Release Notes for Cisco 7200 VXR Router on the NPE-G2 for Cisco IOS Release 12.2 XN

August 23, 2007

Cisco IOS Release 12.2(31c)XN3

OL-10966-10

These release notes for the Cisco 7200 VXR router describe the enhancements provided in Cisco IOS Release 12.2(31c)XN3. Cisco IOS Release 12.2(31c)XN3 is a rebuild of Cisco IOS Release 12.2(31)XN. Cisco IOS Release 12.2(31)XN is based on Cisco IOS Release 12.2(28)SB and Cisco IOS Release 12.2(31)SB2.

Note These release notes list only features that are new to Cisco IOS Release 12.2(31c)XN3, Cisco IOS Release 12.2(31b)XN3, Cisco IOS Release 12.2(31a)XN3, Cisco IOS Release 12.2(31)XN3, Cisco IOS Release 12.2(31c)XN2, Cisco IOS Release 12.2(31b)XN2, Cisco IOS Release 12.2(31)XN2, Cisco IOS Release 12.2(31)XN1, Release 12.2(31)XN, and features inherited from Cisco IOS Release 12.2(28)SB.

For features inherited from Cisco IOS Release 12.2(31)SB2, refer to the *Cross-Platform Release Notes for Cisco IOS Release 12.2SB* located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122sb.htm

For a list of the software caveats that apply to Cisco IOS Release 12.2(31c)XN3, see the "Caveats for Cisco IOS Release 12.2 XN" section on page 69.

Contents

These release notes describe the following topics:

- Inheritance Information, page 2
- System Requirements, page 51
- New and Changed Information, page 57

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Caveats for Cisco IOS Release 12.2 XN, page 69
- Related Documentation, page 92
- Documentation Feedback, page 94

Inheritance Information

Cisco IOS Release 12.2(31c)XN3 is based on Cisco IOS Release 12.2(28)SB and Cisco IOS Release 12.2(31)SB. Features supported on Cisco 7200 platforms in Cisco IOS Release 12.2(28)SB and Cisco IOS Release 12.2(31)SB2 are supported in Cisco IOS Release 12.2(31c)XN3.

Use these inherited feature descriptions with the *Cross-Platform Release Notes for Cisco IOS Release 12.2SB* located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122sb.htm

C7200-Specific Features Inherited from Cisco IOS Release 12.2(28)SB

This section describes the new and changed features in Cisco IOS Release 12.2(28)SB. Some features may have been new to Cisco IOS Release 12.2SB but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and changed in Cisco IOS Release 12.2(28)SB. To determine if a feature was new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

AAA Features

Cisco IOS Release 12.2(28)SB introduces support for the following authentication, authorization, and accounting (AAA) features.

AAA CLI Stop Record Enhancement

The **aaa accounting send stop-record authentication** command was updated with additional support for AAA accounting stop records.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

AAA Double Authentication Secured by Absolute Timeout

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_dasat.htm

AAA Per-User Scalability

The AAA Per-User Scalability feature allows you to configure locally or remotely defined customer templates:

- Locally defined customer templates are defined per VPN with customer definitions. The customer template is stored locally on the VHG. This method can be used to associate a remote user with a specific VPN based on the domain name or dialed number identification service (DNIS) and provide the VPN-specific configuration for virtual access interface and all operational parameters for the customer AAA server.
- Remotely defined customer templates are defined per VPN with customer definitions that are stored on the service provider AAA server in a RADIUS profile. This method is used to associate a remote user with a specific VPN based on the domain name or DNIS and provide the VPN-specific configuration for the virtual access interface and all operational parameters for the AAA server of the customer.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

AAA-PPP-VPDN Non-Blocking

The AAA-PPP-VPDN Non-Blocking feature changes the software architecture such that the number of processes do not limit the rate of call handling. Previously, Cisco IOS software created a statically configurable number of processes to authenticate calls. Each process would handle a single call, but in some situations the limited number of processes could not keep up with the incoming call rate. This resulted in some calls timing out.

Any Transport over MPLS (AToM): Frame Relay over MPLS (FRoMPLS)

The Frame Relay over MPLS feature encapsulates Frame Relay protocol data units (PDUs) in Multiprotocol Label Switching (MPLS) packets and forwards them across the MPLS network. For Frame Relay, you can set up data-link connection identifier (DLCI)-to-DLCI connections or port-to-port connections.

- With DLCI-to-DLCI connections, the PE routers manipulate the packet by removing headers, adding labels, and copying control word elements from the header to the PDU.
- With port-to-port connections, you use high-level data link control (HDLC) mode to transport the Frame Relay encapsulated packets. In HDLC mode, the whole HDLC packet is transported. Only the HDLC flags and FCS bits are removed. The contents of the packet are not used or changed, including the FECN, BECN, and DE bits.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fsatom28.htm

ATM Features

Cisco IOS Release 12.2(28)SB introduces support for the following ATM features.

ATM Conditional Debug Support

The ATM Conditional Debug Support feature allows debugging to be limited specifically to an ATM interface, to a virtual channel identifier (VCI), or to a virtual path identifier/virtual channel identifier (VPI/VCI) pair, through use of the debug condition interface command. Most ATM debugging commands are implemented either at the system level or at the interface level.

For detailed information about this feature (which is also known as the ATM Conditional debug/show Commands feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/12satmdb.htm

ATM Multilink PPP Support on Multiple VCs

The ATM Multilink PPP Support on Multiple VCs feature supports the transport of real-time (voice) and other (data) traffic on Frame Relay and ATM virtual circuits (VCs).

This feature facilitates traffic load balancing on high-speed virtual circuits, using the Multilink Point-to-Point Protocol (MLP) over Frame Relay and ATM. It facilitates traffic load balancing by using MLP to combine packet datagrams on high-speed VCs, as a means for transporting both the voice and data traffic more efficiently.

Load balancing operates at Layer 2 or Layer 3 (the network layer) of the Open System Interconnection (OSI) reference model. Layer 3 load balancing is independent of any link-layer technologies. The ATM Multilink Point-to-Point Protocol (PPP) Support on Multiple VCs feature implements load balancing at Layer 2 and depends on having MLP enabled at the link layer. The ATM MLP functionality keeps track of packet sequencing, and this functionality buffers any packets that arrive early. With this ability, ATM MLP preserves packet order across the entire bundle.

In addition to MLP, low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) are used to prioritize and differentiate the voice and data packets. LLQ and CBWFQ help to ensure that the voice and data traffic receive the proper quality of service (QoS) treatment (such the correct priority queue assignment) when the voice and data traffic are transmitted.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftatmmlt.htm

ATM OAM Ping

The ATM OAM Ping feature sends an ATM Operation, Administration, and Maintenance (OAM) packet to confirm the connectivity of a specific permanent virtual circuit (PVC). The status of the PVC is displayed when a response to the OAM packet is received. The ATM OAM Ping feature allows the network administrator to verify PVC integrity and facilitates ATM network troubleshooting.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/12atmpng.htm

ATM OAM Traffic Reduction

The ATM OAM Traffic Reduction feature is a mechanism for reducing overhead when using loopback cells for fault detection in bidirectional virtual circuits (VCs) over ATM.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/atmoam.htm

Attribute Screening for Access Requests

The Attribute Screening for Access Requests feature allows you to configure your network access server (NAS) to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The filters can be configured on the NAS, or they can be downloaded via downloadable vendor-specific attributes (VSAs) from the authentication, authorization, and accounting (AAA) server.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123b/123b3/gt_asfar.htm

Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPP over ATM (PPPoA)/PPP over Ethernet (PPPoE) autosense functionality by providing autosense support on MUX- and SNAP-encapsulated ATM permanent virtual circuits (PVCs). Before the introduction of this feature, PPPoA/PPPoE autosense was supported on SNAP-encapsulated ATM PVCs only.

PPPoA/PPPoE autosense enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/ftpauto2.htm

BGP Features

Cisco IOS Release 12.2(28)SB introduces support for the following Border Gateway Protocol (BGP) features.

BGP 4 MIB Support for per-Peer Received Routes

The BGP 4 MIB Support for per-Peer Received Routes feature introduces a new table in the CISCO-BGP4-MIB that provides the capability to query (by using Simple Network Management Protocol [SNMP] commands) for routes that are learned from individual Border Gateway Protocol (BGP) peers.

Before this new MIB table was introduced, a network operator could obtain the routes learned by a local BGP-speaking router by querying the local BGP speaker with an SNMP command (for example, the **snmpwalk** command). The network operator used the SNMP command to query the bgp4PathAttrTable of the CISCO-BGP4-MIB.

The routes that were returned from a bgp4PathAttrTable query were indexed in the following order:

- Prefix
- Prefix length
- Peer address

Because the bgp4PathAttrTable indexed the prefixes first, obtaining routes learned from individual BGP peers will required the network operator to "walk through" the complete bgp4PathAttrTable and filter out routes from the interested peer. A BGP Routing Information Base (RIB) could contain 10,000 or more routes, which made a manual "walk" operation impossible and automated walk operations very inefficient.

BGP 4 MIB Support for per-Peer Received Routes introduces a Cisco-specific enterprise extension to the CISCO-BGP4-MIB that defines a new table called the cbgpRouterTable. The cbgpRouterTable provides the same information as the bgp4PathAttrTable with the following two differences:

- Routes are indexed in the following order:
  - Peer address
  - Prefix
  - Prefix length

  The search criteria for SNMP queries of local routes are improved because peer addresses are indexed before prefixes. A search for routes that are learned from individual peers is improved with this enhancement because peer addresses are indexed before prefixes. A network operator will no longer need to search through potentially thousands of routes to obtain the learned routes of a local BGP RIB table.
- Support is added for multiprotocol BGP, Address Family Identifier (AFI), and Subsequent Address Family Identifier (SAFI) information. This information is added in the form of indexes to the cbgpRouterTable. The CISCO-BGP4-MIB can be queried for any combination of AFIs and SAFIs that are supported by the local BGP speaker.

For detailed information about this feature, which is also known as the BGP Received Routes MIB feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s21/sbgprmib.htm

BGP Convergence Optimization

The BGP Convergence Optimization feature introduces a new algorithm for update generation that reduces the time that is required for Border Gateway Protocol (BGP) convergence. Neighbor update messages are optimized before they are forwarded to neighbors. Updates are optimized and forwarded based on peer groups and per-individual neighbors. This enhancement improves BGP convergence, router boot time, and transient memory usage. This enhancement is not user configurable.

Note This feature is also known as BGP: Reduction in Transient Memory Usage.

BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links

The BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links feature provides support for mixed EIGRP MPLS VPN network topologies that contain back door routes.

Before EIGRP Site of Origin (SoO) BGP Cost Community support was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Back door links in an EIGRP MPLS VPN topology will be preferred by BGP if the back door link is learned first. (A back door link, or a route, is a connection that is configured outside of the VPN between a remote and main site. For example, a WAN leased line that connects a remote site to the corporate network).

The "pre-bestpath" point of insertion (POI) was introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The "pre-best path" POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fsbgpcce.htm#wp1027129

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 access lists. This enhancement increases the maximum number of autonomous system access lists that can be configured with the **ip as-path access-list** command from 199 to 500.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/ftiaaspa.htm

BGP Support for IP Prefix Import from a Global Table into a VRF Table

The BGP Support for IP Prefix Import from Global Table into a VRF Table feature introduces the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding instance (VRF) table using an import map. This feature extends the functionality of VRF import-map configuration to allow IPv4 prefixes to be imported into a VRF based on a standard community. Both IPv4 unicast and multicast prefixes are supported. No Multiprotocol Label Switching (MPLS) or route target (import/export) configuration is required.

IP prefixes are defined as match criteria for the import map through standard Cisco IOS filtering mechanisms. For example, an IP access-list, an IP prefix-list, or an IP as-path filter is created to define an IP prefix or IP prefix range, and then the prefix or prefixes are processed through a match clause in a route map. Prefixes that pass through the route map are imported into the specified VRF per the import map configuration.

This feature can be configured to support Black Hole Routing (BHR) or classify global traffic:

- BHR is a method that allows the administrator to block undesirable traffic, such as traffic from illegal sources or traffic generated by a Denial of Service (DoS) attack, by dynamically routing the traffic to a dead interface or to a host designed to collect information for investigation, mitigating the impact of the attack on the network. Prefixes are looked up, and packets that come from unauthorized sources are blackholed by the ASIC at line rate.
- You can classify global IP traffic based on physical location or class of service. Traffic is classified based on administration policy and then imported into different VRFs. On a college campus, for example, network traffic could be divided into an academic network and residence network traffic, a student network and faculty network, or a dedicated network for multicast traffic. After the traffic is divided along administration policy, routing decisions can be configured with the MPLS VPN—VRF Selection using Policy Based Routing or the MPLS VPN—VRF Selection Based on Source IP address features.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fs_bgivt.htm

Bridged 1483 Encapsulated Traffic over ATM SVCs

The Bridged RFC 1483 Encapsulated Traffic over ATM SVCs feature allows you to send bridged RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs).

Previously, bridged ATM interface support was limited to ATM PVCs. When an ATM interface was part of a bridge group, the bridged traffic could be passed only on the PVCs on that interface.

Because PVCs are statically configured along the entire path between the end systems, it would not be practical to route bridged encapsulated traffic over them when the user wants to configure the VCs dynamically and tear down the VCs when there is no traffic.

Unlike PVCs, SVCs need to be triggered by ongoing traffic and might be brought down after they have been idle for some time. The Bridged RFC 1483 Encapsulated Traffic over ATM SVCs feature allows for the SVC to be triggered if down, and pass the traffic on to the SVCs belonging to the bridged ATM interface.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbridge.htm

Byte-Based Weighted Random Early Detection

The Byte-Based Weighted Random Early Detection feature extends the functionality of WRED. In previous releases, you specified the WRED actions based on the number of packets. With the Byte-Based WRED, you can specify WRED actions based on the number of bytes

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsbyte.htm

CEF/dCEF - Cisco Express Forwarding

The Cisco Express Forwarding (CEF) feature is an advanced, Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/cefcon.htm

Configurable MAC Address for PPPoE

The Configurable MAC Address for PPPoE feature configures the Media Access Control (MAC address on ATM permanent virtual circuits (PVCs) in a broadband access (BBA) group to use a different MAC address for PPP over Ethernet over ATM (PPPoEoA).

Because the Cisco IOS aggregation routers use the interface MAC address as the source MAC address for all broadband aggregation protocols on that interface, this feature solves problems that may occur when both RBE and PPPoE are deployed on the same ATM interface.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gt_cmppp.htm

Define Interface Policy-Map AV Pairs AAA

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco Remote Authentication Dial-In User Service (RADIUS) vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xi7/123xiqos.htm

DHCP Features

Cisco IOS Release 12.2(28)SB introduces support for the following Dynamic Host Configuration Protocol (DHCP) features.

DHCP Address Allocation Using Option 82

The DHCP Address Allocation Using Option 82 feature allows the Cisco IOS DHCP server to allocate dynamic IP addresses based on the relay information option (option 82) information sent by the relay agent.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. Option 82 is organized as a single DHCP option that contains information known by the relay agent.

This feature is designed to allow the Cisco IOS DHCP server to use option 82 information to help determine which IP addresses to allocate to clients. The information sent via option 82 will be used to identify which port the DHCP request came in on. This feature does not parse out the individual suboptions contained within option 82. Rather, the address allocation is done by matching a configured pattern byte by byte.

The feature introduces a new DHCP class capability, which is a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcps.htm#wp1097363

DHCP Client Dynamic Subnet Allocation API

The DHCP Client Dynamic Subnet Allocation API feature is an application programming interface (API) that is called by the DHCP Server—On-Demand Address Pool Manager feature to obtain a subnet from or release a subnet to the source server using DHCP. This feature allows automated configuration of Layer 3 devices for simplified deployment.

DHCP—Configurable DHCP Client

The Configurable DHCP Client feature allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server. A DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address.

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 12—This option specifies the name of the client. The name may or may not be qualified with the local domain.
- Option 51—This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address.
- Option 55—This option allows the DHCP client to request certain options from the DHCP server. The **ip dhcp client request** command allows the system administrator to turn off some of the requested options, thus removing them from the request list.
- Option 60—This option allows the user to configure the vendor class identifier string to use in the DHCP interaction.

- Option 61—This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcpc.htm#

DHCP Lease Limit per ATM RBE Unnumbered Interface

The DHCP Lease Limit per ATM RBE Unnumbered Interface feature allows an Internet service provider (ISP) to globally limit the number of leases available to DHCP clients per household or connection. This lease limit can be configured on ATM routed bridge encapsulation (RBE) or serial unnumbered interfaces.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcpa.htm#wp1089642

DHCP Option 82 Support for Routed Bridge Encapsulation

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation (RBE) is used

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrbeo82.htm

DHCP Relay Subscriber Identifier Suboption

The DHCP Relay Subscriber Identifier Suboption feature enables an ISP to add a unique identifier to the subscriber-identifier suboption of the relay agent information option. Before the introduction of this feature, if a subscriber moved, each ISP had to be informed of the change and all ISPs had to reconfigure the DHCP settings for the affected customers at the same time. Even if the service was not changed, every move involved administrative changes in the ISP environment. With the introduction of this feature, if a subscriber moves from one Network Access Server to another, there is no need for a change in the configuration on the part of the DHCP server or ISP.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcpr.htm#wp1095816

DHCP Release and Renew CLI in EXEC Mode

The DHCP Release and Renew CLI in EXEC Mode feature provides the ability to perform two independent operations from the CLI: (1) immediately release a DHCP lease for a DHCP client, and (2) force a DHCP renewal of a lease for a DHCP client.

This functionality provides the following benefits:

- Eliminates the need to go into the configuration mode to reconfigure the router to release or renew a DHCP lease.
- Simplifies the release and renewal of a DHCP lease.
- Reduces the amount of time spent performing DHCP IP release and renewal configuration tasks.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcpc.htm#wp1066977

DHCP Server—Option to Ignore All BOOTP Requests

The DHCP Server—Option to Ignore All BOOTP Requests feature allows the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets.

This functionality is beneficial when there is a mix of BOOTP and DHCP clients in a network segment and there is a BOOTP server and a Cisco IOS DHCP server servicing the network segment. The BOOTP server is configured with static bindings for the BOOTP clients and the BOOTP clients are intended to obtain their addresses from the BOOTP server. However, because a DHCP server can also respond to a BOOTP request, an address offer may be made by the DHCP server causing the BOOTP clients to boot with the address from the DHCP server, instead of the address from the BOOTP server. Configuring the DHCP server to ignore BOOTP requests means that the BOOTP clients will receive address information from the BOOTP server and will not inadvertently accept an address from a DHCP server.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcps.htm#wp1101095

DHCP—Static Mapping

The DHCP—Static Mapping feature enables assignment of static IP addresses without creating numerous host pools with manual bindings by using a customer-created text file that the DHCP server reads. The benefit of this feature is that it eliminates the need for a long configuration file and reduces the space required in NVRAM to maintain address pools.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcps.htm#wp1114732

DHCP—Statically Configured Routes Using a DHCP Gateway

The DHCP—Statically Configured Routes Using a DHCP Gateway feature enables the configuration of static routes that point to an assigned DHCP next hop router. This behavior was not possible before the introduction of this feature because the gateway IP address is not known until after the DHCP address assignment. A static route could not be configured with the command-line interface (CLI) that used that DHCP-supplied address.

The static routes are installed in the routing table when the default gateway is assigned by the DHCP server. The routes remain in the routing table until the DHCP lease expires at which time the routes are removed.

When a DHCP client releases an address, the corresponding static route (the route configured with the **ip route** command) is automatically removed from the routing table. If the DHCP router option (option 3 of the DHCP packet) changes during the client renewal, the DHCP default gateway changes to the new IP address supplied in the renewal.

This feature is particularly useful for VPN deployments such as Dynamic Multipoint VPNs (DMVPNs), or when a non-physical interface like a multipoint generic routing encapsulation (mGRE) tunnel is configured on the router and certain traffic needs to be excluded from going to the tunnel interface.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcps.htm#wp1102927

DHCPv6 Prefix Delegation via AAA

The DHCP for IPv6 prefix delegation feature allows an Internet service provider (ISP) to automate the process of assigning prefixes to a customer for use within the customer's network. Prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE), using the DHCP for IPv6 prefix delegation option. Once the ISP has delegated prefixes to a customer, the customer may further subnet and assign prefixes to the links in the customer's network.

For more information, see the “Implementing DHCP for IPv6” module in the *Cisco IOS IPv6 Configuration Guide, Release 12.4*:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00806cbb2a.html

DHCPv6 Relay Agent

The DHCPv6 Relay Agent feature introduces support for a DHCP relay agent to relay messages between the client and the DHCP server. A client locates a DHCP server by using a reserved, link-scoped multicast address. Therefore, it is a requirement for direct communication between the client and the server that the client and the server be attached to the same link. However, in some situations in which ease of management, economy, or scalability is a concern, it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link. A DHCP relay agent, which may reside on the client’s link, is used to relay messages between the client and the server. DHCP relay agent operation is transparent to the client.

For more information, see the *Implementing DHCP for IPv6* chapter in the *Cisco IOS IPv6 Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6_dhcp.htm

Dialer CEF

The Dialer CEF feature introduces Cisco Express Forwarding (CEF) support for dialer interfaces. This feature allows packets to be Cisco Express Forwarding switched across dialer interfaces rather than being low-end switched (LES) or fast switched. Compared to fast switching, Cisco Express Forwarding switching support improves switching performance by decreasing CPU utilization and lowering the packet loss rate.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdlrcef.htm

DNS Spoofing

The DNS Spoofing feature is designed to allow a router to act as a proxy Domain Name System (DNS) server and "spoof" replies to any DNS queries using either the configured IP address in the i**p dns spoofing ip-address** command or the IP address of the incoming interface for the query. This feature is useful for devices where the interface toward the Internet service provider (ISP) is not up. Once the interface to the ISP is up, the router forwards DNS queries to the real DNS servers.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtdnsspf.htm

Dynamic DNS Support for Cisco IOS Software

The Dynamic DNS Support for Cisco IOS Software feature enables Cisco IOS software devices to perform Dynamic Domain Name System (DDNS) updates to ensure that an IP host DNS name is correctly associated with its IP address.

It provides two mechanisms to generate or perform DDNS: the IETF standard as defined by RFC 2136 and a generic HTTP using various DNS services. With this feature, you can define a list of hostnames and IP addresses that will receive updates, specify an update method, and specify a configuration for Dynamic Host Configuration Protocol (DHCP) triggered updates.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/gt_ddns.htm

Embedded Event Manager 2.1

The Embedded Event Manager EEM 2.1 feature introduces some new event detectors and actions, some new functionality to allow Embedded Event Manager (EEM) policies to be run manually, and the ability to run multiple concurrent policies. Support for Simple Network Management Protocol (SNMP) event detector rate-based events is provided as is the ability to create policies using Tool Command Language (TCL).

EEM is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any desired action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gteem21.htm

Entity/Environment Monitoring

The Entity/Environmental Monitoring feature (also known as the Cisco 7200 Router Enhanced Management feature) improves core network management areas such as inventory, asset and fault management, and expands the number of Management Information Bases (MIBs) included with the router for improved inventory management and monitoring capabilities.

Using the Cisco 7200 Router Enhanced Management feature, you can:

- Manage and monitor Cisco 7200 resources through an SNMP-based network management system (NMS)
- Use SNMP set and get commands to access information in Cisco 7200 router MIBs
- Reduce the amount of time and system resources required to perform functions such as inventory management and bulk data transfers

Other benefits include:

- A standards-based technology (SNMP) for monitoring faults and performance on the router
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3)
- Notification of faults, alarms, and conditions that might affect services
- The ability to aggregate fault and alarm information for multiple entities
- A way to access router information other than through the command line interface (CLI)

For detailed information about this feature, see the *Cisco 7200 Series Router MIB Specifications Guide*:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_technical_reference_book09186a00805fee4b.html

Extended NAS-Port-Type and NAS-Port Support

The Extended NAS-Port-Type and NAS-Port Support feature allows you to better identify what service type is taking place on specific ports with non-RADIUS RFC supported types. Identifying traffic based on service type gives you flexibility to use your own coding mechanism to track users or to track shared resources, such as Ethernet or ATM interfaces.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/rd_naspt.htm

Frame Relay Features

Cisco IOS Release 12.2(28)SB introduces support for the following Frame Relay features.

Frame Relay MIB Enhancements

The Frame Relay MIB Enhancements feature extends the Cisco Frame Relay MIB by adding MIB objects that monitor the following Frame Relay functionality:

- Frame Relay fragmentation
- Frame Relay-ATM Network Interworking (FRF.5)
- Frame Relay-ATM Service Interworking (FRF.8)
- Frame Relay switching
- Input and output rates of individual virtual circuits (VCs)

The Cisco Frame Relay MIB describes managed objects that let you monitor Frame Relay operations remotely by using Simple Network Management Protocol (SNMP).

The Frame Relay MIB Enhancements feature also modifies the load-interval command to let you configure the load interval per permanent virtual circuit (PVC). The load interval is the length of time for which data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability. Before the introduction of this feature, the load interval could be configured only for the interface.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm

Frame Relay—show and debug Command Enhancements

The Frame Relay show Command and debug Command Enhancements feature provides the ability to filter the output of certain Frame Relay show and debug commands on the basis of the interface and data-link connection identifier (DLCI). These enhancements facilitate network scalability and simplify network management and troubleshooting.

For detailed information about this feature, which is also known as the Frame Relay show Command and debug Command Enhancements feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/sbfrshow.htm

Frame Relay VC Bundling

The Frame Relay permanent virtual circuit (PVC) Bundling feature allows you to associate a group of Frame Relay PVCs with a single next-hop address. When Frame Relay PVC bundles are used with IP, packets are mapped to specific PVCs in the bundle on the basis of the precedence value or differentiated services code point (DSCP) settings in the type of service (ToS) field of the IP header. Each packet is treated differently according to the QoS configured for each PVC.

MPLS QoS support for Frame Relay PVC bundles extends Frame Relay PVC bundle functionality to support the mapping of Multiprotocol Label Switching (MPLS) packets to specific PVCs in the bundle. MPLS packets are mapped to PVCs according to the settings of the experimental (EXP) bits in the MPLS packet header.

For detailed information about this feature, see the *Frame Relay PVC Bundles with IP and MPLS QoS Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_frbnd.htm

Generic Routing Encapsulation (GRE) Tunnel Keepalive

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_gretk.htm

IGMP State Limit

The IGMP State Limit feature provides protection against denial of service attacks caused by IGMP packets. The new CLI introduced by this feature allows you to configure a limit on the number of IGMP states that results from IGMP, IGMP Version 3 lite, and URL Rendezvous Directory (URD) membership reports on a per-interface or global basis. Membership reports in excess of the configured limits will not be entered in the IGMP cache, and traffic for those excess membership reports will not be forwarded.

For more information, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

IGMPv3

IGMP Version 3 (IGMPv3) adds support in Cisco IOS software for source filtering, which enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. This membership information enables Cisco IOS software to forward traffic only from those sources from which receivers requested the traffic.

IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:

- INCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the INCLUDE list) from which it wants to receive traffic.
- EXCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the EXCLUDE list) from which it does not want to receive traffic. In other words, the host wants to receive traffic only from sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, like in the case of the Internet Standard Multicast (ISM) service model, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.

IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in Source Specific Multicast (SSM). For SSM to rely on IGMPv3, IGMPv3 must be available in last hop routers and host operating system network stacks, and be used by the applications running on those hosts.

For detailed information about this feature, see the *Customizing IGMP* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap10/mcbcigmp.htm

Improved show commands for MLP-ATM LFI

The Improved show commands for Multilink PPP over ATM Link Fragmentation and Interleaving feature enhances the output of the **show atm pvc**, **show multilink ppp**, and **show interfaces virtual-access** commands to display multilink PPP (MLP) over ATM link fragmentation and interleaving (LFI) information. This feature also introduces the **debug atm lfi** command, which can be used to display MLP over ATM LFI debugging information.

For detailed information about this feature, see the *Troubleshooting Enhancements for Multilink PPP over ATM Link Fragmentation and Interleaving* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gttrbmlp.htm

Intelligent Service Gateway (ISG) Features

Cisco IOS Release 12.2(28)SB introduces support for the following Intelligent Service Gateway (ISG) features on the Cisco 7200 series router:

- ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support

  ISG Option 82 Line ID - AAA Authorization Support enhances ISG automatic subscriber logon by providing support for authorization on the basis of the circuit-id and remote-id.

- ISG: Accounting: Postpaid

  ISG Postpaid Billing provides means to bill for account or service usage. ISG sends accounting start and stop records for sessions and services to an accounting server for postpaid billing. The accounting server interprets the records to generate bills.

- ISG: Accounting: Time-Based Prepaid

  ISG Prepaid Billing allows ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG also supports time-based prepaid billing.

- ISG: Accounting: Volume-Based Prepaid

  ISG Prepaid Billing support allows ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG also supports volume-based prepaid billing.

- ISG: Accounting: Per Session, Service & Flow

  ISG Per Session, Service & Flow uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server.

- ISG: Accounting: Tariff Switching

  Tariff Switching occurs when billing rates change at fixed times and sessions are active across the boundary at which the rates change. ISG provides accounting data to the billing server indicating the boundary. Tariff Switching can also be used between accounting methods, such as switching from prepaid billing to post paid billing.

- ISG: Flow Control: Flow Redirect

  ISG Layer 4 Redirect enables service providers to better control the user experience by allowing subscriber TCP or UDP packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be applied to individual subscriber sessions or flows.

- ISG: Flow Control: QoS Control: Dynamic Rate Limiting

  ISG QoS Control: Dynamic Rate Limiting changes the allowed bandwidth of a session or flow dynamically by applying rate-limiting policies.

- ISG: Instrumentation: Advanced Conditional Debugging

  ISG Advanced Conditional Debugging provides the ability to define various conditions for filtering debug output. Conditional debugging generates very specific and relevant information that can be used for session, flow, subscriber, and service diagnostics.

- ISG: Instrumentation: Session & Flow Monitoring (local and external)

  ISG Session & Flow Monitoring (local and external) provides a mechanism for continuously monitoring interface and CPU statistics. This feature introduces the **show interface monitor** and **show processes cpu monitor** commands, which display statistics that are updated at specified intervals.

- ISG: Network Interface: IP Routed, VRF Aware MPLS

  ISG supports several types of forwarding to connect subscriber sessions to networks. These connections can be to the Internet, corporate intranets, ISPs, or walled gardens for content delivery. ISG supports both routed and MPLS-enabled interfaces for network access.

- ISG: Network Interface: Tunneled (L2TP)

  ISG supports several types of forwarding to connect subscriber sessions to networks. These connections can be to Internet, corporate Intranets, ISPs or walled gardens for content delivery. ISG supports tunnelled interfaces to networks.

- ISG: Policy Control: Cisco Policy Language

  ISG control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies provide an intuitive and extensible framework, with a consistent set of CLI commands, for specifying system behavior. The ISG policy language is aligned with the Cisco Common Classification Policy Language (C3PL).

- ISG: Policy Control: DHCP Proxy

  ISG DHCP Proxy enables ISG to dynamically interact with DHCP and apply policies that influence the IP addresses that DHCP assigns to subscribers.

- ISG: Policy Control: Multidimensional Identity per Session

  ISG Multidimensional Identity per Session allow session policy to be applied iteratively as more elements of identity become available to the system.

- ISG: Policy Control: Policy: Domain Based (Auto-domain)

  ISG control policies manage the primary services and rules used to enforce particular contracts. Polices can be configured to interpret the domain as a request to activate the service associated with that domain name, allowing users to automatically receive services in accordance with the domain to which they are attempting to connect.

- ISG: Policy Control: Policy Server: CoA (QoS, L4 Redirect, User ACL, TimeOut)

  ISG CoA provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization.

- ISG: Policy Control: Policy Server: SSG-SESM Protocol

  ISG supports Cisco's proprietary protocol to communicate with the Subscriber Edge Services Manager (SESM) policy server.

- ISG: Policy Control: Policy: Triggers: Duration

  ISG control policies can be configured with time-based, volume-based, and duration-based policy triggers. Time-based triggers use an internal clock, allowing policies to be applied at specific times. Volume-based triggers are based on packet count; when the packet count reaches a specified value, the specified policy is applied. Duration-based triggers are based on an internal timer. Upon expiration of the timer, the specified policy is applied.

- ISG: Policy Control: Service Profiles

  ISG defines a service as a collection of policies that can be applied to any subscriber session. Services can be configured on the router or on an external AAA server.

- ISG: Policy Control: User Profiles

  ISG user profiles specify services and functionality that should be applied to ISG sessions for the specified subscriber. User profiles are defined on an external AAA server.

- ISG: Session: Auth: PBHK

  ISG Port-Bundle Host Key serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISG gateway and a range of ports. This mapping allows the portal to identify the ISG gateway from which the session originated.

- ISG: Session: Auth: Single Sign On

  ISG Single Sign-On eliminates the need to authenticate a session more than once when a subscriber has access to services provided by other devices in the administrative domain of the access or service provider.

- ISG: Session: Authentication

  ISG automatic subscriber logon enables another specified identifier to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

- ISG: Session: Creation: Interface IP Session: L2

  ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.

- ISG: Session: Creation: Interface IP Session: L3

  ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.

- ISG: Session: Creation: IP Session: Protocol Event (DHCP)

  Most ISG sessions are created upon detection of a data flow that cannot be affiliated with an already active session. An ISG can be configured to create an IP session upon receipt of the first DHCP DISCOVER packet received from a subscriber.

- ISG: Session: Creation: IP Session: Subnet & Source IP: L2

  The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.

- ISG: Session: Creation: IP Session: Subnet & Source IP: L3

  The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.

- ISG: Session: Creation: P2P Session (PPPoE, PPPoXoX)

  The ISG session is the primary context to which services and policies are associated across specific data flows. Point-to-Point (P2P) sessions are established through a signaling protocol. ISG handles many variants of P2P encapsulation, such as PPP, PPPoE, and PPPoA.

- ISG: Session: LifeCycle: Idle Timeout

  ISG Idle Timeout controls how long a connection can be idle before it is terminated.

- ISG: Session: LifeCycle: POD

  A policy server can use RADIUS Packet of Disconnect (POD) to manage the lifecycle of any ISG session. The primary role of the POD message is to terminate an ISG session. An ISG can be configured to interact with external policy servers.

- ISG: Session: VRF Transfer

  ISG sessions are associated with virtual routing and forwarding instances when routing is required for the network service. ISG VRF transfer provides means to dynamically switch an active session between virtual routing domains.

For detailed information about these features, see the *Cisco IOS Intelligent Service Gateway Configuration Guide* that is part of the *Cisco IOS ISG Configuration Library*:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cg/isg_lib/index.htm

IP Features

Cisco IOS Release 12.2(28)SB introduces support for the following IP features.

IPMROUTE-STD-MIB

The IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for IP multicast routing in a manner independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

The IPMROUTE-STD-MIB supports all the MIB objects of the IPMROUTE-MIB and also supports the following four new MIB objects:

- ipMRouteEntryCount
- ipMRouteHCOctets
- ipMRouteInterfaceHCInMcastOctets
- ipMRouteInterfaceHCOutMcastOctets

The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

IP Multicast Load Splitting Across Equal-Cost Paths

The IP Multicast Load Splitting Across Equal-Cost Paths feature provides two ways to split IP multicast traffic among equal-cost paths: native multicast load splitting and load splitting by the unicast routing protocol over a tunnel. Multicast traffic from different sources is load split across equal cost paths to take advantage of multiple paths through the network.

For detailed information about this feature, see the *Load Splitting IP Multicast* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/mcbsplit.htm

IP SLAs - LSP Health Monitor

The IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor feature provides the capability to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature is useful for determining network availability or testing network connectivity between Provider Edge (PE) routers in an MPLS VPN. Once configured, the LSP Health Monitor will automatically create and delete IP SLAs LSP ping or LSP traceroute operations based on network topology.

The LSP Health Monitor feature also allows you to perform multi-operation scheduling of IP SLAs operations and supports proactive threshold violation monitoring through SNMP trap notifications and syslog messages.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/sbchmon.htm

IPv6 Access Services: DHCPv6 Prefix Delegation

The DHCP for IPv6 prefix delegation feature can be used to manage link, subnet, and site addressing changes. DHCP for IPv6 can be used in environments to deliver stateful and stateless information:

- Stateful—Address assignment is centrally managed and clients must obtain configuration information not available through protocols such as address autoconfiguration and neighbor discovery.
- Stateless—Stateless configuration parameters do not require a server to maintain any dynamic state for individual clients, such as Domain Name System (DNS) server addresses and domain search list options.

Extensions to DHCP for IPv6 also enable prefix delegation, through which an Internet service provider (ISP) can automate the process of assigning prefixes to a customer for use within the customer's network. Prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE), using the DHCP for IPv6 prefix delegation option. Once the ISP has delegated prefixes to a customer, the customer may further subnet and assign prefixes to the links in the customer's network.

For more information, see the “Implementing DHCP for IPv6” module in the *Cisco IOS IPv6 Configuration Guide, Release 12.4*:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00806cbb2a.html

ISDN Backup in MPLS Core

The ISDN Backup in MPLS Core feature allows a backup ISDN link on a dialer interface to be brought up to restore network connectivity when a primary link is down in the Multiprotocol Label Switching (MPLS) core network. This feature ensures high availability of the link between two routers in the MPLS core by providing a backup mechanism.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtisdnbk.htm

L2TP and L2TPv3 Features

Cisco IOS Release 12.2(28)SB introduces support for the following L2TP and L2TPv3 features.

L2TP Congestion Avoidance

The L2TP Congestion Avoidance feature provides packet flow control and congestion avoidance by throttling Layer 2 Transport Protocol (L2TP) control messages as described in RFC 2661. Throttling L2TP control message packets prevents dropped sessions when the peer's input buffer overflows.

Before the introduction of the L2TP Congestion Avoidance feature, the window size used to send packets between the network access server (NAS) and the tunnel server was set to the value advertised by the peer endpoint and was never changed. Configuring the L2TP Congestion Avoidance feature allows the

L2TP packet window to be dynamically resized using a sliding window mechanism. The window size grows larger when packets are delivered successfully, and is reduced when dropped packets must be retransmitted.

L2TP congestion avoidance is useful in networks with a relatively high rate of calls being placed by either tunnel endpoint. L2TP congestion avoidance is also useful on highly scalable platforms, which supports a large number of simultaneous sessions.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2scca.htm

L2TP Disconnect Cause Information

The L2TP Disconnect Cause Information feature adds support for additional Layer 2 Tunnel Protocol (L2TP) disconnect error codes using attribute-value (AV) pair 46 as specified by RFC 3145. Prior to the introduction of this feature, L2TP hosts could not exchange PPP disconnect error codes.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtl2disc.htm

L2TP Extended Failover

The L2TP Extended Failover feature extends Layer 2 Tunneling Protocol (L2TP) failover to occur if, during tunnel establishment, a router receives a Stop Control Connection Notification (StopCCN) message from its peer, or during session establishment a router receives a Call Disconnect Notify (CDN) message from its peer. In either case, the router selects an alternate peer to contact. This action is in addition to the existing failover caused by excessive retransmission of Start Control Connection Reply (SCCRQ) messages that indicate there is no response from the peer.

The L2TP Extended Failover feature results in improved load distribution and prevents congestion at a tunnel terminator by allowing the busy tunnel terminator to inform the tunnel initiator that it should try an alternate tunnel terminator.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpef.htm

L2TP Redirect

The L2TP Redirect feature allows a tunnel server participating in Stack Group Bidding Protocol (SGBP) to send a redirect message to the network access server (NAS) if another tunnel server wins the bid for a Layer 2 Tunnel Protocol (L2TP) call.

In a traditional Multichassis Multilink PPP (MMP) deployment, the stack group tunnel servers use Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels to deliver Multilink PPP (MLP) links to the bundle owner. This architecture does not easily scale beyond a few routers per tunnel server stack, and inherently adds hops and latency variations between links in a bundle.

Enabling the L2TP Redirect feature increases the scalability of Multichassis Multilink PPP (MMP) deployments, load balances sessions across the stack group tunnel servers, and smooths traffic as all links in a multilink bundle experience the same delay and latency.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tpmr.htm

L2TP Security

The L2TP security feature allows the security features of IP Security (IPSec) to protect the Layer 2 Tunnel Protocol (L2TP) virtual private dialup network (VPDN) tunnel and the PPP sessions within the tunnel. Without L2TP security, only a one-time, optional mutual authentication is performed during tunnel setup, with no authentication of subsequent data packets or control messages.

The enhanced protection provided by L2TP security increases the integrity and confidentiality of tunneled PPP sessions. The security features of IPSec and Internet Key Exchange (IKE) include confidentiality, integrity checking, replay protection, authentication, and key management. Traditional routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP) will run transparently because a real PPP interface is associated with the secure tunnel.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbl2tsec.htm

L2TP Tunnel Connection Speed Labeling

The L2TP Tunnel Connection Speed Labeling feature introduces the ability to accept or deny a Layer 2 Tunneling Protocol (L2TP) session based on the allowed connection speed that is configured on the Cisco Access Registrar (AR) RADIUS server for that user. The administrator can configure an AR RADIUS server to authorize users based on their Service Level Agreement (SLA). Tunnel connection speed information is forwarded to the AR RADIUS server by default.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbclabel.htm

L2TPv3 Control Message Hashing

The L2TPv3 Control Message Hashing feature introduces a more robust authentication method than the older CHAP-style L2TP control channel method of authentication.

The principal difference between the L2TPv3 Control Message Hashing feature and CHAP-style L2TP control channel authentication is that, instead of computing the hash over selected contents of a received control message, the L2TPv3 Control Message Hashing feature uses the entire message in the hash. In addition, instead of including the hash digest in only the SCCRP and SCCCN messages, it includes it in all messages.

You may choose to enable both methods of authentication to ensure interoperability with peers that support only one of these methods of authentication, but this configuration will yield control of which authentication method is used to the peer PE router. Enabling both methods of authentication should be considered an interim solution to solve backward-compatibility issues during software upgrades.

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

L2TPv3 Control Message Rate Limiting

The L2TPv3 Control Message Rate Limiting feature introduces a means to counter the possibility of a denial-of-service attack on a router running L2TPv3. The L2TPv3 Control Message Rate Limiting feature limits the rate at which SCCRQ control packets arriving at the PE that terminates the L2TPv3 tunnel can be processed. SCCRQ control packets initiate the process of bringing up the L2TPv3 tunnel and require a large amount of the control plane resources of the PE router.

On distributed platforms, most control packet filtering occurs at the line card level, and the CPU of the RP is minimally impacted even in a worst-case denial-of-service attack scenario. This feature has minimal impact on the shared bus or switching fabric, which are typically the bottleneck of a router.

No configuration is required for the L2TPv3 Control Message Rate Limiting feature. This feature automatically runs in the background in supported releases.

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Protocol Demultiplexing for L2TPv3

The Protocol Demultiplexing for L2TPv3 feature introduces the ability to provide native IPv6 support by utilizing a specialized IPv6 network to offload IPv6 traffic from the IPv4 network. IPv6 traffic is transparently tunneled to the IPv6 network using L2TPv3 pseudowires without affecting the configuration of the CE routers. IPv4 traffic is routed as usual within the IPv4 network, maintaining the existing performance and reliability of the IPv4 network.

For detailed information about this feature, see the *Layer 2 Tunnel Protocol Version 3* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm

Layer 2 VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Layer 2 VPN features.

Layer 2 VPN: Syslog, SNMP Trap and Show Command Enhancements for AToM and L2TPv3

The Layer 2 VPN: Syslog, SNMP Trap and Show Command Enhancements for AToM and L2TPv3 feature introduces new and enhanced commands for managing and diagnosing problems with xconnect configurations.

The following commands were introduced:

- **show xconnect**—Displays xconnect-specific information, providing a sortable single point of reference for information about all xconnect configurations.
- **snmp-server enable traps l2tun pseudowire status**—Enables the sending of Simple Network Management Protocol (SNMP) notifications when a pseudowire changes state.
- **xconnect logging pseudowire status**—Enables syslog reporting of pseudowire status events.

The following commands were enhanced:

- **debug vpdn**—The output of this command was enhanced to include authentication failure messages.
- **show l2tun session**—The hostname keyword option was added, allowing the peer hostname to be displayed in the output.
- **show l2tun tunnel**—The authentication keyword option was added, allowing the display of global information about L2TP control channel authentication attribute-value pairs (AV pairs).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s31/l2tpv31s.htm#wp1365293

NSF/SSO: L2VPN Pseudowire Redundancy Support

The NSF/SSO—L2VPN Pseudowire Redundancy feature enables you to set up your network to detect a failure in the network and reroute the L2 service to another endpoint that can continue to provide service. This feature also functions in an nonstop forwarding (NSF) and stateful switchover (SSO) environment. The active pseudowire does not change after SSO.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sudosso.htm

Local AAA Server

The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_laas.htm

MLP LFI over ATM Configuration Scaling

The MLP LFI over ATM Configuration Scaling feature, also known as the Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits feature, supports the transport of real-time (voice) and non-real-time (data) traffic on lower-speed Frame Relay and ATM permanent virtual circuits (PVCs) without causing excessive delay of real-time traffic. (This feature does not support switched virtual circuits.)

This feature implements link fragmentation and interleaving (LFI) using multilink PPP (MLP) over Frame Relay and ATM. The feature enables delay-sensitive real-time packets and non-real-time packets to share the same link by fragmenting the long data packets into a sequence of smaller data packets (fragments). The fragments are then interleaved with the real-time packets. On the receiving side of the link, the fragments are reassembled, and the packets are reconstructed. This method of fragmenting and interleaving helps guarantee the appropriate quality of service (QoS) for the real-time traffic.

Without this feature, MLP supported packet fragmentation and interleaving at the bundle layer; however, it did not support interleaving on Frame Relay or ATM. This feature supports low-speed Frame Relay and ATM as well as Frame Relay/ATM interworking (FRF.8) and Frame Relay fragmentation (FRF.12).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbamlatm.htm

MPLS Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) and MPLS-related features.

MPLS-Aware NetFlow

Multiprotocol Label Switching (MPLS)-Aware NetFlow is an extension of the NetFlow accounting feature that provides highly granular traffic statistics for Cisco routers. MPLS-Aware NetFlow collects statistics on a per-flow basis just as NetFlow does.

MPLS-Aware NetFlow statistics can be used for detailed MPLS traffic studies and analysis that can provide information for a variety of purposes such as MPLS network management, network planning, and enterprise accounting.

A network administrator can turn on MPLS-Aware NetFlow inside an MPLS cloud on a subset of provider backbone (P) routers. These routers can export MPLS-Aware NetFlow data to an external NetFlow collection device for further processing and analysis or display NetFlow cache data on a router terminal.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sx_mnf.htm

MPLS Embedded Management—High Capacity Counter

As of Cisco IOS Release 12.2(28)SB, the MPLS IF MIB has a 64-bit structure to ensure that high-capacity loads can be handled.

MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV

The MPLS Embedded Management—LSP Ping/Traceroute and Any Transport over MPLS Virtual Circuit Connection Verification feature helps service providers monitor label switched paths (LSPs) and quickly isolate MPLS forwarding problems. As Multiprotocol Label Switching (MPLS) deployments increase and the traffic types they carry increase, this enhanced functionality is critical to service providers.

This feature can be used to detect when an LSP fails to deliver user traffic as follows:

- You can use MPLS LSP Ping to test LSP connectivity for IPv4 Label Distribution Protocol (LDP) prefixes, traffic engineering (TE) Forwarding Equivalence Classes (FECs), and AToM FECs.
- You can use MPLS LSP Traceroute to trace the LSPs for IPv4 LDP prefixes and TE tunnel FECs.
- You can use MPLS LSP Ping to test the Pseudo-Wire (PW) section of an AToM virtual circuit (VC).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/lsping28.htm

MPLS Label Distribution MIB: MPLS LDP Trap Enhancement

The **snmp-server enable traps mpls ldp** command allows notification messages to be generated and sent to a designated network management station (NMS) in the network to signal the occurrence of specific events within Cisco IOS.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm

MPLS Label Distribution Protocol (LDP)

The Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding along normally routed paths.

LDP is an IETF standards tracking protocol. From an historical and functional standpoint, LDP is a superset of the Cisco prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For those features that LDP and TDP share in common, the pattern of protocol exchanges between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of LDP, which supports both the LDP and TDP protocols, provides the means for transitioning an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The routing protocol that you select can be configured on a per-interface basis for directly connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, an LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

The primary benefit of LDP over the prestandard TDP protocol is that LDP increases the number of platforms on which MPLS interoperability can be achieved.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftldp13.htm

MPLS—Multilink PPP Support

The Multiprotocol Label Switching (MPLS)—Multilink PPP Support feature ensures that MPLS Layer 3 Virtual Private Networks (VPNs) with quality of service (QoS) can be enabled for bundled links. This feature supports MPLS over Multilink PPP (MLP) links in the edge (provider edge [PE]-to-customer edge [CE]) or in the MPLS core (PE-to-PE and PE-to-provider router [P]).

Service providers that use relatively low-speed links can use MLP to spread traffic across multiple low-speed links in their MPLS networks. Link fragmentation and interleaving (LFI) should be deployed in the CE-to-PE link for efficiency, where you use smaller link bandwidths (less than 768 kbps).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtmpmlp.htm

MPLS QoS—DiffServ Tunnel Mode Support

The MPLS DiffServ Tunnel Mode Support feature allows service providers to manage the quality of service (QoS) that a router will provide to a Multiprotocol Label Switching (MPLS) packet in an MPLS network. MPLS DiffServ Tunnel Mode Support conforms to the IETF draft standard for Uniform, Short Pipe, and Pipe modes. It also conforms to Cisco-defined extensions for scalable command line interface (CLI) management of those modes at customer edge, provider edge, and core routers.

The following features are supported on MPLS DiffServ Tunnel Mode:

- MPLS per-hop behavior (PHB) layer management.
- There is improved scalability of the MPLS layer management by control on managed customer edge (CE) routers.
- MPLS can "tunnel" a packet's QoS (that is, the QoS is transparent from edge to edge).
- The MPLS experimental (MPLS EXP) field can be marked differently and independently of the PHB marked in the IP Precedence or differentiated services code point (DSCP) field.

- There are three MPLS QoS tunneling modes for the operation and interaction between the DiffServ marking in the IP header and the DiffServ marking in the MPLS header: Pipe mode with an explicit NULL LSP, Short Pipe mode, and Uniform mode. Pipe mode with an explicit NULL LSP and Short Pipe mode allow an MPLS network to transparently tunnel the DiffServ marking of packets.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdtmode.htm

MPLS HA Features

Cisco IOS Release 12.2(28)SB introduces changes for the following Multiprotocol Label Switching (MPLS) High Availability (HA) features.

MPLS High Availability

The Multiprotocol Label Switching (MPLS) High Availability (HA) feature provides full nonstop forwarding (NSF) and stateful switchover (SSO) capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Networks (VPNs) features.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fshaov.htm

Command Changes in Relation to MPLS HA

For command changes in relation to the Multiprotocol Label Switching (MPLS) High Availability (HA) feature, see the following:

- Cisco Express Forwarding: Command Changes

  Cisco Express Forwarding provides a forwarding path and maintains a complete forwarding and adjacency table for both the software and hardware forwarding engines. The Cisco Express Forwarding command improvements enable Cisco Express Forwarding to work with the MPLS HA applications and the MFI infrastructure.

  For detailed information about these command changes, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fscefcmd.htm

- MPLS High Availability: Command Changes

  The MPLS control plane software has been enhanced to work in an High Availability environment. The changes made the control plane software more modular, which helps MPLS support newer applications. Some of the control plane software changes made MPLS more scalable and flexible.

  Changes to the MPLS Forwarding Infrastructure (MFI) and the Cisco Express Forwarding component introduced new commands and changed other existing commands. MFI replaced the Label Forwarding Information Base (LFIB) and is responsible for managing MPLS data structures used for forwarding.

  For detailed information about these command changes, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s25/fscmdha.htm

MPLS Traffic Engineering Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features:

MPLS DiffServ-Aware Traffic Engineering (DS-TE)

DiffServ-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a sub-pool, while the regular TE tunnel bandwidth is called the global pool. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For detailed information about this feature, see the *MPLS Traffic Engineering—DiffServ Aware* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/12s_dste.htm

MPLS Traffic Engineering (TE)

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fs23te.htm

MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels

The MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels feature provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsbandaj.htm

MPLS Traffic Engineering (TE)—Configurable Path Calculation Metric for Tunnels

The MPLS Traffic Engineering—Configurable Path Calculation Metric for Tunnels feature enables the user to control the metric used in path calculation for TE tunnels on a per-tunnel basis.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsmetric.htm

MPLS Traffic Engineering (TE)—Forwarding Adjacency

The MPLS TE Forwarding Adjacency feature allows a network administrator to handle a traffic engineering, label-switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm. A forwarding adjacency can be created between routers regardless of their location in the network. The routers can be located multiple hops from each other.B As a result, a TE tunnel is advertised as a link in an IGP network with the link's cost associated with it, and routers outside of the TE domain see the TE tunnel and use it to compute the shortest path for routing traffic throughout the network.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa_3.htm

MPLS Traffic Engineering (TE)—Interarea Tunnels

The MPLS Traffic Engineering—Interarea Tunnels feature allows you to establish Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunnels that span multiple Interior Gateway Protocol (IGP) areas and levels, removing the restriction that had required 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).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsiarea3.htm

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

The MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for an Multiprotocol Label Switching (MPLS) TE label-switched path (LSP).

The feature is enabled through the **ip explicit-path** command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands the **exclude-address** command for specifying addresses to exclude from the path.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaddexc.htm

MPLS Traffic Engineering (TE) MIB

The MPLS Traffic Engineering MIB feature enables the Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) traffic engineering management, as implemented in the MPLS traffic engineering MIB (MPLS TE MIB). The SNMP agent code operating in conjunction with the MPLS TE MIB enables a standardized, SNMP-based approach to be used in managing the MPLS traffic engineering features in Cisco IOS software.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS Traffic Engineering (TE)—Scalability Enhancements

The Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Scalability Enhancement feature improves scalability performance for large numbers of traffic engineering tunnels.

These improvements allow an increase in the number of TE tunnels a router can support when the router is configured as a tunnel headend. Additionally, when the router is configured as a tunnel midpoint, the enhancements reduce the time required to establish large numbers of TE tunnels.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fsscen.htm

MPLS Traffic Engineering (TE)—SNMP Notification Support

The MPLS Traffic Engineering —SNMP Notification Support feature enables the Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) traffic engineering management, as implemented in the MPLS traffic engineering MIB (MPLS TE MIB). The SNMP agent code operating in conjunction with the MPLS TE MIB enables a standardized, SNMP-based approach to be used in managing the MPLS traffic engineering features in Cisco IOS software.

For detailed information about this feature, see the *MPLS Traffic Engineering MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/temib2.htm

MPLS VPN Features

Cisco IOS Release 12.2(28)SB introduces support for the following Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) features.

MPLS VPN—Carrier Supporting Carrier

The Carrier Supporting Carrier feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbb2scsc.htm

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

The Carrier Supporting Carrier—IPv4 BGP Label Distribution feature enables you to configure your carrier supporting carrier network to enable Border Gateway Protocol (BGP) to transport routes and Multiprotocol Label Switching (MPLS) labels between the backbone carrier provider edge (PE) routers and the customer carrier customer edge (CE) routers. Previously you had to use Label Distribution Protocol (LDP) to carry the labels and an Internal Gateway Protocol (IGP) to carry the routes between PE and CE routers to achieve the same goal.

The benefits of using BGP to distribute IPv4 routes and MPLS label routes are that:

- BGP takes the place of an IGP and LDP in a VPN forwarding/routing instance (VRF) table. You can use BGP to distribute routes and MPLS labels. Using a single protocol instead of two simplifies the configuration and troubleshooting.

- BGP is the preferred routing protocol for connecting two ISPs, mainly because of its routing policies and ability to scale. ISPs commonly use BGP between two providers. This feature enables those ISPs to use BGP.

This feature is an extension of the Carrier Supporting Carrier feature.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbbcsc13.htm

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

The MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session feature provides a method to advertise explicit null in a BGP label session for a carrier-supporting-carrier (CSC) customer edge (CE) router.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsxnlbsp.htm

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

The MPLS VPN—Inter-AS—IPv4 BGP Label Distribution feature enables you to set up a Virtual Private Network (VPN) service provider network so that the autonomous system boundary routers (ASBRs) exchange IPv4 routes with Multiprotocol Label Switching (MPLS) labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPNv4 routes by using multihop, multiprotocol, External Border Gateway Protocol (EBGP). This configuration saves the ASBRs from having to store all the VPNv4 routes. Using the route reflectors to store the VPNv4 routes and forward them to the PE routers results in improved scalability.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbb_smlp.htm

MPLS VPN—Inter-Autonomous System Support

The inter-autonomous systems for MPLS VPNs feature provides 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. The autonomous systems' border edge routers use Exterior Border Gateway Protocol (EBGP) to exchange that information. Then, an interior gateway protocol (IGP) distributes the network layer information for VPN-IPv4 prefixes throughout each VPN and each autonomous system.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/interas.htm

MPLS VPN—MIB Support: MPLS VPN Trap Enhancement

The MPLS VPN Trap Enhancement introduces the cMplsNumVrfRouteMaxThreshCleared notification. This notification is generated and sent when the number of routes on a VRF attempts to exceed the maximum number of routes and then drops below the maximum number of routes.

For detailed information about this feature, see the *MPLS VPN—MIB Support* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s25/fsvnmb25.htm#wp1027129

MPLS VPN—VPN-Aware LDP MIB

The MPLS LDP MIB has been implemented to enable standard, SNMP-based network management of the label switching features in Cisco IOS. Providing this capability requires SNMP agent code to execute on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MPLS LDP MIB.

The SNMP agent embodies a layered structure that is compatible with Cisco IOS and presents a network administrative and management interface to the objects in the MPLS LDP MIB and, thence, to the rich set of label switching capabilities supported by Cisco IOS.

By means of an SNMP agent, you can access MPLS LDP MIB objects using standard SNMP get operations to accomplish a variety of network management tasks. All the objects in the MPLS LDP MIB follow the conventions defined in the Internet Engineering Task Force (IETF) draft MIB entitled draft-ietf-mpls-ldp-mib-08.txt, which defines network management objects in a structured and standardized manner. This draft MIB is continually evolving toward the status of a standard. Accordingly, the MPLS LDP MIB will be implemented in a manner that tracks the evolution of this IETF document.

For detailed information about this feature, see the *MPLS Label Distribution Protocol MIB* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm#wp1015327

Multicast-VPN: Multicast Support for MPLS VPN

The Multicast VPN—IP Multicast Support for MPLS VPNs feature allows a service provider to configure and support multicast traffic in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment. This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

For detailed information about this feature (which is also known as the Multicast VPN—IP Multicast Support for MPLS VPNs feature), see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbb_mvpn.htm

MQC Policy Map Support on Configured VC Range

The MQC Policy Map Support on Configured VC Range feature extends policy map functionality to simplify the configuration of ranges of ATM VCs. Using the **service-policy** command, this feature allows you to apply a QoS service policy to a range of VCs.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/28sbvrng.htm

Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support

The Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support feature allows you to specify the criterion used to activate or deactivate a Frame Relay bundle. Consistent with the Frame Relay Forum Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16.1), bandwidth classes A (single link), B (all links), and C (threshold) are supported.

For detailed information about this feature, see the *Multilink Frame Relay (FRF.16.1)* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mfr.htm

NetFlow MPLS Label Export

The NetFlow MPLS Label Export feature allows a label switch router (LSR) to collect and export Multiprotocol Label Switching (MPLS) labels allocated by the LSR when an adjacent router pushes that label on the top of the label stack of a transit packet. At the same time, the LSR collects the prefix associated with the MPLS label and the application that allocated the label. The router collects the information in a table called the MPLS Prefix/Application/Label (PAL) table and exports this data to a NetFlow collector as the label is allocated or, if so configured, periodically exports the full MPLS PAL table.

You can use this information to create a provider edge (PE)-to-PE matrix, which is useful for network traffic planning and billing. To realize this benefit, you must export the MPLS label information to a NetFlow collector for analysis. This feature also provides information that a NetFlow collector can use to create a Virtual Private Network (VPN) routing and forwarding instance (VRF)-to-PE and PE-to-VRF matrix.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sx_pal.htm

Nonstop Forwarding and Stateful Switchover Features

Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature in Cisco IOS software to continue forwarding IP packets following a route processor (RP) switchover. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover.

Cisco 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 Cisco 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 Cisco NSF operation.

For detailed information about this feature, see the *Cisco Nonstop Forwarding* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s20/fsnsf20s.htm

Offload Server Accounting Enhancement

The Offload Server Accounting Enhancement feature allows users to configure their network access servers (NAS) to synchronize authentication and accounting information—NAS-IP-Address (attribute 4) and Class (attribute 25)—with the offload server.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftoffact.htm

Packet Classification Using the Frame Relay DLCI Number

The Packet Classification Using the Frame Relay DLCI Number feature allows customers to match and classify traffic based on the Frame Relay data-link connection identifier (DLCI) number associated with a packet. This new match criterion is in addition to the other match criteria, such as the IP precedence, differentiated service code point (DSCP) value, class of service (CoS), currently available.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/ftdlc26i.htm

peer pool backup Command

The Peer Pool Backup feature provides control over selection of IP address pools in large-scale dial-out networks where authentication, authorization, and accounting (AAA) servers and network access servers (NASs) are controlled by different groups. This feature allows you to define alternate sources for IP address pools in the event the original address pool is not present or is exhausted.

For detailed information about this feature, see the *Peer Pool Backup* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpeerpl.htm

PIM Multicast Scalability

The PIM Multicast Scalability feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Policer Enhancement: Multiple Actions

The Policer Enhancement: Multiple Actions feature extends the functionality of the Cisco IOS Traffic Policing feature (a single-rate policer) and the Two-Rate Policer feature. The Traffic Policing and Two-Rate Policer features are traffic policing mechanisms that allow you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as either conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the packet based on that marking.

With both the Traffic Policing feature and the Two-Rate Policer feature, you can specify only one conform action, one exceed action, and one violate action. With the Policer Enhancement: Multiple Actions feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsmu26s.htm

PPP MLP MRRU Negotiation Configuration

The PPP/MLP MRRU Negotiation Configuration feature allows a router to send and receive frames over Multilink PPP (MLP) bundles that are larger than the default Maximum Receive Reconstructed Unit (MRRU) limit of 1524 bytes.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtmpmrru.htm

PPPoE Features

Cisco IOS Release 12.2(28)SB introduces support for the following PPP over Ethernet (PPPoE) features.

PPPoE Circuit-ID Tag Processing

The PPPoE Circuit-Id Tag Processing feature provides a way to extract a Circuit-Id tag from the digital subscriber line (DSL) as an identifier for the authentication, authorization, and accounting (AAA) access request on an Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Ethernet instead. (In an Ethernet access network, there is no unique mapping between the subscriber line identifier and the interface such as there is on a virtual circuit (VC) in an ATM-based network.) The tag is useful for troubleshooting the network, and is also used in RADIUS authentication and accounting processes.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbecidtg.htm

PPPoE over Gigabit Ethernet Interface

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces.

PPPoE Relay

The PPPoE Relay feature enables an L2TP access concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP network server (LNS) or tunnel switch (multihop node). The relay functionality of this feature allows the LNS or tunnel switch to advertise the services it offers to the client, thereby providing end-to-end control of services between the LNS and a PPPoE client.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpppoer.htm

PPPoE Service Selection

The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. The customer chooses one of the services offered, and the service is provided when the PPPoE session becomes active. This feature enables service providers to offer a variety of services and to charge customers according to the service chosen.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpoess.htm

PPPoE Session Limit per NAS Port

The PPPoE Session Limit per NAS Port feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions on a specific permanent virtual circuit (PVC) or VLAN configured on an L2TP access concentrator (LAC). The network access server (NAS) port is either an ATM PVC or a configured VLAN ID. PPPoE per-NAS-port session limits are maintained in a RADIUS server customer profile database and are downloaded during Subscriber Service Switch (SSS) preauthorization.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_nas.htm

PPPoE Session Recovery After Reload

The PPPoE Session Recovery After Reload feature enables the aggregation device to attempt to recover PPPoE sessions that failed because of reload by notifying CPE devices about the PPPoE session failures. Previously, if the PPP keepalive mechanism was disabled on a customer premises equipment (CPE) device, a PPP over Ethernet (PPPoE) session would hang indefinitely after an aggregation device reload.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtppprec.htm

Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services

The Pseudowire Emulation Edge-to-Edge (PWE3) MIBs for Ethernet, Frame Relay (FR), and Asynchronous Transfer Mode (ATM) Services feature provides Simple Network Management Protocol (SNMP) support within an Any Transport over Multiprotocol Label Switching (AToM) infrastructure emulating Ethernet, Frame Relay, and ATM services over packet switched networks (PSNs). The PWE3 MIBs include the following:

- CISCO-IETF-PW-MIB (PW-MIB)
- CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB)
- CISCO-IETF-PW-ENET-MIB (PW-ENET-MIB)
- CISCO-IETF-PW-FR-MIB (PW-FR-MIB)
- CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbpweatm.htm

QoS Features

Cisco IOS Release 12.2(28)SB supports the following QoS features.

QoS: ATM Cell-Based Policer

The QoS: ATM Cell-Based Policer feature allows you to configure traffic policing for ATM cells. This feature allows you to specify traffic policing in cells, bytes, or percentage of bandwidth.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fscbp.htm

QoS: ATM-CLP and Layer 2 CoS-Based WRED

The QoS: ATM-CLP and Layer 2 CoS-Based WRED feature extends the functionality of the Cisco Weighted Random Early Detection (WRED) software. With the QoS: ATM-CLP and Layer 2 CoS-Based WRED feature, WRED can take into account the Layer 2 Class of Service (CoS) value of a packet and the ATM cell loss priority (CLP) of a packet when calculating the drop probability of network traffic.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swred.htm

QoS: CBQoSMIB Parity Across Cisco IOS Release 12.0S, 12.2SB, and 12.3T

The QoS: CBQoSMIB Parity Across Cisco IOS Release 12.0S, 12.2SB, and 12.3T feature adds several MIB objects to existing tables, and a new table to the Class-Based Quality of Service (QoS) MIB (CBQoSMIB). These additions to the CBQoSMIB provide parity of the MIB across three specific Cisco IOS Releases—Cisco IOS Release 12.0S, 12.2SB, and 12.3T. As a result of these additions and revisions, the CBQoSMIB now supports the same features across all three of these platforms.

The CBQoSMIB now supports the following Cisco IOS features:

- QoS: ATM Cell-Based Policer

  The QoS: ATM Cell-Based Policer feature allows you to configure traffic policing for ATM cells. This feature allows you to specify traffic policing in cells, bytes, or percentage of bandwidth.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fscbp.htm

- QoS: ATM-CLP and Layer 2 CoS-Based WRED

  The QoS: ATM-CLP and Layer 2 CoS-Based WRED feature extends the functionality of the Cisco Weighted Random Early Detection (WRED) software. With the QoS: ATM-CLP and Layer 2 CoS-Based WRED feature, WRED can take into account the Layer 2 class of service (CoS) value of a packet and the ATM cell loss priority (CLP) of a packet when calculating the drop probability of network traffic.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swred.htm

- QoS: Color-Aware Policer

  The QoS: Color-Aware Policer feature enables a “color-aware” method of traffic policing. This feature allows you to police traffic according to the color classification of a packet that is based on packet-matching criteria defined for two user-specified traffic classes: the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command, and the metering rates are defined using the **police** command.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

- Low Latency Queuing with Priority Percentage Support

  The Low Latency Queuing with Priority Percentage Support feature allows you to configure bandwidth as a percentage within low latency queuing (LLQ).

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12sllqpc.htm

- QoS: Percentage-Based Policing

  The QoS: Percentage-Based Policing feature allows you to configure traffic policing on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctpg.htm

- QoS: Percentage-Based Shaping

  The QoS: Percentage-Based Shaping feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctsg.htm

- QoS: Time-Based Thresholds for WRED and Queue Limit

  The QoS: Time-Based Thresholds for WRED and Queue Limit feature allows you to specify the Weighted Random Early Detection (WRED) minimum and maximum thresholds or the queue limit threshold in milliseconds (ms). Previously, these thresholds could only be specified in packets or bytes. Now, all three units of measure are available. Once the threshold limits are configured in a policy map, the policy map can be used on multiple interfaces, including those with different amounts of bandwidth.

  For more information about this feature, see the following Cisco document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12swrdql.htm

The following additional changes have been made to the MIB tables:

- One new table was added (cbQosSetStats), and objects were added to an existing table (chQosSetCFG). These tables are associated with the various **set** commands available in the Cisco IOS software.
- For more information about the Cisco IOS **set** commands, see the Cisco command reference publications for the Cisco IOS release that you are using.

For a list of the specific MIB objects added, see the CISCO-CLASS-BASED-QOS-MIB-CAPABILITY.html file at the following URL:

http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-CLASS-BASED-QOS-MIB-CAPABILITY

For more information about the preceding CBQoSMIB and the MIB objects and tables, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

QoS: Color-Aware Policer

The QoS: Color-Aware Policer feature enables a "color-aware" method of traffic policing. This feature allows you to police traffic according to the color classification of a packet that is based on packet-matching criteria defined for two user-specified traffic classes: the conform-color class and the exceed-color class. These two traffic classes are created using the **conform-color** command, and the metering rates are defined using the **police** command.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/12s_cap.htm

QoS: Frame Relay QoS Hierarchical Queueing Framework Support

The QoS: Frame Relay QoS Hierarchical Queueing Framework Support on the Cisco 7200 Series Router feature describes how Frame Relay (FR) works in Hierarchical Queueing Framework (HQF) to provide an FR service with fragmentation using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_frhqf.htm

QoS: Match on ATM CLP

The QoS: Match on ATM CLP feature allows you to match and classify packets arriving at an interface on the basis of the ATM cell loss priority (CLP) of the packet. With this new match criterion, you can further fine-tune packet classification and apply quality of service (QoS) features to a more select set of packets.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12smcatm.htm

QoS: Percentage-Based Policing

The QoS: Percentage-Based Policing feature allows you to configure traffic policing on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctpg.htm

QoS: Percentage-Based Shaping

The QoS: Percentage-Based Shaping feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spctsg.htm

QoS: Percentage-Based and Time-Based Policing Parameters

The QoS: Percentage-Based and Time-Based Policing feature allows you to configure traffic policing or shaping on the basis of a percentage of bandwidth available on the interface. Percentage-based and time-based options for the police policy map class configuration command are introduced as Modular Quality of Service Command Line Interface (MQC) commands so that you can reuse policy maps across different interfaces of different rates. This feature also allows you to specify the committed burst (bc) size and the extended burst (be) size used for configuring traffic policing in milliseconds (ms).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12spbtbp.htm

QoS: Per-Session Shaping and Queuing on LNS

The QoS: Per-Session Shaping and Queuing on LNS feature provides the ability to shape (for example, transmit or drop) or queue (for transmission later) the traffic going from an Internet service provider (ISP) to an ISP subscriber over Layer 2 Tunneling Protocol (L2TP) Network Server (LNS). With this feature, the outgoing traffic is shaped or queued on a per-session basis.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbsbpssq.htm

Additional QoS Features

Cisco IOS Release 12.2(28)SB also supports the following QoS features:

- Class-Based Marking

  Class-Based Packet Marking provides users with a user-friendly command-line interface (CLI) for efficient packet marking by which users can differentiate packets based on the designated markings.

- Class-Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)

  Class-Based Packet Marking allows users to perform the following tasks:

  - Mark packets by setting the IP Precedence bits or the IP differentiated services code point (DSCP) in the IP ToS byte.
  - Mark packets by setting the Layer 2 class of service (CoS) value.

- Class-Based Policing

  Class-Based Traffic Policing allows you to limit the input or output transmission rate of a class of traffic based on user-defined criteria

- Class-Based Shaping

  Class-Based Shaping provides the means for configuring Generic Traffic Shaping (GTS) on a class, rather than only on an access control list (ACL).

  Using the Class-Based Shaping feature, you can perform the following tasks:

  - Configure GTS on a traffic class
  - Specify average rate or peak rate traffic shaping
  - Configure Class-Based Weighted Fair Queuing (CBWFQ) inside GTS

- Class-Based Weighted Fair Queuing (CBWFQ)

  Class-Based WFQ (CBWFQ) extends the standard Weighted Fair Queuing (WFQ) functionality to provide support for user-defined traffic classes, and allows you to specify the exact amount of bandwidth to be allocated for a specific class of traffic. Taking into account available bandwidth on the interface, you can configure up to 64 classes and control distribution among them.

- DiffServ Compliant WRED

  DiffServ Compliant WRED extends the functionality of Weighted Random Early Detection (WRED) to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). This feature enables customers to implement AF PHB by coloring packets according to DSCP values and then assigning preferential drop probabilities to those packets.

- Low Latency Queueing (LLQ)

  LLQ provides strict priority queueing on ATM VCs and serial interfaces. This feature allows you to configure the priority status for a class within CBWFQ, and is not limited to UDP port numbers, as is IP RTP Priority. LLQ and IP RTP Priority can be configured at the same time, but IP RTP Priority takes precedence.

  Additionally, the functionality of LLQ has been extended to allow you to specify the Committed Burst (Bc) size in LLQ and to change (or vary) the number of packets contained in the hold queue per-VC (on ATM adapters that support per-VC queueing).

- Low Latency Queueing (LLQ) for Frame Relay

  LLQ for Frame Relay provides strict Priority Queueing (PQ) for voice traffic and WFQs for other classes of traffic. Before the release of this feature, LLQ was available at the interface and ATM VC levels. It is now available at the Frame Relay VC level when Frame Relay Traffic Shaping is configured. Strict PQ improves QoS by allowing delay-sensitive traffic such as voice to be pulled from the queue and sent before other classes of traffic.

  LQ for Frame Relay allows you to define classes of traffic according to protocol, interface, or access lists. You can then assign characteristics to those classes, including priority, bandwidth, queue limit, and WRED.

- Modular QoS CLI (MQC)

  Modular CLI is a CLI structure that allows users to create traffic policies and attach these policies to interfaces.

- Priority Queueing (PQ)

  PQ ensures that important traffic gets the fastest handling at each point where PQ is used. PQ can flexibly prioritize according to network protocol (such as IP, IPX, or AppleTalk), incoming interface, packet size, source/destination address, and so on.

- QoS for Virtual Private Networks

  With the growing popularity of VPNs, the need to classify traffic within a traffic tunnel is gaining importance. QoS features have historically been unable to classify traffic within a tunnel. With the introduction of the QoS for VPNs feature, packets can now be classified before tunneling and encryption occur. The process of classifying features before tunneling and encryption is called preclassification.

- QoS Packet Marking

  Class-Based Packet Marking provides users with a means for efficient packet marking by which users can differentiate packets based on the local QoS group value with a packet.

- QoS Policy Propagation via Border Gateway Protocol (QPPB)

  Border Gateway Protocol (BGP) provides a powerful, scalable means of utilizing attributes, such as community values, to propagate destination-based packet classification policy throughout a large network via BGP routing updates. Packet classification policy can be propagated via BGP without writing and deploying complex access lists at each of a large number of routers. BGP ensures that return traffic to customers is handled as premium traffic by the network.

- Random Early Detection (RED)/Weighted RED (WRED)

  WRED, the Cisco implementation of Random Early Detection (RED), combines the capabilities of the RED algorithm with IP Precedence to provide preferential traffic handling for higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service. WRED is also RSVP-aware.

For information about these additional QoS features, see the *Cisco IOS Quality of Service Solutions Configuration Guide*.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

RADIUS Features

Cisco IOS Release 12.2(28)SB introduces support for the following RADIUS features.

Framed-Route in RADIUS Accounting

The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records. The Framed-Route information will be returned to the RADIUS server in the Accounting-Request packets. The Framed-Route information can be used to verify that a per-user route or routes have been applied for a particular static IP customer on the network access server (NAS).

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_fra22.htm

RADIUS NAS-IP-Address Configurability

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123b/123b3/gt_siara.htm

RADIUS Push for MOD CLI Policies

The Define Interface Policy-Map AV Pairs AAA feature allows two new Cisco VSAs to be installed on an ATM VC after a PPPoA or PPPoEoA session establishment. Using RADIUS, the "push" functionality of the feature allows you to modify an existing QoS profile (a policy map) applied to a session while that session remains active, thus allowing QoS policies to be applied as required without session reauthentication disruption. Specific events, including time-of-day, byte count, and user request, can signal the policy server to push a policy map onto a specific VC.

For detailed information about this feature, see the *Define Interface Policy-Map AV Pairs AAA* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xi7/123xiqos.htm

RADIUS Server Load Balancing

The RADIUS Server Load Balancing feature distributes authentication, authorization, and accounting (AAA) authentication and accounting transactions across servers in a server group. These servers can then share the transaction load, resulting in faster responses to incoming requests by optimally using available servers.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbrdldbl.htm

RADIUS Server Reorder on Failure

The RADIUS Server Reorder on Failure feature provides for failover to another server in the server group during periods of high load or when server failure occurs. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

By spreading the RADIUS transactions across multiple servers, authentication and accounting requests are serviced more quickly.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/gt_rsrof.htm

RADIUS Attributes

Cisco IOS Release 12.2(28)SB introduces support for the following RADIUS attributes.

RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

The RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level feature allows you to customize configurations for different RADIUS server groups. This flexibility allows customized network access server- (NAS-) port formats to be used instead of global formats.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/ra5f.htm

RSVP Refresh Reduction and Reliable Messaging

The RSVP Refresh Reduction and Reliable Messaging feature includes refresh reduction, which improves the scalability, latency, and reliability of Resource Reservation Protocol (RSVP) signaling to enhance network performance and message delivery.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fsrelmsg.htm

Secure Shell Version 2 Support

The Secure Shell Version 2 Support feature allows you to configure Secure Shell (SSH) Version 2 (SSHVersion1 support was implemented in an earlier Cisco IOS software release). SSH runs on top of a reliable transport layer, such as TCP or IP, and provides strong authentication and encryption capabilities. SSH supports logging onto another computer over a network, executing commands remotely, and moving files from one host to another.

For detailed information about this feature, including the Secure Shell SSH Version 2 Client Support feature, also known as the SSHv2 feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ssh2.htm

Sticky IP

The Sticky IP feature (also known as the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature) describes the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature. It includes information on the benefits of the new feature, supported platforms, and related documents.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/radattr8.htm

Subscriber Service Switch

The Subscriber Service Switch feature directs PPP between points using a Layer 2 subscriber policy. It also provides the following features for Internet service provides (ISPs):

- Flexible connection options for subscribers seeking available services
- Flexible number of subscribers
- Flexible definition of services

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbsss.htm

TCP MSS Adjustment

The TCP MSS Adjustment feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments in the SYN bit set, when PPP over Ethernet (PPPoE) is being used in the network. PPPoE truncates the Ethernet maximum transmission unit (MTU) 1492, and if the effective MTU on the hosts (PCs) is not changed, the router in between the host and the server can terminate the TCP sessions. The **ip tcp adjust-mss** command specifies the MSS value on the intermediate router of the SYN packets to avoid truncation.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_admss.htm

UDI - Unique Device Identifier

The Unique Device Identifier feature provides the ability to retrieve and display the Unique Device Identifier (UDI) information from any Cisco product that has electronically stored such identity information.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtpepudi.htm

Virtual Sub-Interface

The Virtual Sub-Interface feature (also known as the Configuration Enhancements for Broadband Scalability feature) reduces the amount of memory that is used per terminated PPP session by creating virtual access subinterfaces. This feature also introduces a command to determine if a virtual template is compatible with virtual access subinterfaces.

For detailed information about this feature, see the *Configuration Enhancements for Broadband Scalability* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftbbenh.htm

Virtual Template Interfaces Limit Expansion

The Virtual Template Interfaces Limit Expansion feature allows you to increase the maximum number of virtual template interfaces. Prior to this feature, the maximum number of virtual template interfaces allowed was only 25. This feature allows you to have up to 200 virtual template interfaces. A higher number of virtual template interfaces is required for configuring VPN routing and forwarding (VRF) applications when you want to associate each virtual private dialup network (VPDN) customer to a VRF.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sb_vtle.htm

VLAN ID Rewrite

The VLAN ID Rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

For detailed information about this feature, see the *Any Transport over MPLS* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/fsatom28.htm

VPDN Features

Cisco IOS Release 12.2(28)SB introduces support for the following VPDN features.

Accounting of VPDN Disconnect Cause

The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes that describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. In the past, when a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session failed or disconnected, the network access server (NAS) and Home GateWay (HGW) reported a very generic disconnect-cause code, such as “LOST CARRIER.” These generic codes did not provide enough detailed information for accounting and debugging purposes. These new disconnect-cause codes can be found in the “RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values” appendix of the *Cisco IOS Security Configuration Guide, Release 12.2*:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00801fd174.html

RFC-2867 Tunnel Accounting

The RFC-2867 RADIUS Tunnel Accounting feature introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

For detailed information about this feature, see the *RFC-2867 RADIUS Tunnel Accounting* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbradtac.htm

Shell-Based Authentication of VPDN Users

The Shell-Based Authentication of VPDN Users feature allows the network access server (NAS) and tunnel server to be configured to perform shell-based authentication of virtual private dialup network (VPDN) users. Shell-based authentication of VPDN users provides terminal services (shell login or exec login) for VPDN users to support rollout of wholesale dial networks. Authentication of users occurs via shell or exec login at the NAS before PPP starts and the tunnel is established.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbexvpnt.htm

Timer and Retry Enhancements for L2TP and L2F

The Timer and Retry Enhancements for L2TP and L2F feature introduces configurable control packet timers and retry counters for Layer 2 Transport Protocol (L2TP) and Layer 2 Forwarding (L2F) virtual private dialup network (VPDN) tunnels. Adjustments to these timers and counters allows you to configure the following parameters:

- The amount of time that a router will wait for a reply while establishing a VPDN tunnel.
- The number of times a router will try to contact a peer.
- The amount of time that a router will wait before trying to contact an alternate VPDN peer.

These customizable timers and counters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbretreh.htm

Tunnel Authentication via Radius on LNS

The Tunnel Authentication via RADIUS on LNS feature allows a Layer 2 Tunnel Protocol (L2TP) Network Server (LNS) to perform remote authentication and authorization with RADIUS on incoming L2TP network access server (NAS) dial-in connection requests. This feature also allows the L2TP NAS to perform remote authentication and authorization with RADIUS on incoming L2TP tunnel server dial-out connection requests.

Without this functionality, the tunnel terminator can perform L2TP authentication only locally. Local authentication requires that data about the corresponding tunnel endpoint be configured within a VPDN group. This mechanism does not scale well because the information stored in the VPDN groups on each device must be updated independently.

Remote RADIUS authentication allows you to store configurations on the RADIUS server, avoiding the need to store information locally. New information can be added to the RADIUS server as needed, and a group of tunnel terminators can access a common database on the RADIUS server.

For detailed information about this feature, see the *Tunnel Authentication via RADIUS on Tunnel Terminator* document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbtunaut.htm

VPDN Default Group Template

The VPDN Default Group Template feature allows a virtual private dialup network (VPDN) template to be configured with global default values that will supersede the system default values. These global default values are applied to all associated VPDN groups, unless specific values are configured within an individual VPDN group.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbdevpdn.htm

VPDN Group Session Limiting

The VPDN Group Session Limiting feature allows you to configure a limit on the number of Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) virtual private dialup network (VPDN) sessions allowed for each VPDN group. Before the introduction of this feature, the number of VPDN sessions could be only globally controlled on the router, with limits applied equally to all VPDN groups.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbvpdngs.htm

VPDN Multihop by DNIS

The VPDN Multihop by DNIS feature allows dialed number identification service (DNIS)-based multihop capability in a virtual private dialup network (VPDN). This feature allows you to take advantage of the aggregation capability offered by multihop switching when users dial in to a network using a standard telephone line.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbvmhopd.htm

VPN MIB Enhancements for per-VRF Session Counting

The VPN MIB Enhancements for per-VRF Session Counting feature adds an extension to the virtual private dialup network (VPDN) CISCO-VPDN-MGMT-MIB that returns the total number of active sessions for each VPDN template. For customers that associate a VPDN template to each VPN routing and forwarding (VRF) instance, this MIB extension provides a way to monitor session usage per VRF.

Service providers can terminate sessions from multiple customer accounts on the same L2TP network server (LNS). Sharing of the LNS is done by creating one VRF per customer. Session limits on VPDN templates and VPDN groups are configured to control the allocation of sessions among customers and among users within the same customer account. A VPDN template is associated with each VRF, and its session limit restricts the total number of sessions for a customer account. Within that account, users may be assigned to different VPDN groups as their access requirements dictate. Session limits on VPDN groups further control the allocation of customer sessions among VPDN users. In such a setup, the service provider must use Simple Network Management Protocol (SNMP) to retrieve the total number of active sessions per customer to monitor their usage on the LNS.

Prior to the introduction of this MIB enhancement, only the total number of sessions on the LNS across all customer accounts could be retrieved through SNMP. This enhancement extends the CISCO-VPDN-MGMT-MIB to include a read-only table of VPDN template entries, with each entry reporting the number of active sessions across all VPDN groups that are associated with that template. The table entries can be accessed individually by using GET requests or consecutively using repeated GET-NEXT requests.

VPDN Session Disconnect AAA Attribute

The VPDN Session Disconnect AAA Attribute feature adds support for a new vendor-specific attribute (VSA) to be included in accounting stop records. The VSA provides information about the reason for the session disconnect and the identity of the device that initiated the disconnection. This feature includes support for the **accounting** keyword of the **vpdn-logging** command in Cisco IOS Release 12.2(28)SB, and is enabled by entering the **vpdn-logging accounting** command and keyword.

VRF-Aware VPDN Tunnels

The VRF-Aware VPDN Tunnels feature provides support for virtual private dialup network (VPDN) tunnels that terminate on a Virtual Private Network (VPN) routing and forwarding (VRF) instance. This feature allowing you to use IP addresses from a VRF routing table for the endpoints of a VPDN tunnel, rather than specifying IP addresses from the global routing table.

The VRF-Aware VPDN tunnels feature enhances the support of VPDN tunnels by allowing VPDN tunnels to start outside a Multiprotocol Label Switching (MPLS) VPN and terminate within the MPLS VPN. For example, this feature allows you to use a VRF address from a customer VRF as the destination address.

For detailed information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/sbvpdnmh.htm

Warm Reload

The Warm Reload feature enables you to reload your routers without reading images from storage. That is, the Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the image from flash to RAM or self-decompressing the image. Thus, the overall availability of your system improves because the time to reboot your router is significantly reduced.

For additional information about this feature, see the following Cisco document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtwrmrbt.htm

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(31c)XN3 and includes the following sections:

- Memory Recommendations, page 52
- Supported Hardware, page 54
- Feature Set Tables, page 54

Memory Recommendations

Warning **Unlike other network processing engines, the Cisco NPE-G2 has its own Cisco IOS software images with the prefix of "c7200p-" in the software image file names. All other network processing engines such as NPE-225, NPE-400 and NPE-G1 are compatible with images with the prefix of "c7200-." The Cisco NPE-G2 does not boot up with a software image with the prefix of "c7200-". Conversely, the other network processing engines such as NPE-225, NPE-400, and NPE-G1 do not boot up with the software image with the prefix of "c7200p-".**

Table 1 Image and Memory Recommendations for Cisco IOS Release 12.2(31c)XN3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	SBC Feature Set 4	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 2 Image and Memory Recommendations for Cisco IOS Release 12.2(31b)XN3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	SBC Feature Set 4	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 3 Image and Memory Recommendations for Cisco IOS Release 12.2(31a)XN3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	SBC Feature Set 4	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 4 Image and Memory Recommendations for Cisco IOS Release 12.2(31)XN3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	SBC Feature Set 4	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 5 Image and Memory Recommendations for Cisco IOS Release 12.2(31c)XN2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	Phase 2 Feature Set, Rebuild	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 6 Image and Memory Recommendations for Cisco IOS Release 12.2(31b)XN2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	Phase 2 Feature Set, Rebuild	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 7 Image and Memory Recommendations for Cisco IOS Release 12.2(31a)XN2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	Phase 2 Feature Set	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 8 Image and Memory Recommendations for Cisco IOS Release 12.2(31)XN2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	Phase 2 Feature Set	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 9 Image and Memory Recommendations for Cisco IOS Release 12.2(31)XN1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	QoS Feature Set	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Table 10 Image and Memory Recommendations for Cisco IOS Release 12.2(31)XN

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 VXR Router	SBC Feature Set	Cisco 7200 Series IOS IP SBC	c7200p-g9js-mz	64 MB Flash	1 GB DRAM	RAM

Supported Hardware

Cisco IOS Release 12.2(31c)XN3 supports the following Cisco 7000 series routers:

- Cisco 7200 VXR routers on the NPE-G2

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31c)XN3.

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31b)XN3.

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31a)XN3.

Table 11 lists the features and feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31)XN3:

Table 11 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN3

	Software Images by Feature Sets
Features	**c7200p-g9js-mz**
Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200	12.2(31)XN3
Coupled Pinholes (Hairpin)	12.2(31)XN3
Discarded Packets Statistic	12.2(31)XN3
Extension to H.248 Audit Support	12.2(31)XN3
H.248 Network Quality Alert Event	12.2(31)XN3

Table 11 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN3

Features	Software Images by Feature Sets
	c7200p-g9js-mz
H.248 Session Failure Reaction (SFR) Package	12.2(31)XN3
H.248 Termination State Control (TSC) Package	12.2(31)XN3
H.248 VLAN Package Syntax-Level Support	12.2(31)XN3
IP NAPT Traversal Support and Latch/Relatch Support (including full Relatch support)	12.2(31)XN3
IPv6 Support on SBC DBE Deployment: IPv6 Pinholes IPv6 No NAPT Support for Media Flows IPv6 Single NAPT for Signaling	12.2(31)XN3
Local Address Sharing	12.2(31)XN3
H.248 Traffic Management (Tman) Package Support (including Asymmetric Policing)	12.2(31)XN3

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31c)XN2.

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31b)XN2.

There are no new features or feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31a)XN2.

Table 12 lists the features and feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31)XN2:

Table 12 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN2

Features	Software Images by Feature Sets
	c7200p-g9js-mz
Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200	12.2(31)XN2
9-Tier Termination Name Hierarchy	12.2(31)XN2
DBE Signaling Pinhole Support	12.2(31)XN2
Extension to H.248 Termination Wildcarding Support	12.2(31)XN2
H.248 Ginfo Package Becomes Optional	12.2(31)XN2
H.248.1v3 Support	12.2(31)XN2
Interim Authentication Header Support	12.2(31)XN2
IP NAPT Traversal Support	12.2(31)XN2
MGC-Controlled Flow Policing	12.2(31)XN2
MGC-Controlled Gateway-Wide Properties	12.2(31)XN2
MGC Specified Local Addresses/Ports	12.2(31)XN2
Multi-Stream Terminations	12.2(31)XN2
Optional Local/Remote Descriptors	12.2(31)XN2

Table 12 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN2 (Continued)

Features	Software Images by Feature Sets
	c7200p-g9js-mz
Provisioned Inactivity Timer	12.2(31)XN2
Remote Source Address Mask Filtering	12.2(31)XN2
RTP Specific Behavior Support	12.2(31)XN2
Additional New Features	12.2(31)XN2
DHCPv6 Relay Agent Notification for Prefix Delegation	12.2(31)XN2
DHCPv6 Relay Options: Remote ID for Ethernet Interfaces	12.2(31)XN2
DHCPv6 Relay: Reload Persistent Interface-ID Option	12.2(31)XN2
IPv6 Multicast - MLD Group Limit	12.2(31)XN2
IPv6 Multicast Triggered RPF Check	12.2(31)XN2
PPPoE Session Limit Local Override	12.2(31)XN2
QoS: Bandwidth Remaining Ratio	12.2(31)XN2

Table 13 lists the features and feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31)XN1:

Table 13 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN1

Features	Software Images by Feature Sets
	c7200p-g9js-mz
QoS Deployment for the Cisco 7200	12.2(31)XN1
Disable VPDN Logging CLI Support	12.2(31)XN1
Equal Bandwidth Sharing (EBS)	12.2(31)XN1
IPv6 Support	12.2(31)XN1
Multi-Level Priority Queues (MPQ)	12.2(31)XN1

Table 14 lists the features and feature sets introduced by the Cisco 7200 VXR routers in Cisco IOS Release 12.2(31)XN:

Table 14 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN

Features	Software Images by Feature Sets
	c7200p-g9js-mz
Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200	12.2(31)XN
Bandwidth Allocation and CAC Functions	12.2(31)XN
Billing	12.2(31)XN
DBE Status Notification	12.2(31)XN
Firewall (Media Pinhole Control)	12.2(31)XN

Table 14 Feature List by Feature Set for Cisco IOS Release 12.2(31)XN (Continued)

Features	Software Images by Feature Sets
	c7200p-g9js-mz
Network Address and Port Translation (NAPT) and NAT/FW Traversal	12.2(31)XN
Policing and Marking (DSCP)	12.2(31)XN

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31c)XN3.

New Hardware Features in Cisco IOS Release 12.2(31c)XN3

There are no new hardware features supported in Cisco IOS Release 12.2(31c)XN3.

New Software Features in Cisco IOS Release 12.2(31c)XN3

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31c)XN3:

New Hardware Features in Cisco IOS Release 12.2(31b)XN3

There are no new hardware features supported in Cisco IOS Release 12.2(31b)XN3.

New Software Features in Cisco IOS Release 12.2(31b)XN3

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31b)XN3:

New Hardware Features in Cisco IOS Release 12.2(31a)XN3

There are no new hardware features supported in Cisco IOS Release 12.2(31a)XN3.

New Software Features in Cisco IOS Release 12.2(31a)XN3

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31a)XN3:

New Hardware Features in Cisco IOS Release 12.2(31)XN3

There are no new hardware features supported in Cisco IOS Release 12.2(31)XN3.

New Software Features in Cisco IOS Release 12.2(31)XN3

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31)XN3:

Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200

The following new SBC software features are supported by the data border element (DBE) function on the Cisco 7200 router for Cisco IOS Release 12.2(31)XN3.

See the *Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200* feature document for more information and detailed command information.

Coupled Pinholes (Hairpin)

The Coupled Pinholes (Hairpin) feature enhances the data border element (DBE) to support coupled pinholes for IPv4 and IPv6 packets. Pinhole is an informal term for a pair of terminations in the same stream and same context. Coupled pinholes are two pinholes on the DBE that the media gateway controller (MGC) has provisioned with local and remote addresses, whereby media from one pinhole should travel directly (loop back) to the other pinhole. The MGC (also known as a signaling border element (SBE)) does not differentiate whether ADD requests are sent to the same or different DBEs for a flow setup. A coupled pinhole pair is also called a hairpin.

This feature is useful for interoperation with SBEs that provision two pinholes, even in the case where the SBE does not require media to be sent further into the network. The DBE successfully forwards media on demand through IPv4 Twice NAPT pinholes that form coupled pairs. IPv6 NO-NAPT pinholes can form coupled pairs under certain circumstances.

Discarded Packets Statistic

The Discarded Packets Statistic feature uses the Gate Management package to report a new “GM Discarded Packets” statistic, which is counted and reported per termination.

The statistic reports the number of packets discarded by a termination due to the packet’s source address or port, and is reported in both the **show sbc dbe media-flow-stats** and **show sbc dbe signaling-flow-stats** command output.

Extension to H.248 Audit Support

The Extension to H.248 Audit Support feature enhances the data border element (DBE) to support auditing of the Signals, ObservedEvents, and EventBuffer descriptors in any of the **Add**, **Modify**, **Subtract**, or **AuditValue** commands at any time on both sides of a media flow.

H.248 Network Quality Alert Event

The H.248 Network Quality Alert Event feature introduces the **h248-media-alert-event** command, which is used to enable or disable Middlebox Pinhole Timer Expired event reporting when the data border element (DBE) detects media loss.

The Middlebox Pinhole Timer Expired event can be independently generated based on whether the media gateway controller (MGC) has requested or subscribed for this event.

H.248 Session Failure Reaction (sfr) Package

The H.248 Session Failure Reaction (sfr) package enables a media gateway controller (MGC) to instruct a media gateway (MG) to put a specified termination in the OutOfService state (either gracefully or forcefully) at the point where the H.248 association is lost. This feature is used to prevent signaling messages from reaching the call agent in the case of failure or administrative shutdown of MGC and MG communication.

H.248 Termination State Control (tsc) Package

The H.248 Termination State Control (tsc) package enhances the termination state capabilities of the media gateway controller (MGC). The tsc package contains the following two features:

- tsc-quiesce

  The tsc-quiesce feature allows the MGC to instruct the media gateway (MG) to set the ServiceState property of a signaling pinhole to OutofService state at the point where all associated (media) terminations are subtracted. The MG informs the MGC when this has occurred.

- tsc-suspend

  The tsc-suspend feature allows the MGC to put a signaling pinhole out of action for a given period of time. The MG informs the MGC when the signaling pinhole becomes operational again, and the MGC can query the time remaining until this happens.

A signaling pinhole is composed of two terminations. If either termination is out of service, the entire pinhole is out of service. It is up to the MGC whether to provision one or both terminations with the relevant properties. If the MGC chooses to provision only one termination, the MG does not impact the other termination.

H.248 VLAN Package Syntax-Level Support

The H.248 VLAN Package Syntax-Level Support feature enhances the data border element (DBE) to provide syntax-level support of the H.248 VLAN package. The media gateway controller (MGC) can program up to two VLAN tags and associated Ethernet priorities, as defined in the H.248 VLAN package. The DBE can accept, store, and return VLAN tag and priority information on a syntax level for media streams.

The VLAN tag and priority information is returned in the **show sbc dbe media-flow-stats** and **show sbc dbe signaling-flow-stats** command output.

IP NAPT Traversal Support and Latch/Relatch Support

In Cisco IOS Release 12.2(31)XN2, the IP NAPT Traversal Support feature was introduced to enhance data border element (DBE) functionality to support the IP NAT (Network Address Translator) Traversal package (ipnapt), defined in H.248.37. IP NAPT is an alternative method to the NAT Traversal package (ntr) defined in ETSI TS 102 333. IP NAPT defines two signals, latch and relatch, to control how the DBE learns remote addresses for endpoints behind a NAT.

With Cisco IOS Release 12.2(31)XN3, IP NAPT is further enhanced to provide full Relatch support.

IPv6 Support on SBC DBE Deployment

IPv6 Support on SBC DBE Deployment on the Cisco 7200 router includes the following features:

- DBE Support of IPv6 Pinholes

  DBE support of IPv6 pinholes for both media endpoints and signaling endpoints, includes the following functionality:

  - The data border element (DBE) supports forwarding of media from one IPv6 endpoint to another IPv6 endpoint.
  - The DBE supports IPv4 and IPv6 endpoints simultaneously. However, no interworking between IPv4 and IPv6 endpoints is supported. IPv4 endpoints can only forward media to other IPv4 endpoints and IPv6 endpoints can only forward media to other IPv6 endpoints.
  - The DBE supports configuration of IPv6 pinhole addresses and pinhole address pools.
  - The DBE supports signaling pinholes using IPv6 addresses.

- IPv6 No NAPT Support for Media Flows

  No NAPT support means that no IP addresses and ports are translated by the DBE from a private address to a public address (for multiple users to share a single public address). Media flows do not support Network Address and Port Translation (NAPT), thus they must be No NAPT. As a result, you cannot configure any media addresses under IPv6. Media flows may consist of only voice or video.

- IPv6 Single NAPT for Signaling

  Support of IPv6 signaling flows requires Single NAPT. With Single NAPT only one IP address and port is translated. In Single-NAPT processing, the flow on one side of the pinhole is programmed with a local address and port that do not belong to the signaling border element (SBC). Instead, that local address and port of the flow are specified by the media gateway controller (MGC) to match the remote address and port on the other side of the pinhole. Thus, incoming traffic (downstream traffic of the session initiation protocol (SIP) server to the access side) is addressed directly to the remote endpoint and the SIP server details are hidden from subscribers.

Local Address Sharing

The Local Address Sharing feature enhances the data border element (DBE) to allow multiple terminations to share a single local address and port as long as the terminations' Remote Source Address Masks (RSAMs) have the same mask length. A RSAM, also know as gm/sam, defines a remote subnet. The mask length is a property of the local address and port combination. Only multiple terminations that share the same local address and port are required to have the same RSAM mask length. Terminations with different local addresses or ports can have different RSAM lengths.

Note A termination can be described as a point of entry or exit of media flows relative to the DBE.

This enhancement allows call signaling from different subscribers to be routed to the media gateway controller (MGC) through different pinholes on the DBE. These different pinholes can share the same IP address and port on the subscriber side on the DBE, a typical scenario on the User-Network Interface, where it is simpler to publish a single IP and port to many subscribers.

H.248 Traffic Management (tman) Package Support

H.248 Traffic Management (tman) Package Support has been enhanced to allow the data border element (DBE) to support the sustained data rate (tman/sdr), maximum burst size (tman/mbs), and policing (tman/pol) properties of the ETSI TS 102 333 version 1.1.2 Traffic Management (tman) package. Support of these tman properties allows additional pinhole programming in the tman package to inform the DBE how to police media and signaling flows.

In Cisco IOS Release 12.2(31)XN2, the DBE supported symmetric flow policing; in Cisco IOS Release 12.2(31)XN3, the DBE has been enhanced to support asymmetric flow policing. The asymmetric flow policing enhancement allows the tman/pol property to be specified separately for the two sides of a gate, which typically are the access side and the back bone side. The tman/pol property can be specified as ON, OFF, or Absent on either the access side or the back bone side for either a media flow or signaling flow. Once tman/pol is specified as ON and both the tman/sdr and tman/mbs properties are present, the DBE polices traffic based on the values of the tman/sdr and tman/mbs parameters.

Note The tman/pdr and tman/dvt parameters are not supported in Cisco IOS Release 12.2(31)XN3.

New Hardware Features in Cisco IOS Release 12.2(31c)XN2

There are no new hardware features supported in Cisco IOS Release 12.2(31c)XN2.

New Software Features in Cisco IOS Release 12.2(31c)XN2

There are no new software features supported in Cisco IOS Release 12.2(31c)XN2.

New Hardware Features in Cisco IOS Release 12.2(31b)XN2

There are no new hardware features supported in Cisco IOS Release 12.2(31b)XN2.

New Software Features in Cisco IOS Release 12.2(31b)XN2

There are no new software features supported in Cisco IOS Release 12.2(31b)XN2.

New Hardware Features in Cisco IOS Release 12.2(31a)XN2

There are no new hardware features supported in Cisco IOS Release 12.2(31a)XN2.

New Software Features in Cisco IOS Release 12.2(31a)XN2

There are no new software features supported in Cisco IOS Release 12.2(31a)XN2.

New Hardware Features in Cisco IOS Release 12.2(31)XN2

There are no new hardware features supported in Cisco IOS Release 12.2(31)XN2.

New Software Features in Cisco IOS Release 12.2(31)XN2

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31)XN2:

Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200

The following new SBC software features are supported by the data border element (DBE) function on the Cisco 7200 router for Cisco IOS Release 12.2(31)XN2.

See the *Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200* feature document for more information and detailed command information.

9-Tier Termination Name Hierarchy

The 9-Tier Termination Name Hierarchy feature adds support for a 9-tier termination name schema, where the multi-tier prefix is supplied by the media gateway controller (MGC), and the final element, the channel ID, is generated by the media gateway (MG). Termination is the point of entry or exit of media flows relative to the MG. The MG understands how the flows entering and leaving each termination are related to each other. All MGCs that the MG is configured to contact must use the same termination name schema.

DBE Signaling Pinhole Support

The DBE Signaling Pinhole Support feature allows the media gateway controller (MGC) to directly control policing of signaling flows through the SBC interfaces on the data border element (DBE). The policing is at a per signaling flow level, via the H.248 association between the MGC and the DBE.

Without this feature, signaling packets are addressed to the SBE, and the DBE acts as a router, forwarding the packets to the SBE. With this feature enabled, the DBE can police signaling packets. The DBE has application-level pinholes created to allow those packets to be forwarded to the SBE. This feature removes the need to have a separate firewall device to protect the MGC.

Extension to H.248 Termination Wildcarding Support

The Extension to H.248 Termination Wildcarding Support feature adds support for partially wildcarded termination names, which allow a single command to replace one or more elements of a termination name with the wildcard character '*'.

The media gateway controller (MGC) can issue H.248 commands using wildcarding at any level of the 9-Tier Termination Name hierarchy. For example, any of the following wildcarded termination names would be valid:

```
ntt/sip/*/0/1023/0/*/*/*
ntt/sip/*/0/1023/0/4094/*/*
*/*/*/0/1023/0/*/*/*
```

H.248 Gate Information (ginfo) Package Becomes Optional

The H.248 Gate Information (ginfo) Package Becomes Optional feature removes the ginfo package properties as required in the data border element (DBE) H.248 profile. The DBE continues to support the ginfo package properties as optional properties and supplies default values if values are not specified.

H.248.1v3 Support

The H.248.1v3 Support feature allows the DBE to interoperate with an SBE that requires H.248.1 v3 or Media Gateway Controller (MGC) version 3. The DBE can accept H.248 version 2 through version 3. The DBE rejects attempts to negotiate with the MGC to a lower version once the DBE is configured to support version 3.

Interim Authentication Header Support

The Interim Authentication Header (IAH) Support feature is a protocol-level support that allows you to insert an IAH in the messages, and to set all fields in the IAH header to zeros. You are able to send and receive null IAH headers.

IP NAPT Traversal Support

The IP NAPT Traversal Support feature enhances data border element (DBE) functionality to support the IP NAT (Network Address Translator) Traversal (ipnapt) package, defined in H.248.37. IP NAPT is an alternative method to the existing support of NAT Traversal (ntr) package defined in ETSI TS 102 333. IP NAPT defines two signals, latch and relatch, to control how the DBE learns remote addresses for endpoints behind a NAT.

MGC-Controlled Flow Policing

The MGC-Controlled Flow Policing feature adds support for the sustained data rate (sdr), maximum burst size (mbs), and policing (pol) properties of the ETSI TS 102 333 version 1.1.2 Traffic Management (tman) package. MGC-Controlled Flow Policing allows additional pinhole programming in the tman package to inform the DBE how to police media and signaling flows.

MGC-Controlled Gateway-Wide Properties

The MGC-Controlled Gateway-Wide Properties feature adds support for all of the properties in Version 2 of the H.248 Base Root package as defined in H.248.1 v3.

This feature is subject to the following restriction:

The property field values are stored where set by H.248 and returned on subsequent audits. However, the property values are not used by the DBE and do not affect the DBE behavior.

MGC Specified Local Addresses/Ports

The MGC Specified Local Addresses/Ports feature allows a media gateway controller (MGC) to specify a local address or port for media and signaling flows through the data border element (DBE). The MGC specifies a specific address or port for terminations in H.248 add and modify requests, instead of using the “choose” wildcard.

Multi-Stream Terminations

The Multi-Stream Terminations feature allows a single H.248 termination to contain multiple streams. Previously, only a single stream for each termination was allowed.

Optional Local/Remote Descriptors

The Optional Local/Remote Descriptors feature allows the media gateway controller (MGC) to specify one or more local and remote descriptors in a modify command because the MGC does not always specify the descriptors in a single add command. A descriptor might be an address or port allocation or bandwidth reservation.

Provisioned Inactivity Timer

The Provisioned Inactivity Timer feature enhances data border element (DBE) functionality so that the DBE can be configured with a default value for the H.248 connection’s inactivity timer value (the it and ito properties). This default value is used if the media gateway controller (MGC) does not request that the DBE run an inactivity timer.

The advantage is that the DBE can detect MGC failure whether or not the MGC has subscribed to the inactivity timer event.

Remote Source Address Mask Filtering

The Remote Source Address Mask Filtering feature adds support for the Remote Source Address Filtering (saf) and Remote Source Address Mask (sam) properties of the ETSI TS 102 333 version 1.1.2 Gate Management (gm) package. The feature allows the media gateway controller (MGC) to program multiple terminations with the same local address and port, VPN ID, and transport protocol, as long as the multiple terminations are distinguished by their remote address and port or Remote Source Address Mask, and the local address is taken from an MGC-managed address range.

RTP Specific Behavior Support

The RTP Specific Behavior Support feature adds support for the real-time transport protocol (RTP) Specific Behavior (rsb) property of the ETSI TS 102 333 version 1.1.2 Gate Management (gm) package. This support allows the media gateway controller (MGC) to disable RTP specific behavior for a given

termination. In this case, the MGC overrides the default data border element (DBE) behavior for RTP flows. The result is that RTP traffic is not controlled through a single H.248 stream, representing both the RTP and RTCP flows.

DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCPv6 Relay Agent Notification for Prefix Delegation feature is used to insert and remove IPv6 routes from the routing table of a router working as a DHCPv6 relay agent. This feature inserts and removes IPv6 routes from the DHCPv6 relay agent by including the IPv6 route information in the prefix section of the DHCPv6 packet. The relay agent then extracts the information from the prefix of the DHCP packet when relaying the packet and adds the IPv6 route to its routing table.

See the *PXF Information for Cisco 7304 Routers* document for more information.

DHCPv6 Relay Options: Remote ID for Ethernet Interfaces

The DHCPv6 Relay Options: Remote ID for Ethernet Interfaces adds the Remote-ID option to relayed (RELAY-FORW) DHCPv6 messages for Ethernet interfaces.

The Remote-ID option provides information to the DHCPv6 server, including port information, the system's DHCP Unique Identifier (DUID) number, and the vlan-id. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem.

See the *PXF Information for Cisco 7304 Routers* document for more information.

DHCPv6 Relay: Reload Persistent Interface-ID Option

The DHCPv6 Relay: Reload Persistent Interface-ID Option feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a relay-reply message, persistent. A persistent interface-ID option will not change if the router acting as a relay agent goes offline (such as during a reload, power outage, and so on).

This feature makes the interface-ID option persistent by storing the interface-ID option at the DHCPv6 server. The DHCPv6 server than sends the interface-ID option to the relay agent in a reconfigure message when needed.

See the *PXF Information for Cisco 7304 Routers* document for more information.

IPv6 Multicast - MLD Group Limit

The IPv6 Multicast Listener Discovery (MLD) Group Limit feature provides protection against denial of service (DoS) attacks caused by MLD packets. Membership reports in excess of the configured limits will not be entered in the MLD cache, and traffic for those excess membership reports will not be forwarded.

MLD limits can be configured globally by using the **ipv6 mld state-limit ipv6** command, or per interface by using the **ipv6 mld limit** command. Both global and per-interface MLD limits can be configured on the same router. The global and per-interface MLD limits operate independently of each other.

See the *Cisco IOS IPv6 Configuration Guide* for more information about this feature, including configuration information.

IPv6 Multicast Triggered RPF Check

The IPv6 Multicast Triggered RPF Check feature sets the backoff intervals at which Protocol Independent Multicast (PIM) Reverse Path Forwarding (RPF) failover is triggered by changes in the routing tables.

See the *IPv6 Multicast Triggered RPF Check* feature module document for more information.

PPPoE Session Limit Local Override

The PPPoE Session Limit Local Override feature allows the locally configured per-port session limit to be applied before sending out a PPPoE Active Discovery Offer (PADO), even when PPPoE pre-authorization is enabled at BRAS. By enabling this feature, the locally configured session limit at BRAS overrides the session limit configured at RADIUS.

To enable this feature, the **sessions pre-auth limit ignore** command must be configured under the bba-group associated with the interface.

See the *PPPoE Session Limit Local Override* feature module document for more information.

QoS: Bandwidth Remaining Ratio

The QoS: Bandwidth Remaining Ratio feature allows service providers to prioritize subscriber traffic during periods of congestion. A bandwidth-remaining ratio is used to determine how the router allocates excess bandwidth (unused by priority traffic) to a class of non-priority traffic.

See the *QoS: Bandwidth Remaining Ratio* feature module document for more information.

New Hardware Features in Cisco IOS Release 12.2(31)XN1

There are no new hardware features supported in Cisco IOS Release 12.2(31)XN1.

New Software Features in Cisco IOS Release 12.3(31)XN1

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31)XN1:

Disable VPDN Logging CLI Support

The **no vpdn logging cause normal** and **no vpdn history failure cause normal** commands are supported on the Cisco 7200 routers in Cisco IOS Release 12.2(31)XN1.

The **no vpdn logging cause normal** command prevents display of the syslog message "VPDN-6-CLOSED" on the router console when a session terminates normally, so these messages do not overfill the log.

The **no vpdn history failure cause normal** command prevents the message "The remote server closed the session" from overwriting useful messages in the virtual private dialup network (VPDN) connection failure log when a session terminates normally, so these messages do not overfill the log.

See the *Disable VPDN Logging for Normal Session Termination* feature module document for more information.

Equal Bandwidth Sharing (EBS)

After priority traffic is served, the Equal Bandwidth Sharing feature provides for equal sharing of un-used interface bandwidth among all subscribers.

See the *Equal Bandwidth Sharing (EBS)* feature module document for more information.

IPv6 Support

QoS matching is performed only on the following subset of fields, which are common to IPv4 and IPv6:

- dscp/precedence
- access group (matches only on ACE entries common to IPv4 and IPv6)
- class
- qos group
- mpls
- input if
- l2 cos
- discard class

The **match protocol** command now includes the *ipv6* keyword to specify this protocol as a matching criterion. The **match ip dscp** and **match ip precedence** commands apply only to IPv4 traffic. The **match dscp** and **match precedence** commands apply to both IPv4 and IPv6 traffic.

For marking packets, the **set ip dscp** and **set ip precedence** commands have been changed to **set dscp** and **set precedence**. They now apply to both IPv4 and IPv6 traffic.

See the *Cisco IOS IPv6 Implementation Library* at the following location for information about how to configure and use IPv6 features on Cisco platforms:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00805766e4.html

Multi-Level Priority Queues (MPQ)

The Multi-Level Priority Queues (MPQ) feature allows you to configure multiple priority queues for multiple traffic classes by specifying a different priority level for each of the traffic classes in a single service policy map. You can configure multiple service policy maps per router. Having multiple priority queues enables the router to place delay-sensitive traffic (for example, voice) on the outbound link before delay-insensitive traffic. As a result, high priority traffic receives the lowest latency possible on the router.

See the *Multi-Level Priority Queues (MPQ)* feature module document for more information.

New Hardware Features in Cisco IOS Release 12.2(31)XN

There are no new hardware features supported in Cisco IOS Release 12.2(31)XN.

New Software Features in Cisco IOS Release 12.2(31)XN

The following new software features are supported by the Cisco 7200 VXR routers for Cisco IOS Release 12.2(31)XN:

Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200

Deployment of the data border element (DBE) function on the Cisco 7200 router integrates a subset of the session border controller (SBC) feature set with Cisco IOS for the Cisco 7200 router. A likely deployment scenario is that typical routing and broadband features are configured on the Cisco 7200 router serving as the DBE operating with a third-party vendor or external signaling border element (SBE). The SBC functionality on the Cisco 7200 router will eventually comprise both DBE and SBE functions, with DBE being the first to be deployed.

Cisco IOS Release 12.2(31)XN integrates the SBC DBE feature set on the Cisco 7200 under the SBC distributed model supporting session initiation protocol (SIP) and H.248 VoIP signaling protocol.

For the DBE on the Cisco 7200, a new interface type is defined for SBC virtual interface. Cisco IOS commands have been introduced in Cisco IOS Release 12.2(31)XN to create an SBC virtual interface and to configure the DBE.

The SBC feature set is platform independent. Cisco IOS images containing SBC software leverage existing IOS install and packaging facilities for software release, delivery, and installation.

See the *Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200* feature document for more information and detailed command information.

The DBE deployment supports the following IOS features:

Bandwidth Allocation and CAC Functions

The Bandwidth Allocation and CAC Functions feature allows the data border element (DBE) to support quality of service (QoS) bandwidth allocation (for Call Admission Control [CAC]). Call Admission Control is the set of actions taken by a network during the set-up phase of a call event to determine whether the event should be accepted or rejected.

The DBE can modify the bandwidth reservation. If the reservation request arrives from the signaling border element (SBE) through the control interface, the DBE indicates to the signaling border element (SBE) whether the reservation was successful or unsuccessful.

Billing

The Billing feature allows the data border element (DBE) to collect statistics data and send the data to the signaling border element (SBE).

DBE Status Notification

The DBE Status Notification feature allows the data border element (DBE) to notify the signaling border element (SBE) about critical status changes (for example, a resource shortage or performance degradation).

Firewall (Media Pinhole Control)

The Firewall (Media Pinhole Control) feature allows the signaling border element (SBE) Call Admission Control (CAC) function to inspect the signaling message and instruct the firewall in the data border element (DBE) to open and close pinholes as needed for the media streams (and possibly signaling).

Network Address and Port Translation (NAPT) and NAT/FW Traversal

The Network Address and Port Translation (NAPT) and NAT/FW Traversal feature allows the data border element (DBE) to perform translation of IP addresses and port numbers (using NAPT) in both directions and provides Network Address Translation (NAT) Traversal functions.

NAT converts an IP address from a private address to a public address in real time. It allows multiple users to share a single public IP address. The DBE can learn the NAT's public address and latch onto it for that flow.

Policing and Marking (DSCP)

The Policing and Marking (DSCP) feature allows the data border element (DBE) to support the rate limiter for ingress traffic, based on service level agreement (SLA). The DBE also supports re-marking of differentiated services code point (DSCP) bits for egress traffic and media relay.

Caveats for Cisco IOS Release 12.2 XN

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for Cisco IOS Release 12.2 XN.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og in** to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

Open Caveats—Cisco IOS Release 12.2(31c)XN3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31c)XN3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.2(31c)XN3.

Resolved Caveats—Cisco IOS Release 12.2(31c)XN3

Cisco IOS Release 12.2(31c)XN3 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31c)XN3, but may be open in previous Cisco IOS releases.

- CSCsj44980

  An IPv4 pinhole is shown with a /48 or /128 mask. Pinholes in the affected context cannot be modified or subtracted.

  This issue occurs when IPv4 and IPv6 pinholes are being repeatedly added and subtracted.

  Workaround: There are no known workarounds.

  Further Problem Description: This problem only occurs in the following scenarios:

  - When an internal IPv6 data structure is re-used for IPv4. The data structures are only re-used when each of them has been used at least once, and there are 20,000 in total, so the problem only occurs after at least 10,000 pinholes (that is, 20,000 terminations) have been added.
  - After an IPv6 pinhole with latching is deleted before it has time to latch.

- CSCsj88952

  The data border element (DBE) reloads when the DBE is processing an AuditValue that requires a response that is greater than 64 kilobytes. If DBE logging is enabled, the following message is displayed prior to the DBE hitting software forced reload:

  ```
  An internal consistency check has failed
  ```

  Workaround: There are no known workarounds.

- CSCsk01281

  The Real-time Transport Control Protocol (RTCP) policing rate is increased from 2 packets per second (pps) to 250 pps. Note that this increase can have a potential negative impact on performance if there is heavy RTCP traffic through a large number of terminations.

Open Caveats—Cisco IOS Release 12.2(31b)XN3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31b)XN3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.2(31b)XN3.

Resolved Caveats—Cisco IOS Release 12.2(31b)XN3

Cisco IOS Release 12.2(31b)XN3 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31b)XN3, but may be open in previous Cisco IOS releases.

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- CSCsg60220

  When global hccp is unconfigured and reconfigured, the snmp community string private disappears from the running configuration. As a result, you are unable to query any MIBs that use community string as private.

  Workaround: Reconfigure the snmp community string private.

- CSCsh54999

  A router may crash when the dynamic access control list (ACL) timer expires.

  This issue occurs on the router only when the **show access-list** command is entered before the timer expires.

  There are no known workarounds.

- CSCsh81510

  An IP Version 6 (IPv6) route that is automatically inserted by the Dynamic Host Configuration Protocol (DHCP) for IP version6 (DHCPv6) relay upon relaying a Prefix-Delegation packet is removed when the relay sees a Release packet that mentions the prefix delegated. No examination of the IAID and DUID is done to verify that the Release packet is coming from the appropriate client.

  There are no known workarounds.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsj22363

  An IP Version 6 (IPv6) static route that is automatically inserted by the Dynamic Host Configuration Protocol (DHCP) for IP version6 (DHCPv6) relay upon relaying a Prefix-Delegation packet to a client is not automatically re-inserted when the related interface goes down and comes back up.

  This issue occurs when **ipv6 address** xxx **linklocal** is configured under the subinterface.

  Workaround: Do not use an explicit ipv6 linklocal address.

Open Caveats—Cisco IOS Release 12.2(31a)XN3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31a)XN3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsj22363

  An IP Version 6 (IPv6) static route that is automatically inserted by the Dynamic Host Configuration Protocol (DHCP) for IP version 6 (DHCPv6) relay when relaying a Prefix-Delegation packet to a client, is not automatically re-inserted when the related interface goes down and comes back up.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(31a)XN3

Cisco IOS Release 12.2(31a)XN3 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31a)XN3, but may be open in previous Cisco IOS releases.

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi42334

  When the IP Version 6 (IPv6) **mld state limit** is configured or unconfigured, MLD assertion error messages are generated.

  There are no known workarounds.

- CSCsi52350

  When the data border element (DBE) returns an error message, the message is in long format; the message should be returned in the sort format.

  For example, the following message is returned in long format:

  ```
  MEGACO/3 [20.0.0.1]:2944 REPLY = 53480 {. ERROR = 442 { "An unsupported value was
  received" }.}
  ```
  This message should be returned in the following short format:

  ```
  !/3 [20.0.0.1]:2944 P = 53480 { ER = 442 { "An unsupported value was received" } }
  ```
  There are no known workarounds.

- CSCsj09546

  When a Transmission Control Protocol (TCP) packet is received with a checksum that equals 0x0000, the data border element (DBE) is not recalculating the checksum, but is instead processing this value as “no checksum”. As a result, the customer’s end device is dropping packets because of a checksum error.

  According to RFC standards, a 0x0000 checksum value should be processed as “no checksum” only for the User Datagram Protocol (UDP). For TCP packets, if the checksum value is 0x0000, and the source address, destination address, or port changes, then the checksum should be recalculated.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(31)XN3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31)XN3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg69458

  A Cisco 7200 series router does not purge multicast/unicast packets in the queue when the link goes down.

  This issue occurs on Gigabit Ethernet interfaces on the NPE-G2 when a link flaps (goes down) as a result of the cable being pulled. A burst of packets is observed coming out of the interface. This issue occurs even if the time duration for the down period is in the minutes range. If the payload has sequence numbers, note that these packets are a continuation of the last successfully received packet before link went down. This issue does not occur when the link is **shut/no shut** using CLI commands.

  There are no known workarounds.

- CSCsi41119

  The data border element (DBE) should reject a MODIFY request that includes E=1 {} when attempting to delete an event descriptor (qualert event). The correct format should be E.

  Workaround: Use the correct format of E to cancel the subscription.

Resolved Caveats—Cisco IOS Release 12.2(31)XN3

Cisco IOS Release 12.2(31)XN3 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31)XN3, but may be open in previous Cisco IOS releases.

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

- CSCsh01690

  A data border element (DBE) does not update the “No Media Count" value in the **show sbc global dbe media-stat** command.

  This issue occurs when one or more media flows time-out due to the absence of media.

  There are no known workarounds.

- CSCsh11904

  The **no local-port** command (the **no** form of the **local-port** command) provides the same functionality as the **use-any-local-port** command; to avoid confusion the **use-any-local port** command should be removed.

  There are no known workarounds.

- CSCsh58386

  If the incoming interface on a system being used as a DHCPv6 relay is configured with **ipv6 address autoconfig**, the DHCPv6 Prefix Delegation packets are not relayed because the incoming interface does not have a globally routable address. These packets should be relayed with a linkaddr address of 0::0.

  Workaround: Assign the interface a globally routable address.

- CSCsh62887

  When **ipv6 mld state-limit** is configured under global configuration, or **ipv6 mld limi**t is configured under interface configuration, the mroutes are deleted and reinstalled after a new query/response takes place. This behavior causes multicast traffic to be interrupted whenever the configuration is changed.

  There are no known workarounds.

- CSCsh66424

  When the Multicast Listener Discovery (MLD) limit is reached, no syslog is available.

  There are no known workarounds.

- CSCsh66700

  A data border element (DBE) does not perform latching after receiving a napt=latch/relatch in a MODIFY request.

  This issue occurs if napt=off when setting up a pinhole.

  There are no known workarounds.

- CSCsh75108

  When an out-of-port-range packet is sent in a single Network Address and Port Translation (NAPT) setup and a **show sbc global dbe forwarder-stats** command is issued, the packet displays as “Punted” in the Summary output, but displays under the “Dropped Packets” counter in the Detail output.

  This issue occurs when a packet is sent with an out-of-range destination port in the pinhole.

  There are no known workarounds.

- CSCsh77301

  The number of terminations collected by AuditValue is smaller than the value which has been set.

  This issue can occur during long hours of testing.

  There are no known workarounds.

- CSCsh79931

  When packets are sent to the same address, but a different port of a latched address/port, the packets are not routed as non-SBC traffic, but discarded by the data border element (DBE).

  This issue occurs on a signaling pinhole with a NO-NAPT setup that uses the Transmission Control Protocol (TCP) as transport.

  There are no known workarounds

- CSCsh80303

  ER=421 is reported when two calls are made in an IPv6 No-NAPT hairpin setup.

  There are no known workarounds.

- CSCsh88105

  Multiple terminations can now share the same local address for NO-NAPT in the case of interleaved Video on Demand (VoD) service.

  This is new enhancement for NTT; a workaround is not applicable.

- CSCsh88220

  The data border element (DBE) does not send a response to a request before creating a pinhole.

  This issue occurs when a wildcard AuditValue is requested before creating a pinhole.

  There are no known workarounds.

- CSCsi12475

  Real-Time Control Protocol (RTCP) packets are dropped by the data border element (DBE) for an IPv6 media pinhole.

  There are no known workarounds.

- CSCsi12512

  The data border element (DBE) reboots after a twelve-hour long duration test.

  There are no known workarounds.

- CSCsi16281

  The data border element (DBE) does not forward IPv4 traffic for both the media and signaling pinhole.

  There are no known workarounds.

- CSCsi16755

  The data border element (DBE) stop forwarding IPv6 Session Initiation Protocol (SIP) traffic after the Term state is changed from OS to IV.

  There are no known workarounds.

- CSCsi16742

  The data border element (DBE) reboots during a long duration test.

  There are no known workarounds.

- CSCsi17289

  The data border element (DBE) rejects a second hairpin pair with ER=510. The first pair is created, but the request for the second pair is rejected by the DBE.

  There are no known workarounds.

- CSCsi21493

  The session border controller (SBC) performed a core dump under a stress test with IPv6.

  There are no known workarounds.

- CSCsi39202

  When an IPv6 Multicast router configured with a global MLD limit is connected to MLD clients using subinterfaces, and leaves are sent in parallel on multiple subinterfaces followed by joins, certain joins are not accepted because of the time involved to remove the host from the MLD groups table.

  Workaround: Increase the global MLD limit value.

- CSCsi44091

  The data border element (DBE) crashes under long term testing.

  This issue occurs under the following conditions:

  - H.248 traffic for the pinholes
  - Call interval is 0.5 seconds with a call duration of 60 seconds
  - IPv4 background traffic of 720Mbps.
  - Traffic is sent for long durations

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(31c)XN2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31c)XN2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.2(31c)XN2.

Resolved Caveats—Cisco IOS Release 12.2(31c)XN2

Cisco IOS Release 12.2(31c)XN2 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31c)XN2, but may be open in previous Cisco IOS releases.

- CSCek51702

  The NPE-G2 crashes with a watchdog timeout after the occurrence of many SYS-3-CPUHOG messages.

  This issue only occurs on the NPE-G2, and is preceded by numerous messages on the console (generally debugs.)

  Workaround: There are three possible workarounds:

  1. Disable debugs, or
  2. Disable console logging, or
  3. Limit console logging to a minimum, or
  4. Enter the **no logging console guaranteed** command.

- CSCsg63466

  The **show int stat** and **show interface** command outputs display twice the number of packets dropped because of a Unicast Reverse Path Forwarding (uRPF) check failure in an IPv6 Multicast scenario.

  There are no known workarounds. Other than the reporting of incorrect statistics, this issue does not affect functionality.

- CSCsg80988

  The Dynamic Host Configuration Protocol (DHCP) for IP version 6 (DHCPv6) relay agent removes the inserted DHCP route from its routing table after 34 minutes.

  Workaround: Configure the DHCP allocated route manually as a static route on the relay agent.

- CSCsh12840

  The **ipv6 mld limit** command, which configures the IP Version 6 (IPv6) Multicast Listener Discovery (MLD) limit, doesn't work when the **ipv6 mld explicit tracking** command is configured on the same subinterface.

  For example, the configuration below will not work:

  ```
  interface GigabitEthernet0/1.100
  ipv6 mld explicit-tracking
  ipv6 mld limit 1
  ```

  Workaround: There is no workaround other than disabling the **ipv6 mld explicit tracking** command in the interface configuration.

- CSCsh49038

  A Cisco 7200 series router acting as a data border element (DBE) crashes during a port scan by an external application of the (media gateway controller) megaco port.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(31b)XN2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31b)XN2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.2(31b)XN2.

Resolved Caveats—Cisco IOS Release 12.2(31b)XN2

Cisco IOS Release 12.2(31b)XN2 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31b)XN2, but may be open in previous Cisco IOS releases.

- CSCsg75372

  The following message appears on the router console:

  ```
  *Aug 11 20:54:53 UTC: %QOS-3-HQFPOOLERR: interface GigabitEthernet0/1: failed to
  allocate hqf particle
  ```

  This issue occurs when the router is replicating a lot of multicast traffic and the cable connected to the Multicast Listener Discovery (MLD) Multicast clients is disconnected abruptly, or when the next hop router is rebooted.

Workaround: There are two known workaround for this issue:

1. Configure **keepalive 1** on the Gigabit Ethernet interface so that the router quickly brings down the line protocol.

2. Configure the following buffer tuning: **buffers particle-clone 4000**.

- CSCsg87235

  When Embedded Event Manager (EEM) is configured, Telnet connections fail under the following scenario: the device sends three quick "Username" prompts and then kills the connection, without providing the user the time to actually enter a username.

  This issue only occurs when EEM is configured.

  Workaround: Try the Telnet connection twice. The first time Telnet will fail for the above reason; the second time Telnet will work.

- CSCsh10876

  When there is no traffic passing through the signaling or media pinhole for more than 35 minutes, packets from the terminal are dropped due to incorrect rate limiting.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(31a)XN2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31a)XN2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no new open caveats for Cisco IOS Release 12.2(31a)XN2.

Resolved Caveats—Cisco IOS Release 12.2(31a)XN2

Cisco IOS Release 12.2(31a)XN2 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31a)XN2, but may be open in previous Cisco IOS releases.

- CSCsg34907

  The data border element (DBE) cannot set the tman/sdr rate limit higher than 1000 pps for incoming traffic. Even when the rate limit of outgoing traffic is set to a higher value and the incoming traffic flowing into the open gate is greater than that value, the DBE rate limit remains at 1000 pps.

  An enhancement in timer handling is needed to fix this problem.

  There are no known workarounds.

- CSCsg75011

  When one side has no Traffic management (Tman) parameters set, and the second side is set to TMAN=OFF, the media flow are being rate limited. According to Tman policy, the flow should not be rate limited.

  This issue only occurs on media flow; no problem occurs on signal flow.

  Workaround: Always specify TMAN as either TMAN=ON or TMAN=OFF.

Open Caveats—Cisco IOS Release 12.2(31)XN2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31)XN2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek51702

  The NPE-G2 crashes with a watchdog timeout after the occurrence of many SYS-3-CPUHOG messages.

  This issue only occurs on the NPE-G2, and is preceded by numerous messages on the console (generally debugs.)

  Workaround: There are three possible workarounds:

  1. Disable debugs, or

  2. Disable console logging, or

  3. Limit console logging to a minimum.

- CSCir00095

  The cbQosPoliceActionCfgConformSetValue, cbQosPoliceActionCfgExceedSetValue, and cbQosPoliceActionCfgViolateSetValue instances for the transmit action are missing in the QosPoliceActionCfgTable.

  This issue occurs when the "transmit" values configured under conform, exceed and violate actions for the **police** command.

  There are no known workarounds.

- CSCse85047

  Calling-Station-Id Attribute 31 is not sent to the authentication, authorization, and accounting (AAA) RADIUS server on L2TP network server (LNS) router in Accounting Start/Stop messages.

  This issue occurs when you bring up or tear down a Point-to-Point Protocol (PPP) session on LNS.

  Workaround: Configure the following command on the LNS to explicitly send Attribute 31:

  ```
  radius-server attribute 31 send nas-port-detail
  ```

- CSCsf20072

  The data border element (DBE) does not display the active media terminations.

  This issue occurs when you **add** and then **modify** a signaling pinhole, or when you **add** and then **modify** a media pinhole. Although the Audit does respond with active terminations, the **show** command doesn't display the active media terminations.

  There are no known workarounds.

- CSCsg34907

  The data border element (DBE) cannot set the tman/sdr rate limit higher than 1000 pps for incoming traffic. Even when the rate limit of outgoing traffic is set to a higher value and the incoming traffic flowing into the open gate is greater than that value, the DBE rate limit remains at 1000 pps.

  There are no known workarounds.

- CSCsg63466

  The **show int stat** and **show interface** command outputs display twice the number of packets dropped because of a Unicast Reverse Path Forwarding (uRPF) check failure in an IPv6 Multicast scenario.

  There are no known workarounds. Other than the reporting of incorrect statistics, this issue does not affect functionality.

- CSCsg69458

  A Cisco 7200 series router does not purge multicast/unicast packets in the queue when the link goes down.

  This issue occurs on Gigabit Ethernet interfaces on the NPE-G2 when a link flaps (goes down) as a result of the cable being pulled. A burst of packets are observed coming out of the interface.

  There are no known workarounds.

- CSCsg75011

  When one side has no Traffic management (Tman) parameters set, and the second side is set to TMAN=OFF, the media flow are being rate-limited. According to Tman policy, the flow should not be rate limited.

  This issue only occurs on media flow; no problem occurs on signal flow.

  Workaround: Always specify TMAN as either TMAN=ON or TMAN=OFF.

- CSCsg75423

  The data border element (DBE) tears down the H.248 association after the media gateway controller (MGC) sends an Audit response for more than 1000 active calls.

  Workaround: Avoid sending the Audit request. This issue only occurs with an Audit response for more than 1000 calls, so if the Audit request is not sent, the problem does not occur.

Resolved Caveats—Cisco IOS Release 12.2(31)XN2

Cisco IOS Release 12.2(31)XN2 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31)XN2, but may be open in previous Cisco IOS releases.

- CSCek47249

  The CISCO-IP-LOCAL-POOL-MIB is not supported on the Cisco 7200 NPE-G2. Symptoms include the script for this MIB fails, and the SNMPGet on this MIB returns nothing.

  There are no known workarounds.

- CSCek49476

  When the data border element (DBE) sends ServiceChange with a restart, it should include the ServiceChange Reason.

  This issue was a new enhancement request.

- CSCek52673

  A router that has a Dynamic Host Configuration Protocol (DHCP) server enabled reloads after receiving a malformed User Datagram Protocol (UDP) packet on port 67.

  This issue only occurs on Cisco IOS releases 12.2(31)SB, 12.2(31)XN and 12.2(31)XN1. No other releases are affected.

  See also CSCek53559, which affects Cisco IOS releases12.2(31)SB, 12.2(31)SB1, 12.2(31)XN and 12.2(31)XN1.

  There are no known workarounds.

- CSCek53559

  A router reloads after receiving a malformed User Datagram Protocol (UDP) packet on port 67.

  This issue occurs on a Cisco router that functions as a Dynamic Host Configuration Protocol (DHCP) server.

  There are no known workarounds.

- CSCek58674

  Drops occur at very low traffic rates when the **scheduler alloc** command is configured.

  Workaround: Do not use the **scheduler alloc** command.

- CSCek61686

  After a reload, the Gigabit Ethernet interface link status displays as Up, even when there is no cable connected to the port.

  There are no known workarounds.

- CSCin33082

  If the distance of two or more static IP routes are changed in a particular order, then all the routes do not appear in the routing table.

  This issue occurs if your initial change is to change the distance for any route other than the route that appears first in the routing table.

  Workaround: Enter the **clear ip route *** command.

- CSCir00018

  The far end alarm is not asserted on a native Gigabit Ethernet port when a **shut/no shut** is executed.

  There are no known workarounds.

- CSCsc33350

  By default, dot1q subinterfaces do not report link up/down conditions using Simple Network Management Protocol (SNMP) traps. While this problem can be changed using the interface configuration **snmp trap link-status** command on the subinterface, the command's configuration is not retained after a reload of the device.

  Workaround: Re-apply the command after the device has been restarted.

- CSCse16268

  When default or nondefault values for RADIUS 'timeout', 'retransmit', and "radius-server backoff exponential max-delay 1 backoff-retry 5" are configured, the retransmit pattern doesn't match the configured global values.

  There are no known workarounds.

- CSCse23232

  The system sends out two RADIUS accounting-request packets per Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session. Each accounting-request packet has its own unique acct-session-id.

  This issue occurs when PPPoE and Radius accounting are used.

  There are no known workarounds.

- CSCse49651

  In a broadband L2TP Access Concentrator (LAC) scenario when the service policy is applied both on the virtual LAN (VLAN) and virtual template, the following messages occur every 10 milliseconds:

  ```
  *Mar 8 17:49:27 UTC:%QOS-3-INVALID_POLICY: queueing policy at session can co-exist
  only with class-default shaping policy at sub-interface/pvc
  ```

  This issue occurs only when the outbound quality of service (QoS) service policy is applied on the virtual template.

  There are no known workarounds.

- CSCse66625

  The router does not accept a **pppoe limit max-sessions** configuration at the subinterface.

  Workaround: Configure the **limit max-session** under the **bba-group** and attach that **bba-group** to the subinterface.

- CSCse86388

  When the media gateway controller (MGC) sends an **add** request, the remote descriptor should be optional, and the data border element (DBE) should accept the request

  There are no known workarounds.

- CSCse89897

  When a Cisco 7200 series router with NPE-G2 running c7200-g9js-mz.2006-07-24.XNTD is loaded with mixed traffic of IPv6 multicast, IPv6 unicast, session border controller (SBC) Real-Time Protocol (RTP), and PPP over Ethernet (PPPoE), it reports the following errors:

  ```
  *Jul 26 12:47:44.975:%QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to
  allocate hqf particle
  *Jul 26 12:47:44.975:%QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to
  allocate hqf particle
  *Jul 26 12:49:30.939:%SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (154/17),process = Logger.
  -Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328
  *Jul 26 12:49:33.483:%SYS-3-CPUHOG: Task is running for (4004)msecs, more than
  (2000)msecs (290/17),process = Logger.
  -Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328
  ```

  There are no known workarounds.

- CSCse90247

  The data border element (DBE) accepts only decimal Differentiated Services Code Point (DSCP) values, such as ds/dscp=80. According to the H.248 standard, octet values should also be accepted.

  There are no known workarounds.

- CSCse90255

  The data border element (DBE) H.248 stack should support ServiceState property in the TerminationState descriptor.

  There are no known workarounds.

- CSCse92887

  The data border element (DBE) does not send ServiceChange Disconnect to its previously connected media gateway controller (MGC) before sending ServiceChange Failover to the second configured MGC.

  This issue occurs when two MGCs are configured and first one goes down.

  There are no known workarounds.

- CSCse92897

  The RequestID is missing in the H.248 EventDescriptor from the data border element (DBE).

  There are no known workarounds.

- CSCse97861

  The Class of Service (CoS) bits in the VLAN header do not get set according to the quality of service (QoS) configuration.

  This issue occurs when QoS marking of CoS bits is configured at the subinterface/interface level.

  There are no known workarounds.

- CSCse98200

  The data border element (DBE) does not report the ServiceState in the TerminationState when the media gateway controller (MGC) audits the DBE.

  This issue occurs when the MGC sends an **add** request, followed by an **AV** request.

  There are no known workarounds.

- CSCse99720

  When an **audit** request is sent for terminations, the data border element (DBE) reports the wrong codec in the media line.

  There are no known workarounds.

- CSCsf01780

  The data border element (DBE) does not send out ServiceChange with Method Forced for normal deactivation of all active H.248 calls.

  There are no known workarounds.

- CSCsf10884

  The data border element (DBE) does not bit-reverse the DS field according to the H.248.1 Annex B.3 when executing Differentiated Services Code Point (DSCP) marking.

  There are no known workarounds.

- CSCsf13308

  After performing a **shut/no shut** operation on a Gigabit Ethernet interface, the Address Resolution Protocol (ARP) table cannot be created, and as a result, the bidirectional traffic in the session border controller (SBC) does not flow. Traffic flows in only one direction.

  The occurrence of this issue is extremely rare.

  There are no known workarounds.

- CSCsf33015

  When an NPE-G2 has Gigabit Ethernet negotiation disabled, and its peer interface is in the shut state, line protocol up and down messages appear at the console at three-minute intervals.

  Workaround: Enable negotiation.

- CSCsf33175

  The data border element (DBE) sends an incorrect version number in the ServiceChange (MT = DC) when the inactivity timer expires.

  There are no known workarounds.

- CSCsf97195

  The data border element (DBE) does not report a Differentiated Services Code Point (DSCP) value when the media gateway controller (MGC) audits the DBE with media.

  This issue occurs when the MGC sends an **add** request to set up the pinhole, followed by an **audit** request with media. In the audit response, the DSCP value is missing.

  There are no known workarounds.

- CSCsg00562

  The data border element (DBE) does not report a remote descriptor in the media gateway controller (MGC) audit media descriptor.

  This issue occurs when the MGC sends an **add** request to set up the signaling pinhole, followed by an AuditValue (AV) to audit the media descriptor. In the response, the DBE does not report the remote descriptor.

  There are no known workarounds.

- CSCsg00564

  The data border element (DBE) does not respond to a second wildcard audit when there are 30 active contexts

  There are no known workarounds.

- CSCsg01964

  A Cisco 7206VXR router with NPE-G2 running Cisco IOS Release 12.4(4)XD2 does not recognize SFP-GE-Z on G0/2 and G0/3.

  There are no known workarounds.

- CSCsg03091

  A **modify** reply contains an extra stream.

  This issue occurs when the media gateway controller (MGC) sends an **add** request for the signaling pinhole, followed by a **modify** command, and the response sent by the DBE includes "ST=1" for side b even though no parameter was under specified or over specified.

  There are no known workarounds.

- CSCsg04405

  When the remote side of a link goes down, the Gigabit Ethernet interface on the NPE-G2 stays in the Up/Down state instead of the Down/Down state.

  This issue occurs when NPE-G2 native interfaces are used, and the remote interface is shut down or the cable is not connected.

  Workaround: Shut down the NPE-G2 interface when the remote interface is down.

- CSCsg06159

  When the media gateway controller (MGC) sends an **add/modify** request with the Traffic Management (Tman) package for only one gate, the data border element (DBE) rejects the call with error 421:

  ```
  a device attempted to use the Traffic Management package on only one stream of a flow
  pair or attempted to police only one stream of a flow pair
  ```

  There are no known workarounds.

- CSCsg08823

  The local descriptor in an H.248 **add** operation should be optional so that if the media gateway controller (MGC) sends an **add** request to the data border element (DBE) without a local descriptor, the DBE does not reject the call.

  This issue was a new enhancement request.

- CSCsg11511

  When the media gateway controller (MGC) sends an **add** request with a **gm/sam** value specified within double quotes (" "), the data border element (DBE) rejects the request with Error=421 because of an invalid source address mask format. According to Annex B.2 of the H.248.1v3 standards, the DBE should only accept **gm/sam** values specified within double quotes (" ").

  There are no known workarounds.

- CSCsg17862

  When a remote descriptor is set to 0.0.0.0/0 with napt=RELATCH, the data border element (DBE) rejects the **add** request.

  This issue occurs because the DBE incorrectly requires the remote descriptor address to be the same as the gm/sam address even when napt=RELATCH in the **add** request.

  There are no known workarounds.

- CSCsg31421

  Although the media gateway controller (MGC) sent Traffic management (Tman) parameters for both gates, only the first gate parameters are used for policing on both sides. If no parameters are specified on the first gate (side A), then no policing is performed.

  This issue occurs when the MGC sends an **add** request with different Tman parameters on side A and side B.

  There are no known workarounds.

- CSCsg31742

  False environment warnings about certain voltages are posted to the NPE-G2 console.

  The false warnings can be ignored.

  There are no known workarounds.

- CSCsg35405

  A data border element (DBE) crashes when the DBE receives an unsupported sfr package from the media gateway controller (MGC).

  This issue occurs when the MGC sends an ADD request with the unsupported sfr package in the local control description.

  Workaround: MGC should not send an unsupported sfr package.

- CSCsg37074

  Cisco IOS does not accept the **ipv6 mld state-limit** global command.

  There are no known workarounds.

- CSCsg46753

  The data border element (DBE) does not impose the limit for maxterminationpercontext and does not report the correct value for max number of terminations.

  There are no known workarounds.

- CSCsg46758

  The data border element (DBE) should support 32 Terminations per Context, (ROOT/MAXTERMINATIONSPERCONTEXT=32), but when the media gateway controller (MGC) tries to add 32 Terminations in a Context, the DBE rejects the **add** request.

  This issue occurs because the DBE is not checking for this limit or reporting the MAXTERMINATIONPERCONTEXT value correctly.

  There are no known workarounds.

- CSCsg49832

  When more than 100 calls are active and **no activate/activate** is executed on the data border element (DBE), the DBE crashes.

  There are no known workarounds.

- CSCsg50543

  A router crashes when the service-policy information of a session is displayed using the **show policy-map interface** command.

  This issue occurs when the input and output policy are attached to the same session.

  There are no known workarounds.

- CSCsg63932

  An IPv6 static route is removed from the IPv6 routing table, even though the IPv6 static route is valid and still exists.

  This issue occurs in the following scenario:

  a. An identical IPv6 static route (same next-hop, interface, and distance) is learnt from two sources, such as, through manual configuration and the Dynamic Host Configuration Protocol (DHCP) PD.

  a. The route is installed in the IPv6 routing table.

  b. One source deletes the IPv6 static route. Although the route should remain in the IPv6 routing table, because it is still being known by other source, the route is removed from the IPv6 routing table.

Workaround: To prevent the occurrence of this error, ensure that sources contribute identical IPv6 static routes at different administrative distances. If identical static routes occur, adjust the administrative distance of the manually-configured static route.

- CSCsg65296

  Output drops occur on the egress interface when priority queuing is configured even if the total traffic is less than the link bandwidth.

  This issue occurs when there is a large number of multicast users listening to same group.

  There are no known workarounds.

- CSCsg71344

  When a Cisco 7200 VXR router running IPv6 Source Specific Multicast (SSM) is connected is to an Upstream router using two Reverse Path Forwarding (RPF) interfaces, and the one of the RPF interfaces is **shut/unshut**, the Protocol Independent Multicast (PIM) **join** message is not sent, resulting in no IPv6 multicast topology.

  This issue occurs because during the interval that first RPF interface was **shut**, a PIM **join** message was sent using the other RPF interface. When the original RPF interface is **unshut**, the PIM **join** message is not resent.

  There are no known workarounds.

- CSCsg75054

  A crash occurs when the logging level is set to a low level (such as, 10), and a filter is set to **media**.

  Workaround: Do not use a logging level lower than 63 in the production system.

Open Caveats—Cisco IOS Release 12.2(31)XN1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31)XN1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek24232

  A PPP over Ethernet (PPPoE) user cannot get a prefix assigned from the IOS DHCPv6 server when the IOS DHCPv6 server is configured to get the delegated prefixes from a RADIUS server. The message exchange method used is a 2-way message exchange.

  There are no known workarounds.

- CSCek41328

  When unconfiguring and configuring **ipv6 multicast-routing** with a large number of virtual LANs (VLANs) (2000-3000), CPUHOGS messages appear at bootup on the route, and sometimes these CPUHOGS messages are followed by a crash.

  Workaround: Configure **ipv6 multicast-routing** globally prior to enabling and configuring all of the individual subinterfaces. Thereafter, no interface should be deleted from the configuration or a similar HOG will occur. Nor, should **ipv6 multicast-routing** be deconfigured. The other alternative is not to configure/unconfigure **ipv6 multicast-routing** and to reboot the router if needed.

- CSCir00015

  atmIntfPvcFailuresTrap is not generated for all permanent virtual circuit (PVC) failures.

  atmIntfPvcFailuresTrap is generated only once (for the first **shut/no shut** on the ATM interface); for subsequent PVC failures there is no trap generated.

  There are no known workarounds.

- CSCir00018

  The far end alarm is not asserted on a native Gigabit Ethernet port when a **shut/no shut** is executed.

  There are no known workarounds.

- CSCir00095

  When "transmit" is configured under conform, the cbQosPoliceActionCfgConformSetValue, cbQosPoliceActionCfgExceedSetValue, cbQosPoliceActionCfgViolateSetValue instances for transmit actions are missing in the QosPoliceActionCfgTable.

  There are no known workarounds.

- CSCsd39528

  When IPv6 Protocol Independent Multicast (PIM) tunnels are created, duplicate Interface Index numbers are assigned to the tunnel interfaces. This issue can cause traffic to not switch out between these multicast interfaces, and can cause the router to crash with a bus error when these tunnels are deleted and recreated.

  You can verify this problem has occurred by entering the **show idband** command and looking for duplicate if-index entries for the tunnel interfaces.

  There are no known workarounds.

- CSCse16268

  When default or nondefault values for RADIUS 'timeout', 'retransmit', and "radius-server backoff exponential max-delay 1 backoff-retry 5" are configured, the retransmit pattern doesn’t match the configured global values.

  There are no known workarounds.

- CSCse49651

  In a broadband L2TP Access Concentrator (LAC) scenario when the service policy is applied both on the virtual LAN (VLAN) and virtual template, the following messages occur every 10 milliseconds:

  ```
  *Mar 8 17:49:27 UTC: %QOS-3-INVALID_POLICY: queueing policy at session can co-exist
  only with class-default shaping policy at sub-interface/pvc
  ```

  This issue occurs only when the outbound quality of service (QoS) service policy is applied on the virtual template.

  There are no known workarounds.

- CSCse66625

  The router does not accept a **pppoe limit max-session**s configuration under the subinterface.

  Workaround: Configure the **limit max-sessions** under the **bba-group** and attach that **bba-group** to the subinterface.

- CSCse80880

  Multiple Accounting Start and Stop records are sent to a RADIUS server on the router acting as a L2TP Access Concentrator (LAC) when a quality of service (QoS) service policy is applied to virtual template.

  There are no known workarounds.

- CSCse85047

  The L2TP network server (LNS) is not sending the Calling-Station-Id (Attribute 31) to the RADIUS authentication, authorization, and accounting (AAA) Remote Authentication Dial-In User Service in Accounting Start/Stop messages.

  This problem occurs when you bring up or tear down a Point-to-Point Protocol (PPP) session on the LNS.

  Workaround: Configure the following LNS command to explicitly send attribute 31:

  radius-server attribute 31 send nas-port-detail

- CSCse86200

  The following message occurs during Trivial File Transfer Protocol (TFTP) bootup when the bootloader image used is 12.2(31)XN-based and Modular QoS CLI (MQC) is configured on the subinterface virtual LANs (VLANs):

  ```
  % Configuring IP routing on a LAN subinterface is only allowed if that subinterface
  is already configured as part of an IEEE 802.10, IEEE 802.1Q, or ISL vLAN.
  MQC features are not supported for this interface
  MQC features are not supported for this interface
  ```

  The number of messages that appear depends upon number of VLANs configured with quality of service (QoS).

  Workaround: The only known workaround is to use the 12.4 XD3-based bootloader image.

- CSCse89897

  When a Cisco 7200 series router with NPE-G2 running c7200-g9js-mz.2006-07-24.XNTD is loaded with mixed traffic of IPv6 multicast, IPv6 unicast, session border controller (SBC) Real-Time Protocol (RTP), and PPP over Ethernet (PPPoE), it reports the following errors:

  ```
  *Jul 26 12:47:44.975: %QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to
  allocate hqf particle
  *Jul 26 12:47:44.975: %QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to
  allocate hqf particle
  *Jul 26 12:49:30.939: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (154/17),process = Logger.
  -Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328
  *Jul 26 12:49:33.483: %SYS-3-CPUHOG: Task is running for (4004)msecs, more than
  (2000)msecs (290/17),process = Logger.
  -Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328
  ```

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(31)XN1

Cisco IOS Release 12.2(31)XN1 is a rebuild release for Cisco IOS Release 12.2 XN. The major caveats in this section are resolved in Cisco IOS Release 12.2(31)XN1, but may be open in previous Cisco IOS releases.

- CSCse59101

  The router crashes to the "Rommon>" prompt. The following line appears in the console log immediately prior to the crash:

  ```
  Assertion failed: '(&nbb_assert_method == 0)', file ../sbc/sbc-app/src/mgm/bmmfprc.c,
  line 794
  ```

  This issue occurs when an invalid H.248 GATE ADD request, which does not specify either the ntr/nap property or a remote address for the gate, is received.

  Workaround: Ensure all H.248 GATE ADD requests from the signaling border element (SBE) contain either the ntr/nap property or a remote address for the gate.

- CSCse65907

  During configuration of the Logical Line ID (LLID) feature, the Calling-Station-id (Attribute 31) is not sent from the L2TP access concentrator (LAC) to the authentication, authorization, and accounting (AAA) server.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(31)XN

This section documents possible unexpected behavior by Cisco IOS Release 12.2(31)XN and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCse30630

  When a **no attach-controller** command is issued in VDBE submode of a session border controller (SBC) data border element (DBE), the following logs are seen:

  ```
  ----------------------------------------------------------------------------------
  *May 21 13:37:00.847: %SBC-1-MSG-4D01-0020: (bmmeprod.c 177)
  Two components of the SBC have lost their communication connection. New calls may not
  be set up in the MEDIA component until this has been resolved.
  Existing calls will be unaffected
  (Extra information: MGM has lost the join to the GCI slave (AL or BM)


  *May 21 13:37:00.847: %SBC-2-MSG-4B01-0006: (ahslhaf.c 895)
  A partner on a master join is unavailable
  Interface ID:0X54800000
  Partner type:0X4E030000
  Partner index:0X00000001
  Sub-index:0X00000000
  ----------------------------------------------------------------------------------
  ```

  These logs occur if the **no attach-controllers** command is issued while the DBE is active. The logs are benign.

  Workaround: Although the logs are benign, they can be avoided if the **no activate** command is issued for the SBC DBE before issuing the **no attach-controllers** command.

- CSCse46170

  In bursty traffic conditions (where 200 or more calls are being made at once) some calls fail, and the data border element (DBE) reports the following errors:

```
Jun 7 23:11:19.323: %SBC-2-MSG-2E01-0140: (gcmbmeg6.c 317)
A buffer was supplied to the message build library of insufficient size to add all
requested parameters.

Jun 7 23:11:19.323: %SBC-2-MSG-4E03-0030: (bmahsrp.c 168)
A resource failure has prevented SBC-Media from sending a message to its controller.
SBC-Media will continue to operate normally, but may repeat an action if the
controller re-sends the request.
Message was request?: False
Megaco transaction ID: 3749024
Reason for failure: Failed to build message response
```

  This issue occurs when the start-to-start time between call channels is 0.

  Workaround: Increase the start-to-start time between call channels to 0.1 seconds.

- CSCse59101

  The router crashes to the “Rommon>” prompt. The following line appears in the console log immediately prior to the crash:

```
Assertion failed: '(&nbb_assert_method == 0)', file ../sbc/sbc-app/src/mgm/bmmfprc.c,
line 794
```

  This issue occurs when an invalid H.248 GATE ADD request, which does not specify either the ntr/nap property or a remote address for the gate, is received.

  Workaround: Ensure all H.248 GATE ADD requests from the signaling border element (SBE) contain either the ntr/nap property or a remote address for the gate.

Resolved Caveats—Cisco IOS Release 12.2(31)XN

Because Cisco IOS Release 12.2(31)XN is the initial special release, there are no resolved caveats.

Related Documentation

The following sections describe the documentation available for the Cisco 7200 VXR routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and http://www.cisco.com/univercd/home/home.htm

Use these release notes with these documents:

- Platform-Specific Documents, page 93
- Feature Modules and Documentation, page 93

Platform-Specific Documents

These documents are available for Cisco 7200 VXR routers on Cisco.com:

- *Cisco7200 VXR Installation and Configuration Guide*
- *Cisco 7200 VXR Routers Quick Start*

On http://www.cisco.com/univercd/home/home.htm at:

Routers > Cisco 7200VXR

Feature Modules and Documentation

Feature modules describe new features supported by Cisco IOS Release 12.2(31c)XN3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

Cisco IOS Release 12.2(31)XN2 includes the following feature modules and documentation:

- *Cisco IOS IPv6 Configuration Guide*, which includes further information about the IPv6 Multicast - MLD Group Limit feature
- *Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200* feature document
- *IPv6 Multicast Triggered RPF Check* feature document
- *PPPoE Session Limit Local Override* feature document
- *QoS: Bandwidth Remaining Ratio* feature document
- *PXF Information for Cisco 7304 Routers* document, which includes further information about the DHCPv6 features in Cisco IOS Release 12.2(31)XN2

Cisco IOS Release 12.2(31)XN1 includes the following feature modules and documentation:

- *Cisco IOS IPv6 Implementation Library*, which includes further information IPv6 support
- *Disable VPDN Logging for Normal Session Termination* feature document
- *Equal Bandwidth Sharing (EBS)* feature document
- *Multi-Level Priority Queues (MPQ)* feature document

Cisco IOS Release 12.2(31)XN includes the following feature module:

- *Cisco IOS Session Border Controller DBE Deployment for the Cisco 7200* feature document

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 92.