PROVIDER	S120Z-12.0.22S	gsr-p-mz	20MB	256MB
12000	Cisco 12000 Series IOS SERVICE PROVIDER/SECURED SHELL 56	S120K3Z-12.0.22S	gsr-k3p-mz	20MB	256MB
12000	Cisco 12000 Series IOS SERVICE PROVIDER/SECURED SHELL 3DES	S120K5Z-12.0.22S	gsr-k4p-mz	20MB	256MB
12KPRP	Cisco 12K Series PRP IOS SERVICE PROVIDER	S12KZ-12.0.22S	c12kprp-p-mz	64MB	512MB
12KPRP	Cisco 12K Series PRP IOS SERVICE PROVIDER/SECURED SHELL 56	S12KK3Z-12.0.22S	c12kprp-k3p-mz	64MB	512MB
12KPRP	Cisco 12K Series PRP IOS SERVICE PROVIDER/SECURED SHELL 3DES	S12KK5Z-12.0.22S	c12kprp-k4p-mz	64MB	512MB
12000 12KPRP	Cisco 12000 Series FIELD DIAGNOSTICS	N/A	c12k-fdiasgbflc-mz	20MB	256MB
7200	Cisco 7200 Series IOS SERVICE PROVIDER	S72Z-12.0.22S	c7200-p-mz	16MB	128MB
7200	Cisco 7200 Series IOS SERVICE PROVIDER/SECURED SHELL 56	S72K3Z-12.0.22S	c7200-k3p-mz	16MB	128MB
7200	Cisco 7200 Series IOS SERVICE PROVIDER/SECURED SHELL 3DES	S72K5Z-12.0.22S	c7200-k4p-mz	16MB	128MB
7500	Cisco RSPx Series IOS SERVICE PROVIDER	S75Z-12.0.22S	rsp-pv-mz	16MB	128MB
7500	Cisco RSPx Series IOS SERVICE PROVIDER/SECURED SHELL 56	S75K3Z-12.0.22S	rsp-k3pv-mz	16MB	128MB
7500	Cisco RSPx Series IOS SERVICE PROVIDER/SECURED SHELL 3DES	S75K5Z-12.0.22S	rsp-k4pv-mz	16MB	128MB
10720	Cisco 10700 Series IOS SERVICE PROVIDER	S107Z-12.0.22S	c10700-p-mz	40MB	256MB
10720	Cisco 10700 Series IOS SERVICE PROVIDER/SECURED SHELL	S107K5Z-12.0.22S	c10700-k4p-mz	40MB	256MB
10000	Cisco 10000 Series IOS EDGE SERVICES ROUTER	S10KZ1-12.0.22S	c10k-p10-mz	40MB	512MB
10000	Cisco 10000 Series IOS SERVICE PROVIDER/SECURED SHELL 3DES	S10KK5Z1-12.0.22S	c10k-k4p10-mz	40MB	512MB

CISCO SYSTEMS



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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France

www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912

www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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

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 © 1992–2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARtnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO 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. (0203R)