New and Changed Information

This section lists the new hardware and software features that are supported in Cisco IOS Release 12.2 and contains the following sections:

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.

Note MPLS Class of Service is now referred to as MPLS Quality of Service. This transition reflects the growth of MPLS to encompass a wider meaning and highlight the path towards *Any Transport over MPLS*.

New Software Features in Release 12.2(26)

The following features are supported in Cisco IOS Release 12.2(26).

Route Switch Processor 16

The Route Switch Processor 16 (RSP16) is the latest-generation main system processor module for the Cisco 7500 series routers. The RSP16 is not available as an upgrade to an existing RSP, but supports VIP2, VIP4, and the new VIP6-80. The RSP16 contains the CPU and most of the memory components for the router.

For more information, refer to the *Route Switch Processor (RSP16) Installation and Configuration Guide* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/rte_swit/13963r16.htm

New Software Features in Release 12.2(19c)

The following features are supported in Cisco IOS Release 12.2(19c).

Channelized T3 PA CLI

Cisco IOS Release 12.2(19c) introduces new and modified CLI commands for the Multichannel T3 Port Adaptor (PA-MC-2T3+ and PA-MC-T3) for the Cisco 7200 series and Cisco 7500 series routers.

The new CLI commands are:

error throttling–disables the T1 clock in order to stop receiving error data packets on a T1 controller.

logging-events–prints T3 controller Up and Down messages. The **detail** keyword enables the printing of a reason code when the T3 changes to Down status.

t1 logging-events–prints T1 controller Up and Down messages. The **detail** keyword enables the printing of a reason code when a T1 controller of a T3 changes to Down status.

The modified CLI command is:

show controllers t3–added error throttling information and alarm events that indicate the reason for the T3 controller entering a failure state.

New Software Features in Release 12.2(16b)

The following features are supported in Cisco IOS Release 12.2(16b).

Hot Standby MAC Address

The Hot Standby MAC Address (HSMA) feature achieves redundancy and fault tolerance and avoids a single point of failure of Cisco Channel Interface Processors (CIPs) or Channel Port Adapters (CPAs). This feature also ensures that multiple devices on the Ethernet can have a common MAC address.

Refer to the following document for further information:

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

New Software Features in Release 12.2(16)

The following features are supported in Cisco IOS Release 12.2(16).

Hot Standby MAC Address

The Hot Standby MAC Address (HSMA) feature achieves redundancy and fault tolerance and avoids a single point of failure of Cisco Channel Interface Processors (CIPs) or Channel Port Adapters (CPAs). This feature also ensures that multiple devices on the Ethernet can have a common MAC address.

Refer to the following document for further information:

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

New Software Features in Release 12.2(10)

The following features are supported in Cisco IOS Release 12.2(10).

Voice DSP Control Message Logger and Offline Checker

The Voice DSP Control Message Logger and Offline Checker feature provides improved debugging capabilities through Cisco IOS software to allow the ability to log control messages that pass through the Cisco IOS software and TI-based voice digital signal processor (DSP) firmware on the Host Port Interface (HPI). The logged messages can later be examined when diagnosing voice problems are diagnosed.

There are two main types of HPI messages that flow through the HPI interface: control messages and data messages. Control messages carry control information between Cisco IOS software and the DSP. Data messages carry voice data.

The Voice DSP Control Message Logger and Offline Checker feature captures platform-independent control messages, which are those messages sent between the platform-independent portions of Cisco IOS software and the DSP. The HPI subsystem in Cisco IOS software contains the platform-independent portion of Cisco IOS software. This feature addresses the sequence and contents of the control messages, and when examined by a Cisco engineer, the logged messages can be checked for parameters that might cause undesirable DSP behavior, including the following:

- Incorrect parameters
- Out-of-sequence function calls
- Interactions between parameters of different HPI calls

In a large number of cases, DSP problems have resulted from bad control messages being passed to the DSP. By logging all of these messages for offline analysis, you can better integrate and debug during engineering development and test, as well as capture at-speed issues in the field for engineering analysis.

New Software Features in Release 12.2(1)

The following features are supported in Cisco IOS Release 12.2.

- AAA Broadcast Accounting (CSCdk39995)
- AAA DNIS Map for Authorization
- AAA Server Group Deadtimer (CSCdp13160)
- AAA Session MIB
- Airline Product Set Enhancements (CSCdp64339)
- Answer Supervision Reporting (CSCdp21888)
- Asynchronous Rotary Line Queueing
- AutoInstall Using DHCP for LAN Interfaces (CSCdr88175)
- Baseline Privacy Interface MIB
- Bidirectional PIM
- Bridging Between IEEE 802.1Q VLANs
- Cable Downstream Frequency Override CLI
- Cable Monitor Web Diagnostics Tool
- Cable Subinterfaces and Interface Bundling
- Caller ID
- CEF Support for IP Routing Between IEEE 802.1Q VLANs
- CEF Switching for Routed Bridge Encapsulation
- Circuit Interface Description MIB (CSCdp81924)
- Cisco AAA Server MIB and Additional Enhancements for the Cisco AS5300 and Cisco AS5800
- Cisco Cable Clock Card Support
- Cisco Quality of Service Device Manager 2.0 Support

- Class-Based Ethernet CoS Matching and Marking (802.1p & ISL CoS)
- Class-Based Marking
- Class-Based Policer for the DiffServ AF PHB
- Class-Based Quality of Service Management Information Base
- Class-Based Shaping
- Closed User Group Selection Facility Suppress Option
- Common Application Programming Interface (CAPI)
- Configurable H.225 Timer
- Configurable per ATM-VC Hold Queue Size
- Configurable Timers in H.225 (CSCdp30190)
- Configuration Through SNMP (CSCdj10821)
- Configuring Burst Size in Low Latency Queueing
- COPS for RSVP
- DES/3DES VPN Encryption AIM for 2600/3600
- DFP Support in DistributedDirector—Cisco 2501 and Cisco 2502 Only
- Dial-on-Demand Authentication Enhancements (CSCdp96375)
- Dial Peer Enhancements
- DiffServ Compliant Weighted Random Early Detection
- Distributed Traffic Shaping
- DistributedDirector Enhancements
- DOCSIS 1.0+ Extensions
- DOCSIS Quality of Service Enhancements
- Dynamic Host Configuration Protocol Proxy Support
- Dynamic Mobile Hosts
- Ecosystem Gatekeeper Interoperability Enhancements (CSCdp48320)
- Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 (CSCdp70719)
- Enhanced Modem Status Display
- Enhanced Per Modem Error Counter
- Enhanced Voice Services
- Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms
- Event MIB
- Express Real-Time Transport Protocol and TCP Header Compression (CRTP)
- Expression MIB Support of Delta, Wildcarding, and Aggregation
- FastEther Channel Enhancements on Cisco 7200 Series Routers
- Fax Relay Packet Loss Concealment
- Feature Group D Support on Digital T1/E1 Packet Voice Trunk Network Modules
- Firewall Enhancements
- Frame Relay ELMI Address Registration

- Frame Relay Fragmentation with Hardware Compression
- Frame Relay PVC Interface Priority Queueing
- Frame Relay Support
- Frame Relay Switching Diagnostics and Troubleshooting
- Frame Relay Switching Enhancements
- FXO Supervisory Disconnect Tone
- Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism
- Gateway-to-Gatekeeper Billing Redundancy
- General Packet Radio Service Release 1.4
- H.323 Enhancements
- H.323 Support for Virtual Interfaces
- H.323 Version 2, Phase 2 Enhancements
- H.323 Version 2 Enhancements for the Cisco 1750 Router
- HSRP Support for ICMP Redirects
- HSRP Support for MPLS VPNs
- IGMP Version 3
- IKE Extended Authentication
- IKE Shared Secret Using AAA Server
- Implementing DiffServ for End-to-End Quality of Service
- Inband MICA Control Messages for PPP Framing
- Individual SNMP Trap Support
- Integrated Routing and Bridging, Transparent Bridging, and PVST+ Between VLANs with IEEE 802.1Q Encapsulation
- Interactive Voice Response Version 2.0 on Cisco VoIP Gateways
- Inter-Autonomous Systems MPLS VPN Support
- Interface Command Enhancements
- Interface Index Persistence
- Interface Range Specification
- Interworking Signaling Enhancements for H.323 and SIP VoIP
- IP Address Negotiation
- IP DSCP Marking for Frame-Relay PVC
- IP over a CLNS Tunnel
- ISDN Network Side for ETSI Net5 PRI
- ISDN Progress Indicator Support for SIP using 183 Session Progress
- L2TP Tunnel Management Enhancements
- L2TP Tunnel Switching
- Leased line Support for 2600/3600 Analog Modems NM-16AM and NM-8AM
- Low Latency Queueing for Frame Relay

- MC16S LED Enhancement
- Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway
- Media Gateway Control Protocol Residential Gateway Support
- MGCP Support for CallManager (IP-PBX)
- Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes
- Monitoring Resource Availability on Cisco AS5300, AS5400, and AS5800 Universal Access Servers
- MPLS Quality of Service Enhancements
- MPLS Egress NetFlow Accounting
- MPLS Scalability Enhancements for LSC and ATM LSR
- MPLS Traffic Engineering and Enhancements
- MPLS VPN Support for Subinterfaces and Interface Bundles
- MSDP MIB
- Multicast Hoot and Holler Conferencing over IP
- Multimedia Conference Manager with Voice Gateway Image with RSVP to ATM SVC Mapping
- Multiprotocol Label Switching on Cisco Routers
- NAT—Enhanced H.225/H.245 Forwarding Engine
- NAT—Support for NetMeeting Directory (Internet Locator Service - ILS)
- NAT—Support of H.323 v2 Call Signaling (FastConnect)
- NAT—Support of IP Phone to Cisco Call Manager
- Network-Based Application Recognition
- Network Side ISDN PRI Signaling, Trunking, and Switching
- NextPort Port Service Management for the Cisco AS5400 Universal Access Server
- NM-1A-OC3MM-1V NM-1A-OC3SM1 and NM-1A-OC3SML-1V
- NTP MIB
- OSPF Flooding Reduction
- Parser Cache
- PIM Dense Mode State Refresh
- Point-to-Point Protocol (PPP) over ATM Using Dialer Interfaces
- PPP Over ATM SVC
- PPP over Ethernet on ATM
- PPP Over Fast Ethernet 802.1Q
- PPPoE Over IEEE 802.1Q VLANs
- PPPoE RADIUS Port Identification
- PPPoE Termination on Cable interfaces
- Pragmatic General Multicast (PGM)
- Preauthentication Enhancements for Callback
- Preauthentication with ISDN PRI

- Preauthentication with ISDN PRI and Channel-Associated Signaling
- Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements
- Prepaid Distributed Calling Card via Packet Telephony
- PRI/Q.931 Signaling Backhaul for Call Agent Applications
- PRI QSIG on the Cisco 7200
- PSTN Fallback
- QSIG Protocol Support
- Quality of Service for Virtual Private Networks
- Quality of Service Voice Enhancements
- RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements
- RADIUS Attribute 8 (Framed-IP-Address) in Access Requests
- RADIUS Packet of Disconnect
- RADIUS Tunnel Attribute Extensions
- Redirect-Number Support for RADIUS and TACACS+ Servers
- RFC 2233 Support
- Router-Port Group Management Protocol
- RSVP Support for Frame Relay
- RSVP Support for Low Latency Queuing (LLQ)
- SDLC SNRM Timer and Window Size Enhancements
- Secure Shell Version 1 Integrated Client
- Service Assurance Agent Enhancements
- Session Initiation Protocol (SIP)
- Session Initiation Protocol Gateway Call Flows
- Set ATM CLP Bit
- Settlement for Packet Telephony with Roaming and Multiple Roots
- Settlement Plus Roaming and PKI Multiple Roots on Cisco Access Platforms (Settlements for Packet Voice, Phase 2)
- SGCP Call Control Protocol Support on the Cisco MC3810 and 3600 series routers
- SNMP Cable Modem Remote Query
- SNMP Enhancements
- SNMP Support for IOS vLAN Subinterfaces
- Source Specific Multicast (SSM)
- SSH Version 1 Server Support
- State-Refresh
- T1/E1 Alarm Conditioning for Switched Calls and Permanent Connection Trunks
- T.37/T.38 Fax Gateway
- T.38 Fax Relay for VoIP H.323
- TCP Clear Performance Optimization

- TN3270 Server Connectivity Enhancements
- Traceroute Enhancement for MPLS
- Transparent CCS and Frame Forwarding Enhancements on the Cisco MC3810
- Transparent Common Channel Signalling (T-CCS)
- Trunk Conditioning Enhancements
- Trunk Conditioning for FRF.11 and Cisco Trunks
- Turbo Access Control Lists
- UDLR Tunnel ARP and IGMP Proxy
- uOne (Unified Messaging) on Cisco 3660 Multiservice Platforms
- Cable Subinterfaces and Interface Bundling
- V.110 Support for 3600 Digital Modems
- Virtual Profile CEF Switched
- VIC-2BRI-NT/TE, MC3810-BVM4-NT/TE
- VIP-Based Distributed FRF.11/12
- VIP-Based Distributed FRF.11/12
- VIP-Based WFQ Support for RSVP
- Virtual Private Network (VPN) Module for the Cisco 1700 Series
- Virtual Switch Interface Master MIB
- Voice Busyout Enhancements
- Voice Over ATM
- Voice over ATM with AAL2 Trunking
- Voice Over Frame Relay
- Voice over Frame Relay Configuration Updates Using FRF.11 and FRF.12
- Voice over IP
- Voice Port Enhancements
- Voice Port Testing Enhancements
- VoIP Call Admission Control using RSVP
- WCCP Redirection on Inbound Interfaces
- Wildcard Pre-Shared Key Enhancement

AAA Broadcast Accounting (CSCdk39995)

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple authentication, authorization, and accounting (AAA) servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

With the introduction of this feature, broadcasting is now allowed among groups of servers. The server groups can be either RADIUS or TACACS+. And each server group can define its backup servers for fail over independently of other groups. (Fail over is a process that may occur when more than one server

has been defined within a server group. Fail over refers to the process by which information is sent to the first server in a server group; if the first server is unavailable, the information is sent to the next server in the server group. This process continues until the information is successfully sent to one of the servers within the server group or until the list of available servers within the server group is exhausted.) Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt_aaaba.htm

AAA DNIS Map for Authorization

The AAA DNIS Map for Authorization feature allows you to select authentication, authorization, and accounting (AAA) server groups—to which authorization requests can now be sent—using Dialed Number Information Service (DNIS). This feature is an enhancement to Selecting AAA Server Groups Based on DNIS, Cisco IOS Release 12.0(7)T, which allows you to send authentication and accounting requests when selecting a AAA server group using DNIS.

With the introduction of this feature, authorization requests are available so that you can specify the same server group for AAA services or a separate server group for each AAA service. Thus, you can configure authorization on different physical devices and provide fail-over backup support. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtaudnis.htm

AAA Server Group Deadtimer (CSCdp13160)

The AAA Server Group Deadtimer feature allows each authentication, authorization, and accounting (AAA) server to be fully configured in the server group. Thus, it allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

With the introduction of this feature, deadtime has been added as a new attribute to the server group structure. In addition, a separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and times-out, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note The deadtime attribute is supported only for RADIUS hosts.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtaaasge.htm

AAA Session MIB

Customers are demanding the ability to both monitor and terminate their authenticated client connections via Simple Network Management Protocol (SNMP). Furthermore, customers are requesting that the client data provided be directly related to the accounting information reported by authentication,

authorization, and accounting (AAA) to either RADIUS or TACACS. Moreover, additional real-time information, such as idle times, is also requested for this feature in order to provide the ability to terminate calls with no activity present.

This feature allows Cisco customers to extend and expand their ability to monitor end users by providing access to some client data objects via SNMP. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_asmib.htm

Airline Product Set Enhancements (CSCdp64339)

The Airline Product Set Enhancements feature in Cisco IOS Release 12.1(2)T introduces additions to the Airline Product Set (ALPS) service messages and extensions to the ALPS P1024B Airline Control (ALC) protocol support. This feature includes customized options to configure the format, address, and transmission of service messages. The ALPS ALC support is extended to be more scalable. This feature is an enhancement to the existing ALPS technology.

Note Remote routers must have the Cirrus Logic CD2430 chipset on a synchronous serial interface module to connect to the ALC or Unisys Terminal System (UTS) agent set control units (ASCUs).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/2dt_alps.htm

Answer Supervision Reporting (CSCdp21888)

The Answer Supervision Reporting feature is an enhancement to the information request (IRR) Registration, Admission, and Status protocol (RAS) message that enables gatekeepers to maintain call accounting information by reporting the call connection time of connected calls to the gatekeeper.

In H.323 configurations, direct call-routed signaling is utilized by the endpoint (gateway). Gatekeepers do not have real-time knowledge or control over the state of a call and are dependent on the endpoints to provide them the necessary real-time information, such as the call connect time, call termination time, and call termination reason.

When a call ends, the gateway sends a Disengage Request (DRQ) message with the BillingInformationToken (which contains the duration of the call) to the gatekeeper. However, if the gatekeeper does not receive the DRQ message for some reason, the gatekeeper will not have the information about when the call started or the duration of the call, which is necessary to maintain accounting information.

The Answer Supervision Reporting feature addresses the need to report the call connection time to the gatekeeper upon the connection of a call and at periodic intervals thereafter. The Answer Supervision Reporting feature adds a proprietary Cisco parameter, the call connection time parameter, to the perCallInfo parameter in the nonStandardData field, which is located in the IRR message. When a CONNECT message is received, the originating gateway sends the unsolicited IRR message to its gatekeeper. On sending a CONNECT message, the terminating gateway sends the unsolicited IRR message to its gatekeeper. If the admission confirmation (ACF) message has a nonzero value for the IRR frequency parameter, the gateway sends the unsolicited IRR message to its gatekeeper at periodic intervals, which are determined by the value in the IRRfrequency parameter. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/asreport.htm

Asynchronous Rotary Line Queueing

The software Asynchronous Rotary Line Queueing feature allows Telnet connection requests to busy asynchronous rotary groups to be queued so that users automatically obtain the next available line, rather than needing to try repeatedly to open a Telnet connection. The Cisco IOS software sends a periodic message to the user to update progress in the connection queue.

Connections are authenticated using the method specified for the line configurations for the asynchronous rotary group. If a connection is queued, authentication is done before queueing and no authentication is done when the connection is later established. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtasyncq.htm

AutoInstall Using DHCP for LAN Interfaces (CSCdr88175)

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature that provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. In Cisco IOS Release 12.1(5)T, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI interfaces. Before this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also allows the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. Additionally, this feature allows for the uploading of configuration files using unicast TFTP. Refer to the following document for further information:

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

Baseline Privacy Interface MIB

Cisco uBR7200 series universal broadband routers now include support for the data-over-cable service interface specification (DOCSIS) Baseline Privacy Interface (BPI) MIB. This allows a simple network management protocol (SNMP) manager to monitor and manage the router's BPI configuration, including whether BPI is enabled, status of current authorization keys, current timeout values, real-time status counters, and additional information about authorization errors.

Note The SNMP manager must load the DOCS-BPI-MIB.my MIB to access the BPI attributes.

Bidirectional PIM

Bidirectional PIM(bidir-PIM) is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode

- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning-tree topology rooted in that IP address. This IP address does not need to be that of a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

Membership to a bidirectional group is signaled via explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional mode can scale to an arbitrary number of sources without incurring overhead because of the number of sources.

Bidir-PIM is derived from the mechanisms of PIM sparse mode (PIM SM) and shares many shortest path tree (SPT) operations. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling to an arbitrary number of sources.

Note As of Cisco IOS Release 12.2 or later releases, bidir-PIM is disabled by default and must be explicitly enabled by configuring the **ip pim bidir-enable** command in global configuration mode.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtbipim.htm

Bridging Between IEEE 802.1Q VLANs

This feature supports integrated routing and bridging (IRB), transparent bridging (TB), and Per VLAN Spanning Tree+ (PVST+) between VLANs with IEEE 802.1Q encapsulation features. It provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. This feature supports the following IEEE 802.1Q (Dot1q) functionality:

- IRB—connectivity for multiple VLANs using a Bridge-Group Virtual Interface (BVI) to associate a bridge group.
- TB—connectivity for multiple VLANs bridged between Dot1q interfaces and other interface encapsulations or other types of interface media.
- PVST+ for IEEE 802.1Q trunks—support for Dot1q trunks to map multiple spanning trees to a single spanning tree.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtbridge.htm

Cable Downstream Frequency Override CLI

The following new command-line interface (CLI) command turns off the cable downstream frequency override on a per-interface basis:

no cable downstream override

The default configuration enables the cable downstream frequency override. Only the **no cable downstream override** command is displayed; this command allows the cable downstream frequency override to be turned off.

Cable Monitor Web Diagnostics Tool

The Cable Monitor is a web-based diagnostic tool to display the current status and configuration of the Cisco uBR924 router. The Cable Monitor can also be used when the cable network is down, providing an easy way for subscribers to provide necessary information to service technicians and troubleshooters.

Cable Subinterfaces and Interface Bundling

Cisco uBR7200 series software supports the definition of logical network layer interfaces over a cable physical interface or a bundle of cable interfaces. The system also supports subinterface creation on either a physical cable interface or a bundle of cable interfaces. This allows a service provider to share one IP subnet across multiple cable interfaces that are grouped into a cable interface bundle. All of the cable interfaces on a Cisco uBR7200 series universal broadband router can be grouped into a single bundle so that only one subnet is required for each router. This eliminates the requirement that a separate IP subnet be used for each individual cable interface. This in turn avoids the performance, memory, and security problems that result if a bridging solution is used to manage subnets, especially for a large number of subscribers.

Note Cable interface bundling is applicable only in two-way cable configurations. It is not supported in telco-return configurations.

The Cable Modem Termination System (CMTS) administrator can perform the following tasks:

- Define subinterfaces on a cable physical interface and assign Layer 3 configurations to each subinterface.
- Bundle a group of physical interfaces and define a bundle master Layer 3 configuration or define subinterfaces on the bundle master and give each subinterface Layer 3 configurations.

The command to create a subinterface over a cable interface is the same as that defined by Cisco IOS for other software applications:

interface cable *x/y.n*

where *x* is the slot number, *y* is the port number, and *n* is the subinterface number.

Two new commands implement the bundling feature:

- **cable bundle** *number* [master]—Configures cable interfaces into bundles.
- **show cable bundle** *number* **forwarding table**—Displays all the currently known cable devices in the bundle.

Administrators can create subinterfaces on cable interfaces or cable interface bundles to support Virtual Private Network (VPN). Each subinterface can be assigned to a specific pool of IP addresses, mapping that subinterface to a particular VPN customer network. A Generic Routing Encapsulation (GRE) tunnel can also be created between the Cisco uBR7200 series router and the router that serves as the VPN customer gateway.

When a cable modem registers with the Cisco uBR7200 series universal broadband router, its IP address is used to identify the subinterface being used by the cable modem; this information is used to associate the Service Identifier (SID) assigned to the modem to that subinterface (and thus the VPN customer network).

Note Cisco IOS Release 12.1(1a)T1 and Release 12.1(3)T do not include Multiprotocol Label Switching (MPLS) support as part of its VPN support on the cable subinterfaces. Cisco IOS Release 12.1(2)T and Release 12.1(5)T and higher releases do support MPLS over VPN.

A subinterface can be created on any cable interface that is not part of a cable interface bundle. A subinterface can also be created on the master cable interface bundle; subinterfaces cannot be created on nonmaster bundles.

Subinterfaces support the following existing cable interface commands:

- **cable arp**
- **cable dhcp-giaddr**
- **cable helper-address**
- **cable ip-broadcast-echo**
- **cable ip-multicast-echo cable proxy-arp**
- **cable source-verify**

Caution Configure an IP address on the master interface only. An attempt to add an interface to a bundle will be rejected if an IP address is configured and the interface is not specified as a master interface.

When bundling cable interfaces, only the interface configured to be the bundle master is allowed to have subinterfaces. An interface that has subinterface(s) defined over it will not be allowed to be part of a bundle.

MIB objects on cable interface bundles are not supported as of the date of this publication.

For more information on cable bundling, refer to the chapter *Understanding System Operations* of the *Cisco uBR7200 Series Software Configuration Guide*.

Caller ID

Caller ID (sometimes called CLID or ICLID for incoming call line identification) is an analog service offered by a Central Office (CO) that supplies calling party information to subscribers. Typically, the calling party number, and sometimes the name, appears on a station (also called extension) device such as a PC telephony software application screen or the display on a telephone. Type 1 Caller ID provides the calling party information while the call is ringing, and Type 2 Caller ID provides the additional convenience of calling number display while the recipient is on another call. In this release, Cisco provides only Type 1 Caller ID support. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/clid_t4.htm

CEF Support for IP Routing Between IEEE 802.1Q VLANs

The CEF Support for IP Routing Between IEEE 802.1Q VLANs feature provides the support needed for a Cisco express forwarding (CEF) feature module.

CEF Switching for Routed Bridge Encapsulation

The CEF Switching for Routed Bridge Encapsulation feature adds Cisco Express Forwarding (CEF) switching support to ATM routed bridge encapsulation (RBE) on the Cisco 3640 series. Before this release, ATM RBE supported only fast switching and process switching. The ATM RBE feature is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtatmrbe.htm

Circuit Interface Description MIB (CSCdp81924)

The Circuit Interface Description MIB feature adds support for a new Cisco enterprise MIB used for monitoring individual circuits using Simple Network Management Protocol (SNMP). The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object that can be used to provide a description of individual circuit-based interfaces (for example, interfaces using ATM or Frame-Relay). This description will then be returned when linkup and linkdown SNMP traps are generated for the described interface.

The Circuit Interface Description MIB consists of a single table, with each row being a sequence of two objects: Circuit Interface Description (cciDescr) and Circuit Interface Status (cciStatus).

The cciDescr object is used to identify circuits using a textual description of up to 255 characters specified by the user (note that MIB objects are modified using network management system (NMS) applications and cannot be configured using the Cisco IOS command-line interface). When the row is created by a user, a value is set for the cciDescr object. The table is indexed by ifIndex from the IF-MIB. The cciStatus is the RowStatus object for the rows in the table.

The cciStatus object can be set to only two values by the user: createAndGo(4), which creates a new row, and destroy(6), which removes an existing row. If the row is created successfully, the cciStatus will be active(1). When creating a new row, the user should set the cciDescr object along with the cciStatus in a single **snmp set pdu** command. If the row is already active, only the cciDescr object can be modified. The other option is to delete the row first by setting the cciStatus to destroy(6) and then recreating the row with a new value for cciDescr. When creating a new row, the ifIndex is validated first. If the ifIndex value is not valid, the row is not created and an error code is returned. Similarly, if an interface is deleted, there was a corresponding row in this table, that row will be deleted automatically.

After a description is created for an interface, the description (the cciDescr object) will be sent along with the other varbinds as part of linkup and linkdown trap notifications.

Cisco AAA Server MIB and Additional Enhancements for the Cisco AS5300 and Cisco AS5800

Addition to show caller Command

The **show caller** command combines the output of the existing call-related show commands. This command displays connection status in summary or in detail. The summary field has been added (summary) to display the total number of calls, including the number of ISDN and analog calls, since the last reload. This summary counter is cumulative of all calls since the Network Access Solutions (NAS) has been up, while other counters indicate the current number of calls in the NAS.

Using the **show caller** command provides the following benefits:

- Displays statistics or debug information for connections using a single command
- Replaces the need to know and use the various show commands
- Provides network management across all Cisco platforms

Cisco AAA Server MIB

This MIB provides statistics that reflect the state of authentication, authorization, and accounting (AAA) server operation within the device and AAA communications with external servers.

The Cisco AAA Server MIB provides the following information:

- Distinct statistics for each AAA function
- Status of servers that provide AAA functions
- Identities of external AAA servers

A server is defined as a logical entity that provides any of the three AAA functions. A TACACS+ server consists of all three functions with a single IP address and single TCP port. A RADIUS server can consist of the authentication/accounting pair with a single IP address but distinct User Datagram Protocol (UDP) ports, or it may be just one of authentication or accounting.

Point-to-Point Password Authentication Protocol Refusal

The new command, **ppp pap refuse**, allows refusal of a peer's request to remote (PPP) authenticate using Password Authentication Protocol (PAP).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_3asmb.htm

Cisco Cable Clock Card Support

When using Cisco IOS Release 12.1(1)T or greater, the Cisco uBR924 Cable Access Router automatically supports the Cisco Cable Clock Card feature for voice traffic when the cable modem termination system (CMTS) is a Cisco uBR7200 series universal broadband router with the Cisco Cable Clock Card feature. This feature can enhance reliability in a voice network and reduce delay and jitter in the voice traffic. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_r_sw/natlclck.htm

Cisco Quality of Service Device Manager 2.0 Support

QoS Device Manager (QDM) is a web-based Java application that enables users to configure and monitor advanced IP-based Quality of Service (QoS) functionality within Cisco routers using a graphical user interface (GUI).

QDM 2.0 is available as a separate product download and is free of charge. If you had QDM installed when you purchased your router, QDM is already installed on your router. Refer to the "QuickStarting QDM 2.0" section in the Installation and Release Notes for Quality of Service Device Manager 2.0 before using the QDM 2.0 application. If you want to install or reinstall QDM, refer to the *Release and Installation Notes for Cisco Quality of Service Device Manager 2.0* on Cisco.com.

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

The Class-Based Ethernet CoS Matching and Marking (801.1p & ISL CoS) feature (which is also called Class-Based Marking or QoS Packet Marking in some Cisco documentation) has been enhanced to include the ability to mark and match Class of Service values and to set the ATM cell lose priority (CLP) bit value on packets.

Associating a packet with a local Class of Service (CoS) value enables users to associate a Layer 2 CoS value with a packet. The value can then be used to classify packets based on user-defined requirements. Layer 2 to Layer 3 mapping can also be configured by matching on the CoS value, because switches already have the capability to match and set CoS values. If a packet that needs to be marked to differentiate user-defined Quality of Service (QoS) services is leaving a router and entering a switch, the router should set the CoS value of the packet, since the switch can process the Layer 2 CoS header marking.

Changing the CLP bit setting in the ATM header of a cell provides a method of controlling the discarding of cells in congested ATM environments. A CLP bit contains two settings: 0 or 1. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0. Before users had the ability to change the CLP bit setting in the ATM header, the CLP bit was automatically set to 0 on packets leaving Cisco routers that were converted into ATM cells for ATM networks. The CLP bit on packets leaving Cisco routers for ATM networks can now be set to 1.

For additional information on class-based packet marking, including information on the new enhancements, refer to the *Class-Based Packet Marking* feature module on Cisco.com.

Class-Based Marking

The Class-Based Packet Marking feature provides users with a user-friendly command-line interface for efficient packet marking by which users can differentiate packets by assigning them different identifying values. The Class-Based Packet Marking feature 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 Type of Service (ToS) byte.
- Associate a local Quality of Service (QoS) group value with a packet.

After setting the IP precedence bits or the IP DSCP, a user can classify a packet based on the IP precedence bit or IP DSCP value. These classifications are then used to apply user-defined differentiated QoS services to the packet.

Associating a packet with a local QoS group allows users to associate a group ID with a packet. The group ID can be used to classify packets into QoS groups based on prefix, autonomous system, and community string.

A user can set up to 8 IP precedence markings, 64 IP DSCP markings, and 100 QoS group markings. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/cbpmark.htm

Class-Based Policer for the DiffServ AF PHB

The Class-Based Policer for the DiffServ AF PHB is based on RFC 2697, *A Single Rate Three Color Marker*. The packet stream is metered, and packets are marked either “conform,” “exceed,” or “violate.” Marking is based on a Committed Information Rate (CIR) and two associated burst sizes, a Committed Burst Size (CBS) and an Excess Burst Size (EBS). A packet is marked “conform” if it does not exceed the CBS; “exceed” if it exceeds the CBS, but not the EBS; and “violate” otherwise.

Class-Based Quality of Service Management Information Base

The Class-Based Quality of Service Management Information Base (Class-Based QoS MIB) provides read access to class-based QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS Command Line Interface (CLI), including information regarding class map and policy map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

Class-Based Shaping

Class-based traffic shaping allows you to control the traffic that leaves an interface in order to match its transmission to the speed of the remote, target interface and to ensure that the traffic conforms to policies contracted for it. Traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

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

- Configure Generic Traffic Shaping (GTS) on a traffic class
- Specify average-rate or peak-rate traffic shaping
- Configure class-based weighted fair queueing (CBWFQ) inside GTS
- Enable class-based shaping on any interface that supports GTS

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/clsbsshp.htm

Closed User Group Selection Facility Suppress Option

A closed user group (CUG) selection facility is a specific encoding element that allows a destination DTE to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 DCE interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA). Refer to the following document for further information:

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

Common Application Programming Interface (CAPI)

The CAPI is an application programming interface standard used to access ISDN equipment connected to BRIs and PRIs. RCAPI is the CAPI feature configured remotely from a PC client.

The framing protocols supported by CAPI include High-Level Data Link Control (HDLC), HDLC inverted, bit transparent (speech), and V.110 synchronous/asynchronous.

CAPI integrates the following data link and network layer protocols:

- Link Access Procedure on the D channel (LAPD) in accordance with Q.921 for X.25 D-channel implementation
- PPP
- ISO 8208 (X.25 DTE-DTE)
- X.25 DCE, T.90NL, and T.30 (fax group 3)

CAPI supports the following features:

- Basic call features, such as call setup and teardown
- Multiple B channels for data and voice connections
- Multiple logical data link connections within a physical connection
- Selection of different services and protocols during connection setup and when answering incoming calls
- Transparent interface for protocols above Layer 3
- One or more BRIs as well as PRI on one or more ISDN adapters
- Multiple applications
- Operating-system-independent messages
- Operating-system-dependent exchange mechanism for optimum operating system integration
- Asynchronous event-driven mechanism, resulting in high throughput
- Well-defined mechanism for manufacturer-specific extensions
- Multiple supplementary services

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_rcapi.htm

Configurable H.225 Timer

In previous Cisco IOS releases, the H.225 TCP connection timeout timer was fixed at 15 seconds. Cisco IOS Release 12.1(2)T adds the ability to configure this timer to a value between 1 and 30 seconds, or to disable it entirely.

Configurable per ATM-VC Hold Queue Size

This feature enables customers to specify the number of packets contained in the hold queue, per virtual circuit (VC), on ATM adapters that support per-VC queueing. By default, the queueing mechanism in use determines the size of the hold queue and, therefore, the number of packets contained in the queue. This feature enables customers to expand the default hold queue size and change (or vary) the number of packets that the queue can contain. With this new feature, the hold queue can contain a maximum of 1024 packets. This feature provides a new command, **vc-hold-queue**, that enables the customer to specify the number of packets contained in the per-VC hold queue. This can be a number from 5 to 1024. Refer to the following document for further information:

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

Configurable Timers in H.225 (CSCdp30190)

The Configurable Timers in H.225 feature allows users to configure the H.255 TCP connection timeout value for all outgoing call attempts (on a per VoIP dial-peer basis).

In previous releases of the Cisco IOS software, the call attempt timeout was 15 seconds and could not be changed. In some cases, however, users might need a shorter timeout value to facilitate a faster fail-over. In other cases, users might need a greater timeout value.

The Configurable Timers in H.225 feature addresses those needs by allowing the user to override the default of 15 seconds and configure the timeout value. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtcfgtim.htm

Configuration Through SNMP (CSCdj10821)

Configuration through Simple Network Management Protocol (SNMP) creates messages that are printed to the console when configuration occurs using SNMP (for example, configuration done from a network management system [NMS]). Previously notifications were only sent to the console when the configuration was changed from the Cisco IOS command-line interface.

Configuring Burst Size in Low Latency Queueing

This feature extends the functionality available with low latency queueing (LLQ). This feature allows customers to specify the Committed Burst (Bc) size in low latency queueing and, therefore, configures the network to accommodate temporary bursts of traffic. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtcfgbst.htm

COPS for RSVP

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices. Resource Reservation Protocol (RSVP) is a means for reserving network resources—primarily bandwidth—to guarantee that applications that transmit across the Internet perform at the desired speed and quality. COPS with RSVP gives network managers centralized monitoring and control of RSVP, including the ability to:

- Refer all RSVP flow requests to an external policy server for processing.
- Accept or reject the flow based on policy decision.
- Communicate information about flows installed on the router to policy servers to aid in management.
- Permit policy servers to remove previously installed flows in order to meet bandwidth or policy requirements.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/copsrsvp.htm

DES/3DES VPN Encryption AIM for 2600/3600

This feature supports the data encryption Advanced Integration Module (AIM) and Network Module (NM) to provide hardware-based encryption for the Cisco 2600 and 3600 series routers. This feature requires both Cisco IOS Release 12.1(3a) XI1, or later, and one of the Cisco IOS feature sets that includes IPSec.

DFP Support in DistributedDirector—Cisco 2501 and Cisco 2502 Only

This protocol allows the user to configure the DistributedDirector to communicate with various Dynamic Feedback Protocol (DFP) agents. The DistributedDirector tells the DFP agents how often they should report load information; then the DFP agents can tell the DistributedDirector which LocalDirector cluster to remove from providing service.

Dial-on-Demand Authentication Enhancements (CSCdp96375)

The following enhancements to dial-on-demand authentication are provided with this feature:

- The Network Access Solutions (NAS) IP address plus a configured suffix can be sent to the RADIUS server as a username for authentication.
- A password other than the default password “cisco” can be sent to the RADIUS server for authentication.
- The username for two-way authentication will specified by a new vendor-specific attribute (VSA), “outbound:send-name=<string>”.

This feature also introduces modifications to the **dialer aaa** command, which provides username configuration capability for dial-on-demand. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt3.htm

Dial Peer Enhancements

The dial peer configuration enhancements were previously implemented in 12.1(1)T for Voice over IP on several platforms. In the 12.1(2)T release, these same enhancements are now supported on additional platforms for Voice over Frame Relay and Voice over ATM. In addition, these enhancements are now supported on the Cisco MC3810 for Voice over IP. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt0390s7.htm

DiffServ Compliant Weighted Random Early Detection

This feature 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 WRED to be compliant with the DiffServ standard and the AF PHB standard being developed by the Internet Engineering Task Force (IETF). This feature enables customers to implement AF PHB by coloring packets according to Differentiated Services Code Point (DSCP) values and then assigning preferential drop probabilities to those packets. This feature adds two new commands, **random-detect dscp** and **dscp**. It also adds two new arguments, *dscp-based* and *prec-based*, to two existing WRED-related commands—the **random-detect** (interface) command and the **random-detect-group** command. Refer to the following document for further information:

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

Distributed Traffic Shaping

The Distributed Traffic Shaping feature is one element used to manage the bandwidth of an interface to avoid congestion, to meet remote site requirements, and to conform to a service rate that is provided on that interface.

Distributed Traffic Shaping (DTS) uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate. This ensures that traffic behaves according to the configured descriptor, as defined by command information rate (CIR), Committed Burst (Bc), and Excess Burst (Be). With the defined average bit rate and burst size that is acceptable on that shaped entity, you can derive a time interval value.

DTS provides two types of shape commands: average and peak. When shape average is configured, the interface sends no more than the Bc for each interval, achieving an average rate no higher than the CIR. When shape peak is configured, the interface sends Bc plus Be bits in each interval.

In a link layer network such as Frame Relay, the network sends messages with the forward explicit congestion notification (FECN) or backwards explicit congestion notification (BECN) if there is congestion. With the DTS feature, the traffic shaping adaptive mode takes advantage of these signals and adjusts the traffic descriptors. This approximates the rate to the available bandwidth along the path.

For additional information on Distributed Traffic Shaping, refer to the *Distributed Traffic Shaping* feature module on Cisco.com.

Restrictions:

Hierarchical DTS (that is, DTS configured in both a parent-level policy and a child-level policy) is not supported on subinterfaces.

DistributedDirector Enhancements

The DistributedDirector Enhancements feature sends event information to the Cisco IOS syslog. Refer to the following document for further information:

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

DOCSIS 1.0+ Extensions

In addition to the other quality of service (QoS) features, DOCSIS 1.1 supports a number of features that are required for the delivery of high-quality voice traffic. To use these features before the DOCSIS 1.1 specification is finalized, Cisco has created the DOCSIS 1.0+ extensions that contain the most important of these features:

- Concatenation—Data-over-Cable Service Interface Specifications (DOCSIS) concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. Using concatenation, a DOCSIS cable modem makes only one bandwidth request for multiple packets, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for bursty real-time traffic, such as voice calls.
- Dynamic Multi-SID Assignment—To give priority to voice traffic, the Cisco uBR924 router assigns a different service identifier (SID) to each voice port. Without the DOCSIS 1.0+ extensions, the router creates these SIDs during the provisioning process, and the SIDs remain in effect until the router is rebooted with a different configuration. As part of this process, a minimum guaranteed bandwidth is permanently allocated to the voice ports; this bandwidth is reserved to the voice ports even if no calls are being made.

  To avoid potentially wasting bandwidth in this manner, the DOCSIS 1.0+ extensions support the dynamic creation of multiple SIDs. New MAC messages dynamically add, delete, and modify SIDs when needed. When a phone connected to the router is taken off-hook, the Cisco uBR924 router creates a SID that has the QoS parameters needed for that particular voice call. When the call terminates, the router deletes the SID, releasing its bandwidth for use elsewhere.

The DOCSIS 1.0+ features are introduced in Cisco IOS Release 12.0(7)XR and 12.1(1)T.

Note Both the Cisco uBR924 Cable Access Router and the cable modem termination system (CMTS) must support the dynamic multi-SID and concatenation features in order for them to be used on the cable network. If you are using the Cisco uBR7200 series universal broadband router as the CMTS, Cisco IOS Release 12.0(7)XR or 12.1(1)T (or later) is required on both the Cisco uBR924 and Cisco uBR7200 series routers to use these features.

DOCSIS Quality of Service Enhancements

A number of data-over-cable service interface specifications (DOCSIS) quality of service (QoS) enhancements have been added to Cisco IOS Release 12.1(1a)T1; these features parallel some of those that are expected in the DOCSIS 1.1 specification when it is finalized.

Note These QoS enhancements are in addition to the currently existing QoS traffic shaping and tiered best effort features.

- Concatenation Support—DOCSIS concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, as well as increase transmission efficiency. Using concatenation, a DOCSIS cable modem needs to make only one bandwidth request for a concatenated packet, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for bursty real-time traffic, such as voice calls.

  Concatenation is enabled by default for current cable modem cards (see the "Cable Modem Cards" section on page 79), but can be disabled with the Cisco IOS **no cable upstream** *number* **concatenation** interface command. The **show controller** command displays whether concatenation is enabled on an interface.

  Note Concatenation is supported only with cable modems that support DOCSIS concatenation.

- Embedded Client Signaling (dynamic SIDs)—DOCSIS supports the dynamic creation, configuration, and deletion of Service Identifiers (SIDs) to accommodate different classes of service. This allows cable modems to request high-priority or high-bandwidth data streams as needed, such as when a VoIP call is made.

  Note Dynamic SIDs can be used only with cable modems that also support this feature. Otherwise, cable modems must use the static SIDs supported in previous releases.

- IP Precedence-Based Rate Limiting—In addition to the currently supported traffic shaping techniques, Cisco IOS Release 12.1(1a)T1 supports a new configuration field that associates a maximum bandwidth (in kbps) with a particular setting of the IP type of service (ToS) bits. This can be used to ensure that certain traffic, such as data, does not exceed a preset rate limit and thereby interfere with higher-priority real-time traffic, such as VoIP calls.
- Support for Unsolicited Grants—New fields in the DOCSIS configuration file can be used so that when a cable modem requests a voice or fax SID, the MAC scheduler on the Cisco uBR7200 series router schedules fixed periodic slots on the upstream for that traffic flow. The cable modem does not

have to contend for these slots, and because the Cisco uBR7200 series router controls the timing of the slots, it has a very precise control over potential delay and jitter. This provides a Constant Bit Rate (CBR) traffic flow for real-time traffic such as voice and fax calls.

In addition, the Cisco uBR7200 series router can create QoS profiles for G.711 fax traffic and G.729 voice traffic. These profiles can be customized with the scheduling parameters required for the G.711 and G.729 codecs being used at the subscriber's site.

Dynamic Host Configuration Protocol Proxy Support

The Dynamic Host Configuration Protocol Proxy Support feature helps to automate the configuration of the Cisco uBR924 Cable Access Router in two situations:

- When the Cisco uBR924 Cable Access Router is configured for routing mode, an IP address must be assigned to its Ethernet interface. Dynamic Host Configuration Protocol (DHCP) proxy support allows an external DHCP server to assign an IP address to the Ethernet interface, as opposed to having to assign it manually with the appropriate Command Line Interface (CLI) commands.
- When network address translation (NAT) is used, an inside global address pool must be created on the Ethernet interface. The DHCP Proxy Support feature allows a DHCP server to assign an IP address that automatically creates the NAT address pool, as opposed to manually specifying a static IP address with the appropriate CLI commands.

When configured for DHCP proxy support, during startup the Cisco uBR924 Cable Access Router sends a proxy DHCP request to the DHCP server using the Ethernet interface's MAC address. The DHCP server replies with a second IP address that the router assigns to either the Ethernet interface or the NAT pool, depending on which option was specified. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_dhcpc.htm

Dynamic Mobile Hosts

This feature addresses a security hole that occurs when the Cisco uBR7200 router supports mobile hosts. (Mobile host are hosts that can move from one modem to another modem.) Anyone who knows the MAC address of a mobile host can "fake" the mobile host, thereby causing denial of access for the real mobile host.

To avoid this security hole, the Dynamic Mobile Hosts feature pings the mobile host on the old service identifier (SID) to verify that the host has indeed been moved.

Ecosystem Gatekeeper Interoperability Enhancements (CSCdp48320)

The Ecosystem Gatekeeper Interoperability Enhancements feature allows gateways to move between gatekeepers without requiring a reconfiguration of the gateway or a gatekeeper failover in the gateway.

Gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs. If an outage occurs and gateways move from one gatekeeper to another, there may be an imbalance in the number of gateways registered to each gatekeeper. The Ecosystem Gatekeeper Interoperability Enhancements feature helps to restore the balance (when the outage has been corrected) by allowing some of the gateways to be moved back to their proper gatekeepers.

The Ecosystem Gatekeeper Interoperability Enhancements feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection (GRJ) and registration rejection (RRJ) messages. This allows a gateway to move between gatekeepers during the gatekeeper request (GRQ) and registration request (RRQ) phases. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtarjrrj.htm

Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 (CSCdp70719)

The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection (ARJ). This allows a gateway to move between gatekeepers during the admission request (ARQ) phase.

The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 feature allows gateways to move between gatekeepers without requiring a reconfiguration of the gateway or a gatekeeper failover in the gateway.

Gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs. If an outage occurs and gateways move from one gatekeeper to another, there may be an imbalance in the number of gateways registered to each gatekeeper. The Ecosystem Gatekeeper Interoperability Enhancements: Phase 2 feature helps to restore the balance (when the outage has been corrected) by allowing some of the gateways to be moved back to their proper gatekeepers. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtgkarj.htm

Enhanced Modem Status Display

The Cisco uBR7200 series universal broadband router supports polling of the cable modems to obtain parameter and status information on an ongoing basis. Two new Cisco IOS commands are added to support this feature. The **cable modem remote** command configures the router for the polling interval; the **no** version of this command disables the status polling. The **show cable modem remote-query** command displays the collected information:

- Downstream receive power level
- Downstream signal/noise ratio (SNR)
- Upstream power level
- Transmit timing offset
- Micro reflection (in dB)

Enhanced Per Modem Error Counter

The Cisco uBR7200 series supports display of per modem error counters. The following new command is introduced:

show cable modem [*ip-addr* | *mac-addr*] **errors**

Sample display:

```
cmts# show cable modem errors

MAC Address    SID   I/F          CRC        HCS
00d0.ba26.eee7 1     Cable4/0/U0  0          0
```

Note Both cyclic redundancy check (CRC) and header check sum (HCS) are on a per Campus Manager (CM) basis.

The cable modem termination system (CMTS) maintains the above error counters to begin to populate the MIB objects that pertain to RFC 2670:

- docsIfCmtsCmStatusUnerroreds
- docsIfCmtsCmStatusCorrecteds
- docsIfCmtsCmStatusUncorrectables
- docsIfCmtsCmStatusSignalNoise
- docsIfCmtsCmStatusMicroreflections

This saves administrators from having to poll the “docsIfSignalQualit” table on every cable modem. With the CMTS maintaining error counters, along with the above table and entries in place, administrators can poll the CMTS, rather than all CMs—providing a more scalable network management model.

Enhanced Voice Services

For the Cisco 800 Series

The Enhanced Voice Services features consist of the following voice capabilities for the Cisco 800 series routers:

- **Call Blocking on Caller ID**

  Allows Cisco 800 series routers to reject an incoming voice call based on local directory number (LDN) caller IDs. Using the command-line interface (CLI), you can configure blocking for up to ten caller ID numbers for each LDN.

- **Local Call Waiting**

  Notifies you with a call-waiting tone of an incoming call while you are already connected to a telephone call. You can place the first call on hold by pressing the on-and-off-hook button (flash), connect to the second call, and then return to the first call after finishing with the second.

  The feature uses both B channels of the ISDN line, enabling local call-waiting support on the router. Unlike standard ISDN call waiting, local call waiting does not require a subscription to call waiting from a service provider.

For the Cisco 813 Only

The Enhanced Voice Services features consist of the following voice capabilities for the Cisco 813 series routers *only*:

- **Caller ID—Available in Japan only.**

  Provides analog caller ID support for Japanese-language display, caller-ID-equipped, analog telephones. The Cisco 800 series router receives the caller ID information from the INS-NET-64 switch. The router software prepares the caller ID with a tone, transmits the caller ID to plain old telephone service (POTS) port 1 or 2 on the router, and displays the caller ID on the telephone.

- **E Ya Yo—Available in Japan only.**

  Conceals the caller ID of the outgoing call from the receiving device. To activate the feature, dial 184 before dialing the number of the receiving device, as specified in the Nippon Telegraph and Telephone (NTT) Communications Corporation user manual. This feature is specific to NTT Communications Corporation switches and is offered free of charge. The router handles this feature as a regular outgoing call and requires no special operation.

- **Voice Warp—Available in Japan only.**

On the INS-NET-64 switch, this feature forwards all incoming calls for a terminal device to another device. Voice-warp registration, activation, and deactivation requests are sent to the switch for each LDN. The routers support the registration, activation, and deactivation requests for devices attached to (POTS) port 1 or 2. The forwarding function itself is performed by the INS-NET-64 switch. This feature can be deactivated after its registration and activation phases.

During the registration phase of the device, you can:

- Create a list of forwarding destination numbers and select one as the active destination.
- Specify whether an announcement is made to the caller, to the forwarding device, or both, when the call is forwarded.
- Set the no-answer timer parameter from 5 to 60 seconds at 5-second intervals. This setting affects the redirection of calls when the voice-warp feature is activated.

- **Voice Select Warp—Available in Japan only.**

  This feature is a superset of the Voice Warp feature. You create a list of incoming caller IDs for the Voice Select Warp feature. This list of caller IDs could be used in two different ways. First, an incoming call that bears the caller ID in this list will be redirected. Second, an incoming call that does not bear the caller ID in this list will be redirected. You can also choose to ignore this list altogether. If so, this is effectively the same as the Voice Warp feature for all incoming calls. All other characteristics and limitations remain the same as the Voice Warp feature.

  For all the operations described above, users can use the keypad dialing sequence as specified in the NTT user manual.

- **Nariwake—Available in Japan only.**

  The Nariwake feature requires the user to be subscribed to the NTT service.

  This feature allows the user to register multiple caller ID numbers with the ISDN (NTT INS-NET-64) switch based on the router's local directory numbers. When calls are presented to the NTT switch with a caller ID identified on the list of registered numbers, the NTT switch will notify the router that it should provide a distinctive ring to its telephone port, to which the local directory number just called will be routed.

  Three different ring cadences are available, so the user may choose two of them for each of the following two cases: when calls from registered callers are received and when calls from unregistered callers are received. The default ring cadence setting for unregistered callers is ring 0, while for registered callers it is ring 1. The on/off period of ring 0 (normal ringing signals) and ring 1 (ringing signals for Nariwake service) is defined in the NTT user's manual.

  The number of caller IDs that can be registered at a time is up to a limit defined by the NTT switch. The list of caller ID numbers shall be entered/removed through the keypad.

- **Trouble Call Blocking—Available in Japan only.**

  This feature requires the user to be subscribed to the NTT service troublesome call refusing as described in the NTT user's manual. This feature is also described as nuisance telephone call refusal service by INS Net.

  Trouble call blocking causes all incoming calls to a particular number of User A from the troublesome caller's (User B) number to be rejected by the network. This is done without User A having to specify User B's actual phone number. After User A has activated the feature, future calls to User A made by User B will result in the caller hearing an announcement. User A will not be notified of User B's attempts of incoming calls.

  Multiple numbers can be blocked at a time up to a limit as defined when the service is provisioned. If the user requests an additional number to be blocked beyond the limit, the oldest number is discarded (unblocked) first and the new telephone number will be registered.

- **I Number—Available in Japan only.**

  The I Number feature allows several terminal devices to be used with one subscriber line. In addition to the subscriber's number, numbers for each port of the router are given by the service provider. When any of the assigned numbers is dialed, the call will come through the same subscriber's line and only the corresponding terminal device(s) attached to that port will ring.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtkat800.htm

Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms

Enhancements to the Session Initiation Protocol (SIP) for voice over IP (VoIP) on Cisco Access Platforms enhancements include:

- Configurable in-band alerting.
- Ability to specify the maximum number of SIP redirects.
- Ability to specify SIP or H.323 on a dial-peer basis.
- Configurable SIP message timers and retries.
- Interoperability with unified call services (UCS).
- Support for a variety of signaling protocols, including ISDN, PRI, and channel associated signaling (CAS).
- Support for a variety of interfaces, including
  - Analog interfaces: FXS/FXO/E&M analog interfaces.
  - Digital interfaces: T1 CAS and E1 CAS.
- Support for SIP redirection messages and interaction with SIP proxies. The gateway can redirect an unanswered call to another SIP gateway or SIP-enabled IP phone. In addition, the gateway supports proxy-routed calls.
- Interoperability with Domain Name Service (DNS) servers including support for DNS server (SRV) and "A" records to look up SIP URLs.
- Support for SIP over TCP and User Datagram Protocol (UDP) network protocols.
- Support Real-Time Transport Protocol/ Real-Time Transport Control Protocol (RTP/RTCP) for media transport in VoIP networks.
- Support for the following codecs:

Codec	SDP
G711ulaw	0
G711alaw	8
G723r63	4
G726r16	2
G728	15
G729r8	18

- Support for Record-Route headers.
- Support for IP quality of service (QoS) and IP precedence.

- Support for IP Security (IPSec) for SIP signaling messages.
- Authentication, authorization, and accounting (AAA) support. For accounting, the gateway device generates call data record (CDR) accounting records for export. For authentication, the SIP gateway sends validate requests to the AAA server. For authorization, the existing access lists are used.
- Support for call hold and call transfer features. The call hold sends a mid-call INVITE message, which requests that the remote endpoint stop sending media streams. The call transfer is done without consultation. This is called a blind transfer. The transfer can be initiated by a remote SIP endpoint.
- Support for configurable expiration time for SIP INVITEs and maximum number of proxies or redirect servers that can forward a SIP request.
- Expanded support for the mapping of Public Switched Telephone Network (PSTN) cause codes to SIP events.
- Ability to hide the calling party's identity based on the setting of the ISDN presentation indicator.

Event MIB

The Event MIB is an asynchronous notification mechanism standardized for use by network management systems using Simple Network Management Protocol (SNMP). The Event MIB provides the ability to monitor MIB objects on a local or remote system using SNMP and to initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified). By allowing notifications based on events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed.

When combined with the Expression MIB support introduced in Cisco IOS Release 12.0(5)T, Event MIB support in Cisco IOS software provides a flexible and efficient way to monitor complex conditions on network devices. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtevent.htm

Express Real-Time Transport Protocol and TCP Header Compression (CRTP)

As of Cisco IOS Release 12.0(7)T, if TCP or RTP header compression is enabled, it occurs by default in the fast-switched path or the Cisco Express Forwarding-switched (CEF-switched) path, depending on which switching method is enabled on the interface. Furthermore, the number of TCP and RTP header compression connections is increased to 1000 connections each.

Before this feature, such compression was performed in the process-switching path. That meant that packets traversing interfaces that had TCP or RTP header compression enabled were queued and passed up to the process to be switched. This procedure slowed down transmission of the packet, and therefore, some users preferred to fast switch uncompressed TCP and RTP packets.

Expression MIB Support of Delta, Wildcarding, and Aggregation

This feature adds support of the Delta, Wildcarding, and Aggregation features in the Distributed Management Expression MIB (EXPRESSION-MIB) to Cisco IOS software for use by Simple Network Management Protocol (SNMP).

The Delta function enables the Expression MIB to use Delta values of an object instead of absolute values when evaluating an expression. Delta is obtained by taking the difference between the current value of an object and its previous value.

The Wildcarding function of the Expression MIB allows evaluation of multiple instances of an object. This is useful in cases in which an expression needs to be applied to all instances of an object. You do not need not individually specify all instances of an object in the expression. Rather, you only need to set the expWildcardedObject in expObjectTable to TRUE for the respective object.

Aggregation is performed using the sum function in the Expression MIB. The operand to the sum function must be a wildcarded object. The result of the sum function is the sum of values of all instances of the wildcarded object.

For a complete description of Expression MIB functionality, refer to the *Distributed Management Expression MIB* Internet-Draft document, available through the ITEF at http://www.ietf.org/ids.by.wg/disman.html.

FastEther Channel Enhancements on Cisco 7200 Series Routers

The FastEther Channel feature provides higher bidirectional bandwidth, redundancy, and load sharing. Up to four Fast Ethernet interfaces can be bundled in a port channel, and the router or switch can support up to four port-channels. The FastEther Channel feature is capable of load balancing traffic across the Fast Ethernet links. Unicast, broadcast, and multicast traffic is distributed across the links, providing higher performance and redundant parallel paths. In the event of a link failure, traffic is redirected to remaining links within the FastEther channel without user intervention.

In this release of the FastEther Channel feature, IP traffic is distributed over the port-channel interface while traffic from other routing protocols is sent over a single link. Bridged traffic is distributed based on the Layer 3 information in the packet. If the Layer 3 information does not exist in the packet, the traffic is sent over the first link.

FastEther Channel supports all features that are currently supported on the Fast Ethernet interface. You must configure these features on the port-channel interface rather than on the individual Fast Ethernet interfaces. FastEther channel connections are fully compatible with Cisco IOS virtual VLAN and routing technologies. The Inter-Switch Link (ISL) VLAN trunking protocol can carry multiple VLANs across a FastEther channel, and routers attached to FastEther channel links can provide full multiprotocol routing with support for host standby using Host Standby Router Protocol (HSRP).

The port channel (consisting of up to four Fast Ethernet interfaces) is treated as a single interface. Port channel is used in Cisco IOS software to maintain compatibility with existing commands on the Catalyst 5000 switch. You create the FastEther channel by using the **interface port-channel** interface configuration command. You can assign up to four Fast Ethernet interfaces to a port channel by using the **channel-group** interface configuration command. Refer to the following document for further information:

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

Fax Relay Packet Loss Concealment

This feature improves the current real-time fax over IP (known as fax relay) implementation in Cisco gateways so that fax transmissions work reliably over higher packet-loss conditions.

This feature also includes enhanced real-time fax debugging capabilities and statistics. These features give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.

These improvements include configuration of fax relay ECM (Error Correction Mode) on the voice over IP (VoIP) dial peer. ECM provides for error-free page transmission. This mode is available on fax machines that include memory for storage of the page data (usually high-end fax machines). Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_0393.htm

Feature Group D Support on Digital T1/E1 Packet Voice Trunk Network Modules

This feature adds Feature Group D support on digital T1/E1 packet voice trunk network modules.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_fgd.htm

Firewall Enhancements

Cisco IOS Release 12.1(1a)T1 enhances the previous Cisco IOS Secure Integrated Software feature set with the following set of features:

- Context-Based Access Control (CBAC) that intelligently filters TCP and User Datagram Protocol (UDP) packets based on the application-layer protocol. This includes Java applets, which can be blocked completely or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks, such as Internet Control Message Protocol (ICMP) and UDP echo packet flooding, synchronize/start (SYN) packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.
- Dynamic port mapping that maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Configurable alerts and audit trail.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For detailed information, refer to the *Cisco IOS Firewall Feature Set* documentation set, as well as the sections on traffic filtering and firewalls in the Cisco IOS Security Configuration Guide and *Cisco IOS Security Command Reference* (available on Cisco.com).

Frame Relay ELMI Address Registration

The Frame Relay ELMI Address Registration feature enables a network management system (NMS) to detect connectivity among the switches and routers in a network using the Enhanced Local Management Interface (ELMI) protocol. During ELMI version negotiation, neighboring devices exchange their management IP addresses and ifIndex. The NMS polls the devices to collect this connectivity information.

Before this feature was introduced, NMS could detect only the topology of routers or the topology of switches. The NMS could not detect router and switch interconnection and was therefore unable to create a complete topology of the network. With the Frame Relay ELMI Address Registration feature, the NMS can detect switch and router interconnection and create an end-to-end network topology map for network administrators.

The Cisco Frame Relay MIB has been enhanced to support the new ELMI information. The NMS uses the MIB to extract the IP address and ifIndex of devices neighboring the managed device.

Note The ELMI address registration mechanism does not check for duplicate or illegal addresses.

ELMI address registration takes place on all interfaces on which ELMI is enabled, even if all the interfaces are connected to the same router or switch. The router periodically sends a version inquiry message with version information, the management IP address, and the ifIndex to the switch. The switch sends its management IP address and ifIndex using the version status message. When the management IP address of the switch changes, an asynchronous ELMI version status message is sent to the neighboring device immediately.

When ELMI is enabled, the router automatically chooses the IP address of one of the interfaces to use for ELMI address registration purposes. The router will choose the IP address of an Ethernet interface first, and then of serial and other interfaces. You have the option to use the IP address chosen by the router or to disable the autoaddress mechanism and configure the management IP address yourself. You can also choose to disable ELMI address registration on a specific interface or on all interfaces. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtfripar.htm

Frame Relay Fragmentation with Hardware Compression

The Frame Relay Fragmentation with Hardware Compression feature introduces the following functionality:

Frame Relay Fragmentation and Hardware Compression Interoperability

This new feature enables FRF.12, FRF.11 Annex C, and Cisco proprietary fragmentation to work with hardware compression on interfaces and virtual circuits (VCs) using Cisco proprietary or Internet Engineering Task Force (IETF) encapsulation types.

Hardware Compression and Header Compression Interoperability

The Frame Relay Fragmentation with Hardware Compression feature introduces a new, proprietary hardware and software compression protocol called data-stream compression, which can be used on the same VC or interface as header compression. Data-stream compression is functionally equivalent to FRF.9 compression and must be used with Cisco proprietary encapsulation. Frame Relay fragmentation can also be enabled.

Hardware Compression and Software Compression Interoperability

The Frame Relay Fragmentation with Hardware Compression feature provides hardware and software compression interoperability when hardware compression is configured on one side of the link and software compression is configured on the other side.

Refer to the following document for further information:

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

Frame Relay PVC Interface Priority Queueing

The FR PIPQ feature provides an interface-level priority queueing scheme in which prioritization is based on destination permanent virtual circuit (PVC) rather than packet contents. For example, FR PIPQ allows you to configure a PVC transporting voice traffic to have absolute priority over a PVC transporting signaling traffic, and a PVC transporting signaling traffic to have absolute priority over a PVC transporting data.

FR PIPQ provides four levels of priority: high, medium, normal, and low. The Frame Relay packet is examined at the interface for the data-link connection identifier (DLCI) value. The packet is then sent to the correct priority queue based on the priority level configured for that DLCI.

Frame Relay Support

Frame Relay provides a packet-switching data communications capability that is used across the interface between user devices, such as the Cisco uBR7200 series universal broadband Routers, and network equipment (switching nodes). As an interface between user and network equipment, Frame Relay provides a means for statistically multiplexing many logical data conversations (virtual circuits) over a single physical transmission link. A Frame Relay service may support permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). The Cisco uBR7200 series universal broadband Routers support PVCs only.

Frame Relay features include the following:

- Cisco and IETF encapsulation
- Cisco, ANSI, and ITU LMI with autosensing
- UNI DTE, DCE, and NNI
- Inverse ARP
- Traffic shaping
- Adaptive shaping using BECN
- Broadcast Queue
- CDP over FR
- TCP/IP header compression
- RTP header compression
- Cisco and IETF MIBs
- Syslog trap alert for DLCI loss
- Weighted Fair Queuing at the interface level based on DLCI classification
- DLCI IP RTP priority support

Frame Relay Switching Diagnostics and Troubleshooting

The Frame Relay Switching Diagnostics and Troubleshooting feature enhances Frame Relay switching functionality by providing tools to diagnose problems in switched Frame Relay networks. The **show frame-relay pvc** command has been enhanced to display detailed reasons why packets were dropped from switched permanent virtual circuits (PVCs). The command also displays the local status, the Network-to-Network Inter face (NNI) status, and the overall status of NNI PVCs. If a network problem is observed, the new **debug frame-relay switching** command can be used to display the status of packets

on switched PVCs at regular intervals. This new debug command displays information such as the number of packets that were switched, why packets were dropped, and changes in status of physical links and PVCs. Refer to the following document for further information:

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

Frame Relay Switching Enhancements

The Frame Relay Switching Enhancements feature enables a router in a Frame Relay network to be used as a Frame Relay switch. This feature includes the following Frame Relay switching enhancements:

- Traffic Shaping on Switched PVCs
- Frame Relay Switching over ISDN B Channels
- Traffic Policing on UNI DCE
- Congestion Management on Switched PVCs

Before the Frame Relay Switching Enhancements feature was introduced, routers had limited Frame Relay switching functionality. With this feature, a router acting as a virtual Frame Relay switch can be configured to do the following:

- Apply Frame Relay traffic shaping functionality to switched PVCs, enabling the router to act as a Frame Relay port concentrator.
- Support ISDN interfaces in addition to serial interfaces.
- Discard switched packets with the DE bit set when there is network congestion.
- Police incoming traffic to ensure adherence to service contracts.
- Set the Forward/Backward Explicit Congestion Notification (FECN/BECN) bits in switched packets when there is network congestion.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtfrswen.htm

FXO Supervisory Disconnect Tone

If the FXO Supervisory Disconnect Tone feature is configured and a detectable tone from the public switched telephone network (PSTN) or PBX is detected by the digital signal processor (DSP), the analog Foreign Exchange Office (FXO) port goes on-hook. This feature prevents an analog FXO port from remaining in an off-hook state after an incoming call is ended. You can configure a voice port to detect either of the following tone types:

- Disconnect tones from the PBX or PSTN—You can configure the FXO Supervisory Disconnect Tone feature to function in either of the following ways:
  - Continuously throughout the call duration
  - Before a call is answered

As part of the tone detection process by the DSP, a DSP event is reported to the host software.

- Any tone received from the PBX or PSTN

Detection of any tone is effective only during call setup (before a call is answered), and echo cancellation must be enabled to prevent disconnection due to detection of the route's own ringback tone.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_fxodt.htm

Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism feature expands the capability that is provided by the Redundant H.323 Zone Support feature. With the Redundant H.323 Zone Support feature, the location request (LRQs) are sent simultaneously (in a "blast" fashion) to all of the gatekeepers in the list. The gateway registers with the gatekeeper that responds first. Then, if that gatekeeper becomes unavailable, the gateway registers with another gatekeeper from the list.

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism feature enhances this capability by allowing the user to choose whether the LRQs are sent simultaneously or sequentially (one-at-a-time) to the remote gatekeepers in the list. If the LRQs are sent sequentially, a delay is inserted after the first LRQ and before the next LRQ is sent. This delay allows the first gatekeeper to respond before the LRQ is sent to the next gatekeeper. The order in which LRQs are sent to the gatekeepers is based on the order in which the gatekeepers are listed (using either the **zone prefix** or the **gw-type-prefix** command). Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtseqlrq.htm

Gateway-to-Gatekeeper Billing Redundancy

The Gateway-to-Gatekeeper Billing Redundancy feature enhances the accounting capabilities of the Cisco H.323 gateway and provides support for Vocaltec gatekeepers. The Gateway-to-Gatekeeper Billing Redundancy feature provides redundant billing information to an alternate gatekeeper if the primary gatekeeper to which a gateway is registered becomes unavailable.

During the process of establishing a call, the primary gatekeeper sends an admission confirmation (ACF) message to the registered gateway. The ACF message includes the user's billing information and an access token. To provide the billing information to an alternate gatekeeper if the primary gatekeeper is unavailable when the call session ends, the access token information sent in the ACF message in now also included in the disengage request (DRQ) message that is sent to the alternate gatekeeper.

This features enables the alternate gatekeeper to obtain the billing information required to successfully complete the transaction. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/gwgkbill.htm

General Packet Radio Service Release 1.4

Note General Packet Radio Service (GPRS) Release 1.4 is a specially licensed feature that is available only through a controlled image release in Cisco IOS Release 12.1(3)T. GPRS Release 1.4 is the recommended upgrade for both GPRS Release 1.2 (available in Cisco IOS Release 12.1(1)GA) and GPRS Release 1.3 (available in Cisco IOS Release 12.1(2)GB). For more information about acquiring GPRS Release 1.4, contact your Cisco sales representative. Customer documentation for GPRS Release 1.4 is available on Cisco.com.

GPRS is defined and standardized by the European standards body ETSI. GPRS is an IP packet-based data service for global system for mobile (GSM) networks. The GPRS network essentially consists of two major elements, the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN).

The GGSN is a wireless gateway that allows mobile cellular phone users to access the public data network (PDN) or specified private IP networks. User sessions are connected from a mobile station through a device called a Base Station Subsystem (BSS) and then to an SGSN.

The connection between the SGSN and the GGSN is enabled through a protocol called the GPRS Tunneling Protocol (GTP). Finally, the connection between the GGSN and the PDN is enabled through IP.

In order to assign mobile user sessions an IP address, the GGSN uses the Dynamic Host Configuration Protocol (DHCP). To authorize and authenticate the remote users, the GGSN can use a RADIUS server. DHCP and RADIUS services can be specified for the global configuration, using GPRS DHCP and RADIUS commands, or for each access point configured for the GGSN. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_fxodt.htm

H.323 Enhancements

Cisco IOS Release 12.2 adds a number of H.323v2 features for voice support:

- Fast Connect—This H.323v2 feature allows connections for the most common types of calls to be created without establishing a separate H.245 control channel.
- H.245 Tunneling—Supports two H.245 features during a call without having to establish an H.245 channel:
  - DTMF digit relay—Dual-tone multifrequency (DTMF) tones are often used during a voice call to convey information, such as entering the account number voice-mail commands. Certain forms of compression (such as G.729 and G.723.1) might interfere with these tones, so they must be transmitted “out of band,” separated from the encoded voice stream.
  - Hookflash relay—Many types of PBX and telephone switches give a special meaning to a hookflash (quickly depressing and releasing the hook on your telephone). Because this creates a voltage change that cannot be transmitted across an IP network, the H.323 protocol can send an H.245 User Input Indication message to convey the hookflash to the remote end.

H.323 Support for Virtual Interfaces

The H.323 Support for Virtual Interfaces feature allows users to configure the IP address of the gateway, so that the IP address included in the H.323 packet is deterministic and consistently indicates the same address for the source.

In previous releases of the Cisco IOS software, the source address included in the H.323 packet could vary depending on the protocol (RAS, H.225, H.245, or RTP). This makes it difficult to configure firewall applications to work with H.323 messages.

The H.323 Support for Virtual Interfaces feature addresses that difficulty by allowing the user to explicitly configure an IP address to be used for all protocols. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt323bnd.htm

H.323 Version 2, Phase 2 Enhancements

Cisco H.323 Version 2 Phase 2 enhancements upgrade several optional features of the H.323 Version 2 specification and facilitate customized extensions to the Cisco gatekeeper.

- H.323v2 Fast Connect—The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing before endpoint connections can be established.

- H.245 Tunneling—Through H.245 tunneling, H.245 messages are encapsulated within Q.931 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any Q.931 message. H.245 tunneling is not supported as a stand-alone feature; initiation of H.245 tunneling procedures can be initiated only by using the **dtmf-relay** command, and only from an active Fast Connect call. Furthermore, if the **dtmf-relay** command is configured on a Version 2 voice over IP (VoIP) dial peer and the active call has been established by using Fast Connect, tunneling procedures initiated by the opposite endpoint are accepted and supported.

  H.245 tunneling is backward compatible with H.323 Version 1 configurations.

- H.450.2 Call Transfer—Call Transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco gateways support H.450.2 Call Transfer as the transferred and transferred-to party. The transferring endpoint must be an H.450-capable terminal; the Cisco gateway cannot act as the transferring endpoint. Gatekeeper-controlled or gatekeeper-initiated Call Transfer is not supported.

Note Certain devices are limited in their support of H.450. The Cisco 1700 and uBR820 platforms do not support Interactive Voice Response (IVR). Therefore, these platforms are not able to act as H.450 transferring endpoints.

- H.450.3 Call Deflection—Call Deflection is a feature under H.450.3 Call Diversion (Call Forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 Call Deflection as the originating, deflecting, and deflected-to gateway. The Cisco gateway as the deflecting gateway will support invocation of Call Deflection only by using an incoming PRI QSIG message (a Call Deflection cannot be invoked by using any other trunk type).
- Hookflash Relay—A “hookflash” indication is a brief on-hook condition during a call. The indication is not long enough in duration to be interpreted as a signal to disconnect the call. You can create a hookflash indication by quickly depressing and releasing the hook on your telephone.
- H.235 Security—Security for Registration, Admission, and Status protocol (RAS) signaling between H.323 endpoints and gatekeepers is enhanced in H.323 Version 2 Phase 2 by including secure endpoint registration of the Cisco gateway to the Cisco gatekeeper and secure per-call authentication. The authentication type is “password with hashing” as described in ITU H.235. Specifically, the encryption method is MD5 with password hashing. This functionality is provided by the security token required-for CLI on the gatekeeper and the security password CLI on the gateway.
- GKTMP—The Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco gatekeeper provides a transaction-oriented application protocol that allows an external application to modify gatekeeper behavior by processing specified RAS messages.
- Gateway Support for Alternate Endpoints—The Alternate Endpoint feature allows a gatekeeper to specify alternative destinations for a call when queried with an Admission Request (ARQ) by an originating gateway. If the first destination gateway fails to connect, the gatekeeper tries all the alternate destinations before going to the next dial peer rotary (if a rotary is configured).
- Gateway Support for a Network-Based Billing Number—This feature informs the gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the Admission Request (ARQ) message sent by the ingress gateway. No configuration is necessary for this feature.

- Gateway Support for Voice-Port Description—This feature provides the Gatekeeper with a configurable string that identifies the voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the ARQ message sent by the ingress gateway. The string in the ARQ corresponds to the setting of the voice-port description command.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/h323v2p2.htm

H.323 Version 2 Enhancements for the Cisco 1750 Router

For the Cisco 1750 router, these enhancements provide compliance with all mandatory elements of H.323 Version 2 for the Cisco IOS based Gateway, Gatekeeper, and Proxy products. Along with other selected features, they provide critical new functionality needed for Interoperability and network deployment. New features include:

- V2 Compliant GW/GK/Proxy
- Lightweight registration
- Resource Availability Indication (RAS v2)
- DTMF Digit relay via H.245 User Information Element
- Enhanced GK selection algorithm for Gateways
- Single Proxy Scenario
- GW Registration of E.164 addresses for FXS
- Tunneling of QSIG Supplementary Services via H.225 UUIE
- Gateway support for tunneling of Redirecting Number Information Elements in H.225 messages

HSRP Support for ICMP Redirects

The HSRP Support for ICMP Redirects feature enables Internet Control Message Protocol (ICMP) redirection on interfaces configured with the Hot Standby Router Protocol (HSRP).

When running HSRP, it is important to prevent hosts from discovering the interface (or real) Media Access Control (MAC) addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router, and that router later fails, then packets from the host will be lost. Previously, ICMP redirect messages were automatically disabled on interfaces configured with HSRP.

This feature now enables ICMP redirects on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_hsrpi.htm

HSRP Support for MPLS VPNs

The HSRP support for Multiprotocol Label Switching (MPLS) VPNs feature enables ICMP redirection on interfaces configured with the Hot Standby Router Protocol (HSRP).

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides many diagnostic functions and can send and redirect error packets to hosts.

HSRP provides network redundancy in a way that ensures that user traffic immediately and transparently recovers from first-hop failures in network edge devices and access circuits. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router to the hosts on a LAN. The members of the router group continually exchange status messages by detecting when a router goes down. This HSRP group consists of an active router and a standby router to replace the active router should it fail. The address of this HSRP group is referred to as the "virtual ip address."

When running HSRP, it is important to prevent the host from discovering the primary MAC addresses in its standby group. If a host is redirected by ICMP to a standby group that later fails, the packets are lost. Previously, ICMP redirect messages were disabled on interfaces configured with HSRP. This was done to avoid the host from being directed away from the virtual IP address (the HSRP group address that provides redundancy) to the interface IP and MAC address of a single router. If this single router failed, redundancy was lost.

The HSRP Support for the ICMP Redirect Messages feature now enables ICMP redirects on interfaces configured with HSRP. This feature works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address is changed to an HSRP virtual IP address. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_hsmp.htm

IGMP Version 3

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) adds support for "source filtering" which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host (or by other routers via Protocol Independent Multicast (PIM)) to that network. In addition to restricting traffic on the network of the receiver host, IGMPv3 membership information may also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source Specific Multicast feature, introduced in Cisco IOS Release 12.1(5)T, hosts must explicitly include sources when joining a multicast group (this is known as "channel subscription"). IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases where IGMPv3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable Source Specific Multicast (SSM): URL Rendezvous Directory (URD) and IGMP v3lite. Both of these features were introduced with SSM in Cisco IOS Release 12.1(3)T. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtigmpv3.htm

IKE Extended Authentication

IKE Extended Authentication (Xauth) is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The Xauth feature is an enhancement to the existing Internet Key Exchange (IKE) Protocol feature. Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list-name must match the Xauth configuration list-name for user authentication to occur.

The Xauth feature is an extension to the IKE feature, and does not replace IKE authentication. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/xauth.htm

IKE Shared Secret Using AAA Server

The IKE Shared Secret Using AAA Server feature enables key lookup from a AAA server. Pre-shared keys do not scale well when trying to deploy a large scale Virtual Private Network (VPN) without using a certification authority (CA). When using dynamic IP addressing such as DHCP or PPP dialups, the changing IP address can make key lookup difficult or impossible unless wildcard pre-shared key is used.

In the IKE Shared Secret Using AAA Server feature, the shared secret is accessed during the aggressive mode of IKE negotiation through the AAA server. The ID of the exchange is used as the username to query AAA if no local key can be found on the Cisco IOS router to which the user is trying to connect. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/ikessaaa.htm

Implementing DiffServ for End-to-End Quality of Service

Differentiated services (DiffServ) describes a set of end-to-end quality of service (QoS) capabilities. End-to-end QoS means that the network can deliver service required by specific network traffic from one end of the network to another. Cisco IOS QoS software supports three types of service models: best-effort, integrated (IntServ), and differentiated services (DiffServ).

For more information about the best-effort and integrated-service models, refer to the *Cisco IOS Quality of Service Solution Configuration Guide.*

*Differentiated s*ervices is a multiple service model that satisfies different QoS requirements. The network tries to deliver service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit Differentiated Services Code Point (DSCP) setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, police traffic, and perform intelligent queueing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Cisco IOS QoS includes the following features that support differentiated services:

- Committed access rate (CAR), which performs packet classification through IP precedence and QoS group settings. CAR performs metering and policing of traffic, providing bandwidth management.
- Intelligent queueing schemes such as Weighted Random Early Detection (WRED) and Weighted Fair Queueing (WFQ) and their equivalent features on the Versatile Interface Processor (VIP), which are VIP-distributed WRED services.
- Modular QoS Command-Line Interface (MQC) so that you can specify a traffic class independently of QoS policies.
- Low Latency Queueing (LLQ) brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be unqueued and sent first (before packets in other queues are unqueued), giving delay-sensitive data preferential treatment over other traffic.
- Generic Traffic Shaping (GTS) shapes traffic by reducing outbound traffic flow to avoid congestion. It constrains traffic to a particular bit rate by using the token bucket mechanism. GTS applies on a per-interface basis and can use access lists to select the traffic to shape.

For more information about Cisco IOS QoS features, refer to the *Cisco IOS Quality of Service Solutions Guide* and the *Cisco IOS Quality of Service Command Reference*.

Refer to the following document for further information:

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

Inband MICA Control Messages for PPP Framing

Dialin internet connections typically start in character mode to let the general user log in and select a preferred service. When Cisco IOS determines that the user wants a framed interface protocol during the call, such as PPP or SLIP, commands are sent to the MICA modem so it will provide hardware assistance with the framing. To avoid loss or misinterpretation of framed data during the transition, these commands must be issued at precise times with respect to the data being sent and received. The Inband MICA Control Messages for PPP Framing feature allows the MICA modem framing commands to be sent in the data stream itself, which greatly simplifies Cisco IOS tasks in achieving precision timing, and reduces timeouts during PPP startup and also reduces startup time.

Individual SNMP Trap Support

The Individual SNMP Trap Support Feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are *authentication-failure*, *linkup*, *linkdown*, and *coldstart*. This feature expands the functionality of the **snmp-server enable traps snmp** command. Prior to the introduction of this feature, all four trap types were enabled or disabled simultaneously by the **snmp-server enable traps snmp** command.

Individual SNMP Trap Support is supported for all versions of SNMP supported by Cisco IOS software (SNMPv1, SNMPv2c, and SNMPv3).

Note As both SNMP traps and informs are enabled or disabled thorough the use of the **snmp-server enable traps** command, all references to traps in this document also apply to informs. The term "notifications" is used to refer to both traps and informs.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtitraps.htm

Integrated Routing and Bridging, Transparent Bridging, and PVST+ Between VLANs with IEEE 802.1Q Encapsulation

This feature supports integrated routing and bridging, transparent bridging, and PVST+ between vLANs (virtual LANs) with IEEE 802.1Q encapsulation features. It provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. This feature supports the following IEEE 802.1Q (Dot1q) functionality:

- Integrated routing and bridging (IRB)—connectivity for multiple VLANs using a Bridge-Group Virtual Interface (BVI) to associate a bridge group.
- Transparent bridging (TB)—connectivity for multiple vLANs bridged between Dot1q interfaces and other interface encapsulations or other types of interface media.
- Per-vLAN Spanning Tree (PVST+) for IEEE 802.1Q trunks—support for Dot1q trunks to map multiple spanning trees to a single spanning tree.

Interactive Voice Response Version 2.0 on Cisco VoIP Gateways

IVR Version 2.0 is the fourth release of IVR and TCL scripting on Cisco IOS VoIP gateways. The Cisco IVR feature (first made available in Cisco IOS Release 12.0(3)T and 12.0(7)T) provides IVR capabilities using TCL scripts.

IVR Version 2.0 is made up of several separate components which are described individually in the section that follows. These new features include:

- Media Gateway Control Protocol (MGCP) scripting package implementation
- Real Time Streaming Protocol (RTSP) client implementation
- New Tool Command Language (TCL) verbs to utilize RTSP and MGCP scripting features
- IVR prompt playout and digit collection on IP call legs
- Performance improvements and TCL infrastructure changes
- IVR application MIB for network management

These features add scalability and enable the IVR scripting functionality on VoIP legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_skyn.htm

Inter-Autonomous Systems MPLS VPN Support

The Inter-Autonomous Systems MPLS VPN Support feature on the Cisco 3620 and 3660 series platforms provides a 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. Refer to the following document for further information:

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

Interface Command Enhancements

Several Cisco IOS cable interface commands have been enhanced:

- The **show controller c***x***/0 upstream** *number* and **show interface c***x***/0 upstream** *number* commands display the following additional statistic counters:
  - Average percent of upstream utilization in minislots
  - Average percent of contention slots
  - Average percent of initial ranging slots
  - Average percent of minislots that were due because the MAP scheduler was not able to request them in time
- The **show interface c***x***/0 sid** [*number*] **counters** command now supports a **verbose** option that displays two additional statistics:
  - Number of bandwidth requests successfully received by the Cisco uBR7200 Series Universal Broadband Router from the specified SID on the specified cable interface
  - Number of grants issued by the Cisco uBR7200 Series Universal Broadband Router to the specified SID
- The **show cable flap-list** and **show cable modem** commands now indicate when the Cisco uBR7200 Series Universal Broadband Router has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk appears in the power

adjustment field for a modem when a power adjustment has been made; an exclamation point appears when the modem has reached its maximum power transmit level and cannot increase its power level any further.

- Other power adjustment changes have been made to the **cable upstream power-adjust** command to allow the Cisco uBR7200 series router to better adjust when a cable modem seems to "bounce" (the modem requires frequent power adjustments in opposite directions). When this situation occurs, instead of making large power adjustments for each correction, you can configure the Cisco uBR7200 series router to calculate the average value of the power corrections before making power adjustments.
  - The **cable upstream power-adjust threshold** command now accepts a range of 0–10 dB. The previous range was 0–2 dB.
  - The **cable upstream power-adjust noise** *% of power adjustment* command sets the threshold value (in percent) for a particular upstream switching between regular power adjustments and the noise power adjustment method (which uses an averaging algorithm before sending any correction).
  - The **cable upstream frequency-adjust averaging** *% of frequency adjustment* command sets the threshold (in percent) for a particular upstream switching between regular frequency adjustments and the average frequency adjustment method (which uses an averaging algorithm before sending any correction).
- The **show cable modem** command now supports a number of new options:
  - **show cable modem detail** adds signal/noise ratio (SNR) information for each cable modem on each interface
  - **show cable modem summary** displays the total number of modems connected for each upstream channel, including the number of currently active modems
  - **show cable modem** [**interface** [**upstream** *number*]] displays the total number of modems for the specified interface or upstream
  - **show cable modem** [**interface** [**upstream** *number*]] **registered** displays the total number of registered modems for the specified interface or upstream
  - **show cable modem** [**interface** [**upstream** *number*]] **unregistered** displays the total number of unregistered modems for the specified interface or upstream
  - **show cable modem** [**interface** [**upstream** *number*]] **offline** displays the total number of offline modems for the specified interface or upstream, including status information for each modem before going offline and the time each modem went offline
- The **cable downstream if-output** command is enhanced with the following options to generate test signals on the downstream interface:
  - **cable downstream if-output prbs** shuts down the downstream interface and outputs a PRBS test signal
  - **cable downstream if-output continuous-wave** shuts down the downstream interface and outputs an unmodulated carrier signal

  The previous **cable downstream if-output** command has not changed and continues to output a standard modulated signal. The **no cable downstream if-output** command also has not changed—it stops all signal output and shuts down the interface.
- A new command changes the cable modem registration value (the T9 timer). The **cable registration-timeout** *minutes* command sets the T9 to the new value (from 2 to 60 minutes). The **no cable registration-timeout** command resets the T9 timer to its default of 3 minutes.

- Cisco IOS software has a number of new and enhanced commands to support the point-to-point wireless modem card. For more information, refer to the *Cisco uBR7200 Series Wireless Modem Card and Subsystem Installation and Configuration* publication.

Interface Index Persistence

One of the most commonly used identifiers used in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the "name" of the interface. Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

Cisco IOS Release 12.1(5)T adds support for an ifIndex value that can persist across reboots, allowing users to avoid the workarounds previously required for consistent interface identification. The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer) allows network management data to be more effectively utilized. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5ifidx.htm

Interface Range Specification

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range. The Interface Range Specification feature is implemented with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the **range** keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

Refer to the following document for further information:

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

Interworking Signaling Enhancements for H.323 and SIP VoIP

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables VoIP networks to properly signal the setup and tear-down of calls when interworking with PSTN networks. These enhancements ensure that in-band tones and announcements are generated when needed so that the voice path is cut-through at the appropriate point of call setup and that early alerting (ringing) does not occur. In addition, support for network-side ISDN and the reducing of speech clipping is addressed. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt4t323.htm

IP Address Negotiation

Cisco IOS Release 12.1(3a)T1 for Cisco uBR900 series Cable Access Routers adds support for the **ip address dhcp** command on the cable interface. Previous releases used the **ip address negotiated** command for this purpose, but this command is now reserved for serial interfaces. This change is cosmetic only and does not change how the router obtains its IP address.

IP DSCP Marking for Frame-Relay PVC

The functionality of configuring a policy on a main or a subinterface to match and set IP type of service (ToS) and differentiated services code point (DSCP) bits has existed in Cisco IOS Release 12.0S and Cisco IOS Release 12.0(7)XE. This feature was introduced to Cisco IOS 12.1(2)T with the added support of configuring a policy on an ATM PVC. This feature extends the support of Frame-Relay PVC in Cisco IOS Release 12.1(5)T.

IP over a CLNS Tunnel

The IP over a CLNS Tunnel feature lets you transport IP traffic over CLNS, for instance, on the data communications channel (DCC) of a SONET ring.

The IP over CLNS Tunnel is a virtual interface that enhances interactions with CLNS networks, allowing IP packets to be tunneled through the Connectionless Network Protocol (CLNP) to preserve TCP/IP services.

Configuring an IP over CLNS tunnel (CTunnel) allows you to Telnet to a remote router that has only CLNS connectivity. Other management facilities can also be used, such as SNMP, TFTP, and so on, which otherwise would not be available over a CLNS network. Refer to the following document for further information:

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

ISDN Network Side for ETSI Net5 PRI

The ISDN Network Side for ETSI Net5 PRI feature enables Cisco IOS to replicate the public switched network interface to a PBX that is compatible with the ETSI Net5 switch type.

Routers and PBXs are both traditionally CPE with respect to the public switched network interfaces. For Voice over IP (VoIP) applications, it is desirable to interface access servers to PBXs with the access server representing the public switched network.

Enterprise organizations use the current VoIP features with Cisco products as a method to reduce long distance costs for phone calls within and outside of their organizations. However, there are times that a call cannot go over VoIP and the call needs to be placed using the PSTN. The customer then must have two devices connected to a PBX to allow some calls to be placed using VoIP and some calls to be placed over the Public Switched Telephone Network (PSTN). In contrast, this feature allows Cisco access servers to connect directly to user-side CPE devices such as PBXs and allows voice calls and data calls to be placed without requiring two different devices to be connected to the PBXs.

This feature enables the access server to provide a standard ISDN PRI network side interface to the PBXs and to mimic the behavior of legacy phone switches. To a PBX, the access server functions as a Net5 PRI switch. No change in PBX capability or behavior is required. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtpri_n5.htm

ISDN Progress Indicator Support for SIP using 183 Session Progress

This feature enhancement adds session initiation protocol (SIP) 183 Session Progress and Ringing messages to better map to ISND/CAS messages.

L2TP Tunnel Management Enhancements

The L2TP Tunnel Enhancements feature fills an existing tunnel with sessions up to a configured limit. Then it creates a new tunnel to the next destination IP address in the configured load-sharing group. It fills this new tunnel to the limit.

L2TP Tunnel Switching

The L2TP Tunnel Switching feature is a tunnel aggregation feature. It enables entire tunnels to be switched in the existing VPDN Multihop feature. Previously, only individual sessions could be switched.

Leased line Support for 2600/3600 Analog Modems NM-16AM and NM-8AM

This feature requires a modem firmware upgrade to provide 2-wire leased-line support for the current Cisco analog modems (NM-8AM and NM-16AM) for enterprise customers who require point-to-point connections between locations and for enterprise customers with medium to high data transfer requirements without access to other technologies or with access to only low-grade phone lines. Loop current is required. Refer to the following document for further information:

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

Low Latency Queueing for Frame Relay

Low Latency Queueing for Frame Relay is a new feature that provides a strict priority queue (PQ) for voice traffic and weighted fair queues for other classes of traffic. Before the release of this feature, low latency queueing was available at the interface and ATM virtual circuit (VC) levels. It is now available at the Frame Relay VC level when Frame Relay traffic shaping is configured.

Low Latency Queueing, also called priority queueing/class-based weighted fair queueing (PQ/CBWFQ), is a superset of and more flexible than previous Frame Relay Quality of Service offerings, in particular Real-Time Transport Protocol (RTP) prioritization and priority queueing/weighted fair queueing (PQ/WFQ).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtfrpqfq.htm

MC16S LED Enhancement

Using Cisco IOS Release 12.1(2)T, MGR ACT LED behavior on the Cisco MC16S Cable Modem Card differs (see Table 23). This feature also stops Spectrum Scanning on one or more upstream ports if the upstream or the whole interface is shut down.

Table 23 Cable Modem Card LEDs

LED Label	Color	State	Description
Enabled	Green	On	Indicates that the cable modem card is operating normally: receiving DC power from the router midplane and enabled for operation.
	N/A	Off	Either the card is shut down or the slot is not working.

Table 23 Cable Modem Card LEDs

LED Label	Color	State	Description
Upstream	Green	On	For each upstream port, indicates that the upstream path is enabled.
	N/A	Off	Either the port is not configured, shut down, or the slot is not working.
Downstream	Green	On	For each downstream port, indicates that the downstream path is enabled.
	N/A	Off	Either the port is not configured, shut down, or the slot is not working.
MGR ACT (MC16S only)	Green	On	With Release 12.0.7 XR2 or Release 12.1(1a)T1, indicates that a spectrum group has been configured. With Release 12.1.(2)T, indicates that the MC16S Spectrum Management Card has initiated an upstream frequency hop from a potentially "noisy" channel to a cleaner channel.
	N/A	Off	Either the port is not configured, shut down, or the slot is not working.

Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway

The Media Gateway Control Protocol (MGCP) for the Cisco AS5300 is a protocol that media gateways use for passing voice calls from the Public Switched Telephone Network (PSTN) to call agents in an internet telephony network. Media gateways include trunking gateways, access gateways, and network access servers. The call agents provide the call control intelligence.

Caveat for 12.1(1)T:

The **show mgcp** command displays the status of mgcp on the system. The display includes a line

```
MGCP simple-sdp DISABLED, MGCP cisco fgdos DISABLED
```

These two commands are for Cisco use only in Release 12.1(1)T. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/mgcp1211.htm

Media Gateway Control Protocol Residential Gateway Support

Cisco IOS Release 12.1(3a)T1 for the Cisco uBR924 Cable Access Router supports version 0.1 of the Media Gateway Control Protocol (MGCP), a proposed IETF voice control protocol that is intended to eventually supersede the existing SCGP 1.1 protocol. The MGCP 0.1 and SGCP 1.1 protocols have been merged on the Cisco uBR924 router so that the router can respond efficiently to either protocol.

The Cisco uBR924 Cable Access Router functions as a Residential Gateway, providing an interface between analog FXS phone or fax systems and the Voice over IP (VoIP) network. The Residential Gateway uses a Trunking Gateway to contact the call agent, which in turn provides access to the public telephone switched network (PTSN).

The Cisco uBR924 Cable Access Router supports both call waiting and caller ID when using either MGCP or SGCP for call control. Each of the two voice ports on the Cisco uBR924 router can be configured with the IP address for a default call agent. SNMP management of both the MGCP and SNMP protocols is provided by a single MIBXGCP-MIB).

This feature is described in detail in the *Media Gateway Control Protocol Version 12.1.3 T* feature module, available on Cisco.com. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/mgcp1213.htm

MGCP Support for CallManager (IP-PBX)

Adds MGCP support to IOS gateway to provide Supplementary Services with CallManager.

Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes

With the Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes feature you can set a minimum mask size. The IP address that is added to the aggregation cache is added to the maximum user-entered mask and the routing table mask.

To enable this feature on a Source Prefix or a Destination Prefix, or both, configure the desired Minimum Mask value using the NetFlow aggregation commands. The Minimum Mask value used by the router selects the granularity of the NetFlow data that will be collected.

The mask values range from 1 to 32. For coarse NetFlow collection granularity select a small Minimum Mask value. For fine NetFlow collection granularity select a large Minimum Mask value. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtnfmask.htm

Monitoring Resource Availability on Cisco AS5300, AS5400, and AS5800 Universal Access Servers

This feature provides enhancements to improve the visibility into the line and modem status for the network access server (NAS).

NAS modem health is supported by the following features:

- DS-0 Busyout Traps
- ISDN PRI Requested Channel Not Available Traps
- Modem Health Traps
- Show Controllers Timeslots
- DS-1 Loopback Traps

These features have been developed to monitor the NAS health conditions at the digital signal level zero (DS-0) level, Primary Rate Interface (PRI) bearer channel level, and modem level.

This combined set of features provides the following benefits:

- Improved visibility into the line status for the NAS for comprehensive health monitoring and notification capability.
- Improved troubleshooting and diagnostics for large dial networks.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtbsyout.htm

MPLS Quality of Service Enhancements

When a customer transmits IP packets from one site to another, the IP precedence field (the first three bits in the header of an IP packet) specifies the quality of service (QoS) such as latency or the percent of bandwidth allowed for a particular class of service. The service provider might want to set an MPLS packet's QoS to a different value.

QoS transparency allows the service provider to set the MPLS experimental field instead of overwriting the value in the customer's IP precedence field. The IP header remains available for the customer's use; the IP packet QoS is not changed as the packet travels through the multiprotocol label switching (MPLS) network. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/mct1214t.htm

MPLS Egress NetFlow Accounting

The MPLS Egress NetFlow Accounting feature allows you to capture Internet Protocol (IP) flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS and are transmitted as IP.

Previously, you captured NetFlow data only for flows that arrived on the packet in IP format. When an edge router performed MPLS label imposition (received an IP packet and transmitted it as an MPLS packet), NetFlow data was captured when the packet entered the network. Inside the network, the packet was switched based only on MPLS information, and thus NetFlow information was not captured until after the last label was removed.

One common application of the MPLS egress NetFlow accounting feature allows you to capture the MPLS virtual private network (VPN) IP flows that are traveling from one site of a VPN to another site of the same VPN through the service provider backbone.

Formerly, you captured flows only for IP packets on the ingress interface of a router. You could not capture flows for MPLS encapsulated frames, which were switched through Cisco Express Forwarding (CEF) from the input port. Therefore, in an MPLS VPN environment you captured flow information as packets were received from a customer edge (CE) router and forwarded to the backbone. However, you could not capture flow information as packets were transmitted to a CE router because those packets were received as MPLS frames.

The MPLS egress NetFlow accounting feature lets you capture the flows on the outgoing interfaces.

Refer to the following document for further information:

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

MPLS Scalability Enhancements for LSC and ATM LSR

The MPLS label switch controller (LSC), combined with slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP features in Cisco Internetwork Operating System (IOS) software

The MPLS LSC supports highly scalable integration of MPLS (IP+ATM) services by using a direct peer relationship between the ATM switch and MPLS routers. This direct peer relationship removes the limitation on the number of IP edge routers (typical of traditional IP-over-ATM networks), allowing service providers to meet growing demands for IP services. The MPLS LSC also supports direct and rapid implementation of advanced IP services over ATM networks using ATM switches.

MPLS combines the performance and virtual circuit capabilities of Layer 2 (data link layer) switching with the scalability of Layer 3 (network layer) routing capabilities. This combination enables service providers to deliver solutions for managing growth, providing differentiated services, and leveraging existing networking infrastructures.

The MPLS LSC architecture provides the flexibility to:

- Run applications over any combination of Layer 2 technologies
- Support any Layer 3 protocol while scaling the network to meet future needs

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc7/mpls_lsc.htm

MPLS Traffic Engineering and Enhancements

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.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures.

MPLS traffic engineering

- Enhances standard Interior Gateway Protocols (IGPs), such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows
- Transports traffic flows across a network using MPLS forwarding
- Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources available in the network
- Employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow
- Recovers from link or node failures by adapting to the new constraints presented by the changed topology
- Transports packets using MPLS forwarding crossing a multihop label-switched path (LSP)

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/traffeng.htm

MPLS VPN Support for Subinterfaces and Interface Bundles

Cisco IOS Release 12.2 includes MPLS support as part of its VPN offerings for cable subinterfaces and interface bundles. The software offers enhancements made to tags placed on the fronts of packets that contain forwarding information used to make switching decisions for cable interfaces and bundles. This tag switching infrastructure combines advanced routing protocol capabilities to define IP VPNs by selectively advertising IP reachability information to just those subscribers within the same VPN or extranet on a cable interface.

The MPLS-VPN approach of creating VPNs for individual ISPs requires subinterfaces to be configured on cable interfaces or bundles. Refer to the "Cable Subinterfaces and Interface Bundling" section on page 105 for definitions of subinterfaces and interface bundles. One subinterface is required for each ISP. The subinterfaces are tied to VPN Routing Forwarding (VRF) tables for respective ISPs.

Apart from creating one subinterface for an ISP, an additional subinterface is created on the cable interface bound to the management VPN. The management VPN is the one that connects the Cisco uBR7200 series to a Provider Enterprise (PE) router that connects to management servers such as CNR and ToD. MPLS VPN support also allows interfaces to be bound to a VRF table where each VRF belongs to an ISP. This allows Cisco uBR7200 series downstream and upstream plant segments to be shared by multiple ISPs. PCs behind respective CMs obtain their IP addresses from the respective ISP address pool. Traffic coming from those CMs is routed to the ISP's point of interconnect router.

For MPLS commands, refer to *Cisco MPLS VPN Solutions Command Reference*.

The Cisco uBR7200 series support a CM-to-cable subinterface association by mapping the SIDs that are assigned to that CM to the subinterface. This mapping is created by gleaning DHCP reply messages meant for the PC. The IP address stored in the DHCP reply is matched for its subnet value against the subnet value configured for each of the subinterfaces over a physical interface or a cable bundle. The subnet information can be derived by the IP address and the mask value configured for the subinterface. All other SIDs for the CM that are created after the initial DHCP configuration of CM are bound to the same subinterface by the Cisco uBR7200 series router.

The SID-to-subinterface mapping created by gleaning DHCP reply is used to associate an incoming packet to the correct subinterface and switched using VRF configured on that subinterface.

Note MPLS VPN support is included in Cisco IOS Release 12.1(2)T, Release 12.1(5)T, and higher releases. Release 12.1(3)T does not include MPLS VPN support.

MSDP MIB

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled "Multicast Source Discovery Protocol MIB" (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at http://www.ietf.org. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5msdp.htm

Multicast Hoot and Holler Conferencing over IP

Cisco Hoot and Holler Conferencing over IP is powered using Cisco's VoIP technology, Cisco's IP multicast and Cisco's new DSP audio mixing. This solution provides the ability to transport Hoot and Holler traffic over Cisco equipment. Traditional Hoot and Holler networks are a point-to-multipoint voice applications and are commonly used by brokerage and trading firms to advise brokers and traders on market movements. Brokerage and trading firms can spend millions of dollars in monthly leased line charges to pay for dedicated circuit-switched leased Hoot and Holler long distance connections. The Cisco Hoot and Holler over IP solution enables customers to eliminate these expensive charges while protecting investments in existing Hoot and Holler equipment such as turrets, bridges and four wire phones. The Cisco Hoot and Holler over IP features are implemented with a Cisco IOS software upgrade and is supported over voice-enabled Cisco 2600 and 3600 modular multiservice platforms.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtvmult3.htm

Multimedia Conference Manager with Voice Gateway Image with RSVP to ATM SVC Mapping

This feature is designed to deliver Cisco's H.323 gatekeeper, proxy, and voice gateway solutions with routing as a single Cisco IOS image. In addition, the ability to map H.323 Resource Reservation Protocol (RSVP) reservations to ATM non-real-time variable bit rate (VBR) switched virtual circuits (SVCs) has also been incorporated for guaranteeing quality of service (QoS) over ATM backbones for video applications.

MCM, Gatekeeper, Proxy, and Gateway

The H.323 Multimedia Conference Manager (MCM) provides the network administrator with the ability to identify H.323 traffic and apply appropriate policies. H.323 MCM is implemented on Cisco IOS software. MCM provides a network manager with the ability to limit the H.323 traffic on the LAN and WAN; provides user accounting for records based on the service utilization; injects QoS for the H.323 traffic generated by applications such as voice over IP (VoIP), data conferencing and video conferencing; and provides the mechanism to implement security for H.323 communications. In addition to this functionality, this new and separate image also incorporates Cisco's voice gateway and routing functionalities in the same image.

ATM VBR SVC Support for Video

ATM non-real-time variable bit rate (VBR) switched virtual circuit (SVC) service operates much like X.25 SVC service, although ATM allows much higher throughput. Virtual circuits are created and released dynamically, providing user bandwidth on demand. This service requires a signaling protocol between the router and the switch. Each ATM node is required to establish a separate connection to every other node in the ATM network with which it needs to communicate. All such connections are established using a permanent virtual circuit (PVC) or an SVC with an ATM signaling mechanism.

With this feature, customers that use ATM backbones will be able to guarantee that video sessions will traverse that backbone with QoS features enabled. The Cisco IOS image will take H.323 RSVP reservations and map them to ATM VBR SVCs that will be dynamically established and torn down when video sessions are established and terminated. End-to-end IP routing across the network backbone is no longer required to guarantee video QoS. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_mcm5t.htm

Multiprotocol Label Switching on Cisco Routers

Multiprotocol label switching (MPLS) on Cisco Routers combines the performance and capabilities of Layer 2 (data link layer) switching with the proven scalability of Layer 3 (network layer) routing. MPLS enables service providers to meet the challenges of explosive growth in network utilization while providing the opportunity to differentiate services without sacrificing the existing network infrastructure. The MPLS architecture is flexible and can be employed in any combination of Layer 2 technologies. MPLS support is offered for all Layer 3 protocols, and scaling is possible well beyond that typically offered in today's networks.

MPLS efficiently enables the delivery of IP services over an ATM switched network. MPLS supports the creation of different routes between a source and a destination on a purely router-based Internet backbone. By incorporating MPLS into their network architecture, service providers can save money, increase revenue and productivity, provide differentiated services, and gain competitive advantages.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/rtr_13t.htm

NAT—Enhanced H.225/H.245 Forwarding Engine

During the call setup between H.323 terminals, H.225/H.245 protocols are used. The protocol messages contain embedded IP addresses and ports. If a message passes through a NAT router, it has been decoded, translated and encoded back to the packet. This enhancement extends support to all messages in H.225/H.245 protocols and all embedded addresses. Refer to the following document for further information:

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

NAT—Support for NetMeeting Directory (Internet Locator Service - ILS)

Microsoft NetMeeting is a Windows-based application that enables multi-user interaction and collaboration from a users PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made. Refer to the following document for further information:

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

NAT—Support of H.323 v2 Call Signaling (FastConnect)

Cisco IOS Network Address Translation (NAT) supports all H.225 and H.245 message types, including Fast Connect and Alerting as part of H.323 v2. Any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dth323v2.htm

NAT—Support of IP Phone to Cisco Call Manager

Cisco IP Phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco Call Manager (CCM). Messages flow back and forth that include IP address and Port information which is used to identify other IP Phone users with which a call can be placed.

To be able to deploy Cisco IOS Network Address Translation (NAT) between the IP Phone and CCM in a scalable environment, NAT needs to be able to detect the Selsius Skinny Station Protocol and understand the information passed within the messages.

When an IP Phone attempts to connect to the CCM and it matches the configured NAT translation rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address is what will be reflected in the CCM and be visible to other IP Phone users.

Refer to the following document for further information:

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

Network-Based Application Recognition

Network-Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, including Web-based and other difficult-to-classify protocols that utilize dynamic transmission control protocol/user datagram protocol (TCP/UDP) port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features to provide bandwidth guarantees and limits, traffic shaping, and packet marking.

NBAR introduces several new classification features:

- Classification of applications that dynamically assign TCP/UDP port numbers
- Classification of HTTP traffic by URL, HOST, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although Access Control Lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

NBAR provides a special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

Refer to the following document for further information:

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

Network Side ISDN PRI Signaling, Trunking, and Switching

The Network Side ISDN PRI Signaling, Trunking, and Switching feature enables Cisco IOS software to replicate the public switched network interface to a PBX that is compatible with the National ISDN (NI) switch type and European Telecommunications Standards Institute (ETSI) Net5 switch type. Routers and PBXs are both traditionally CPE devices with respect to the public switched network interfaces. However, for Voice over IP (VoIP) applications, it is desirable to interface access servers to PBXs with the access server representing the public switched network.

Enterprise organizations use the current VoIP features with Cisco products as a method to reduce costs for long distance phone calls within and outside their organizations. However, there are times that a call cannot go over VoIP and the call needs to be placed using the Public Switched Telephone Network (PSTN). The customer then must have two devices connected to a PBX to allow some calls to be placed using VoIP and some calls to be placed over the PSTN. In contrast, this feature allows Cisco access servers to connect directly to user-side CPE devices such as PBXs and allows voice and data calls to be placed without requiring two different devices to be connected to the PBXs.

The ISDN Network Side PRI Signaling, Trunking, and Switching feature allows Cisco ISDN-enabled access servers to switch calls across interfaces as legacy phone switches do today and to mimic the behavior of the legacy phone switches. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtpri_ni.htm

NextPort Port Service Management for the Cisco AS5400 Universal Access Server

The NextPort port service management feature implements digital service port technology for the Cisco AS5400. Ports on the Nextport modem carrier module support both modem and digital services. Ports can be addressed aggregated at the slot level of the Nextport module, the Service Processing Element (SPE) level within the Nextport module, and the individual port level. The Service Processing Element (SPE) is an addressable group of six modems. The Nextport dial feature card is supported by Service Processing Element (SPE) operating software.

Benefits include the following:

- Modem or digital service at the port level resulting in greater flexibility of network configuration
- Addressability at the slot, SPE, or port level resulting in ease and scale of configuration tasks
- Higher port density in the platform resulting in economies of scale
- SPE layer buffers the platform architecture from future changes and advances in port level technology
- Modular architecture with resulting ease and economy of maintenance
- The Nextport architecture is designed to be extended to additional port services and other Cisco access server platforms.

For complete information about NextPort Port Service Management for the Cisco AS5400 Universal Access Server, Refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/nextport/dtnxptxd.htm

NM-1A-OC3MM-1V NM-1A-OC3SM1 and NM-1A-OC3SML-1V

This feature adds online insertion and removal (OIR) support for ATM OC-3 with CES network modules on the Cisco 3660 Series.

NTP MIB

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a Network Management System (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table. For complete details on the Cisco implementation of the NTP MIB, refer to the MIB file itself ("CISCO-NTP-MIB.my", available through Cisco.com at http://tools.cisco.com/ITDIT/MIBS/servlet/index).

OSPF Flooding Reduction

The explosive growth of the Internet has placed the focus on the scalability of Interior Gateway Protocols such as OSPF. The networks using OSPF are becoming larger every day and will continue to expand to accommodate the demand to connect to the Internet.

Internet Service Providers and customers with large networks have regularly complained that OSPF has a traffic overhead, even when the network topology is stable.

By design, OSPF requires link-state advertisements (LSAs) to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to around 50 min. or so.

This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF Flooding Reduction feature works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set, thus making them DoNotAge (DNA) LSAs. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_ospff.htm

Parser Cache

The Parser Cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files. This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines which differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on). Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

The parser cache is enabled by default on all platforms using Cisco IOS 12.1(5)T or later. A new command, **[no] parser cache**, allows the disabling or re-enabling of this feature. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5parse.htm

PIM Dense Mode State Refresh

The PIM Dense Mode State Refresh feature keeps the pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree. Refer to the following document for further information:

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

Point-to-Point Protocol (PPP) over ATM Using Dialer Interfaces

Cisco IOS release 12.2 supports Point-to-Point Protocol (PPP) over ATM using dialer interfaces. This feature points static routes to a negotiated IP address.

You cannot point static routes to a negotiated IP address by cloning from virtual templates because you cannot point a static route to a virtual template or a virtual access interface. A virtual template only stores configuration commands and a virtual access is created and destroyed interface by cloning from dialer interfaces. You can therefore point static routes at this dialer interface.

This feature is related to caveat CSCdp19686.

PPP Over ATM SVC

PPP over ATM SVC implements standards-based PPP over ATM AAL5. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtppposv.htm

PPP over Ethernet on ATM

The PPP over Ethernet (PPPoE) on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. With this model, each host utilizes its own PPPoE stack and the user is presented with a familiar user interface. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis. Before a point-to-point connection over Ethernet can be provided, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier. A unique session identifier is provided by the PPPoE Discovery Stage protocol.

The ATM feature provides service-provider digital subscriber line (DSL) support. As service providers begin DSL deployments, two of their most significant goals are to ease and facilitate consumer end adoption and to preserve as much of the dialup model as possible. PPPoE serves to advance both of these goals by leveraging ethernet scale curves and embedded base (such as ATM NICs) and by preserving the point-to-point session used by internet service providers (ISPs) in today's dialup model. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtpppoe.htm

PPP Over Fast Ethernet 802.1Q

The PPPoE over IEEE 802.1Q Encapsulation feature adds support for running PPP over Ethernet over IEEE 802.1Q encapsulation. IEEE 802.1Q encapsulation enables you to interconnect a VLAN capable router with another VLAN capable device.

PPPoE Over IEEE 802.1Q VLANs

The PPPoE Over IEEE 802.1Q VLANs feature adds support for running PPP over ethernet over IEEE 802.1Q virtual local area networks (VLANs). IEEE 802.1Q is used to interconnect a VLAN-capable router with another VLAN-capable device. The packets on the 802.1Q link contain a standard (fast) Ethernet frame and the VLAN information associated with that frame. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtppp_1q.htm

PPPoE RADIUS Port Identification

This feature adds RADIUS port identification information when using point to point protocol over Ethernet (PPPoE) over ATM, Ethernet, and 802.1Q VLANs. Refer to the following document for further information:

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

PPPoE Termination on Cable interfaces

The PPPoE on Cable Interfaces feature adds support for PPPoE by allowing a direct connection to cable interfaces. PPPoE provides service-provider digital-subscriber line (DSL) support. The support of PPPoE on cable interfaces of the Cisco uBR7200 series routers allows customer premises equipment (CPE) behind the cable modem to use PPP as a mechanism to get their IP addresses and use it for all subsequent data traffic, just like a dial-up PPP client. In a PPP dial-up session, the PPPoE session is authenticated and the IP address is negotiated between the PPPoE client and the server, which could be either a Cisco uBR7200 series router or a Home Gateway.

Pragmatic General Multicast (PGM)

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for multicast applications that require reliable, ordered, duplicate-free multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. PGM has two main parts: a host element (also referred to as the transport layer of the PGM protocol) and a network element (also referred to as the network layer of the PGM protocol).

The transport layer of the PGM protocol consists of two main parts: a source part and a receiver part. The transport layer defines how multicast applications send and receive reliable, ordered, duplicate-free multicast data from multiple sources to multiple receivers. The PGM Host feature is the Cisco implementation of the transport layer of the PGM protocol. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtpgmhst.htm

Preauthentication Enhancements for Callback

The Preauthentication Enhancements for Callback feature allows users to dial into the NAS without being charged. This enables telecommuters, and other remote network users who dial in, to have the charges applied back to the NAS into which they are dialing.

Two Cisco VSAs for preauthentication will be added to Attribute 26 as follows:

cisco-avpair = “preauth:send-name=<string>”

cisco-avpair = “preauth:send-secret=<string>”

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt2.htm

Preauthentication with ISDN PRI

The Preauthentication with ISDN PRI feature allows a Cisco network access server (NAS) to determine if an incoming call may be answered on the basis of the called number, the calling number, or the call type. With an ISDN PRI (Primary Rate Interface), information about an incoming call is available to the NAS before the call is answered. The available call information includes the called station ID (DNIS), the calling station ID (CLID), and the bearer capability (call type).

When an incoming call arrives from the public network switch, but before it is answered, this feature enables the NAS to send the DNIS, CLID, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then

the NAS sends a disconnect message to the public network switch to reject the call. This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication based on the CLID at the same time.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

In the event that the RADIUS server application becomes unavailable, this feature allows a guard timer to be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without the authorization. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtpreaut.htm

Preauthentication with ISDN PRI and Channel-Associated Signaling

The Preauthentication with ISDN PRI and Channel-Associated Signaling feature allows a Cisco network access server (NAS) to determine if an incoming call may be answered on the basis of the called number, the calling number, or the call type. With an ISDN PRI (Primary Rate Interface), or with Channel-Associated Signaling (CAS), information about an incoming call is available to the NAS before the call is answered. The available call information includes the called station ID (DNIS), the calling station ID (CLID), and the bearer capability (call type).

When an incoming call arrives from the public network switch, but before it is answered, this feature enables the NAS to send the DNIS, CLID, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then the NAS sends a disconnect message to the public network switch to reject the call. This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication based on the CLID at the same time.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

In the event that the RADIUS server application becomes unavailable, this feature allows a guard timer to be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without the authorization. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/preaucas.htm

Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements

This feature supports the use of new RADIUS VSAs. These RADIUS VSAs are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used. Enhancements for this feature include:

- Attribute 6 can be set to Service-Type = Framed-User
- Support for new VSAs “preauth:send-name” with text and “preauth:send-secret” with text.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt1.htm

Prepaid Distributed Calling Card via Packet Telephony

Support for the Debit Card feature was extended to the Cisco AS5800 Universal Access Server. The Debit Card feature allows service providers to offer calling service with debit accounting. The Debit Card feature and RADIUS-specific enhancements also support Vendor-Specific Attributes (VSA). The Debit Card for Packet Telephony on the Cisco AS5800 works in tandem with the Cisco Interactive Voice Response (IVR) feature. The IVR voice scripts have been modified to use Tool Command Language (TCL) scripts.

The feature components consist of IVR functionality in Cisco IOS software that works in connection with an integrated third-party billing system. This includes the ability to maintain per-user credit balance information through a RADIUS interface to the Cisco IOS software. When these features are implemented, the billing system and IOS software functions enable a carrier to authorize voice calls and to debit individual user accounts in real time at the edges of a voice over IP network, without requiring external service nodes. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/pul0134x.htm

PRI/Q.931 Signaling Backhaul for Call Agent Applications

The PRI/Q.931 Signaling Backhaul for Call Agent Applications feature provides the ability to reliably transport the signaling (Q.931 and above layers) from a PRI trunk that is physically connected to a media gateway (for example, a Cisco AS5300) to a media gateway controller (Cisco VSC3000) for processing.

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. Two new features, Roaming and Multiple Roots have been added in Cisco IOS Release 12.1(1)T to enhance the OSP. The VoIP/Open Settlement Protocol (OSP) feature offers the ability to authorize, route calls, and billings between two different ISPs via a trusted third party, the settlement clearing house, which is the OSP server. Cisco has built this OSP client on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms, and partnered with a few companies (TransNexus, GRIC, etc.) that provide OSP servers.

The code for this feature is an encrypted image.

Note Before you can download 56-bit or 56i encryption images, you must first go through the entitlement process. This process makes sure your system is coming from a registered DNS address and that you're not coming from an encryption-restricted country (Iraq, Libya, etc.). You (and your customers) can entitle yourselves by filling out the forms located at the following URL: http://www.cisco.com/kobayashi/library/12.0/

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/cfios/cfselfea/0144cors.htm

PRI QSIG on the Cisco 7200

QSIG protocol support allows Cisco voice switching services to connect PBXs, key systems, and central office switches that communicate by using the QSIG protocol, which is becoming the standard for PBX interoperability in Europe and North America. QSIG is a variant of ISDN D-channel signaling. With QSIG, Cisco networks emulate the functionality of the public-switched telephone network (PSTN), and QSIG signaling messages allow the dynamic establishment of voice connections across a Cisco WAN to a peer router, which can then transport the signaling and voice packets to a second private integrated services network exchange (PINX). In addition, QSIG support can enable a toll-bypass application.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_qsig.htm

PSTN Fallback

PSTN Fallback provides a mechanism to monitor congestion in the IP network and either redirect calls to the Public Switched Telephone Network (PSTN) or reject calls based on the network congestion. PSTN Fallback does not provide assurances that a call which proceeds over the IP network is protected from the effects of congestion. This is the function of the other QoS mechanisms such as IP RTP Priority or LLQ. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtpstnfb.htm

QSIG Protocol Support

QSIG protocol support allows Cisco voice switching services to connect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) that communicate by using the QSIG protocol, which is becoming the standard for PBX interoperability in Europe and North America. QSIG is a variant of ISDN D-channel signaling. With QSIG, Cisco networks emulate the functionality of the public-switched telephone network (PSTN), and QSIG signaling messages allow the dynamic establishment of voice connections across a Cisco wide-area network (WAN) to a peer router, which can then transport the signaling and voice packets to a second private integrated services network exchange (PINX).

QSIG support includes the following capabilities:

- Enables digit forwarding on POTS dial peers.
- On Cisco 2600 series routers, enables QSIG-switched calls over Voice over Frame Relay (VoFR) and Voice over IP (VoIP) for T1/E1 and BRI voice interface cards.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_qsig.htm

Quality of Service for Virtual Private Networks

With the introduction of the Quality of Service for Virtual Private Networks (QoS for VPNs) feature, packets can now be classified before tunneling and encryption occur (a process known as preclassification). The preclassification process is important because all tunnel traffic that is not preclassified is treated identically, making traffic flows impossible to adjust in congested environments.

When the QoS for VPN feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be adjusted in congested environments. The end result is more effective packet tunneling.

Refer to the following document for further information:

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

Quality of Service Voice Enhancements

Cisco IOS Release 12.1(3)T supports the following features:

- Low Latency Queuing for Voice over Frame Relay
- H.323 voice (v2) support

- Registration, admission, and status protocol (RAS) voice (v2) enhancement support
- DiffServ
- Fax relay enhancements

To configure these features on Cisco 1700 series routers, refer to the online document *Quality of Service Solutions Configuration Guide*. From Cisco.com, click on the path (under the heading **Service & Support**):

Technical Documents: Documentation Home Page: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1: Configuration Guides and Command References: Configuration Guides and Command References: Quality of Service Solutions Configuration Guide**

RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature enables the user to specify the hostname of the NAS in attribute 66, rather than the IP address. This feature frees the user from having to remember the numerical IP address of the NAS, and may also provide a small measure of security by protecting the numerical IP address of the NAS. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt4.htm

RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtrattr8.htm

RADIUS Packet of Disconnect

This feature provides a method for terminating a call that has already been connected. This “Packet of Disconnect” (POD) is a RADIUS access_request packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call. A price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

RADIUS Tunnel Attribute Extensions

The RADIUS Tunnel Attribute Extensions feature introduces RADIUS attribute 90 (Tunnel-Client-Auth-ID) and RADIUS attribute 91 (Tunnel-Server-Auth-ID). Both attributes help support the provision of compulsory tunneling in virtual private networks (VPNs) by allowing the user to specify authentication names for the network access server (NAS) and the RADIUS server.

Once a NAS has set up communication with a RADIUS sever, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. Attributes 90 and 91 support Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP).

Attributes 90 and 91 must be included if the RADIUS sever accepts the request and the desired authentication name is different from the default.

Attributes 90 and 91 should be included in an accounting request that contains Acct-Status-Type attributes with values of either start or stop and that pertains to a tunneled session. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtattr90.htm

Redirect-Number Support for RADIUS and TACACS+ Servers

If a telco-return customer is being authenticated by a RADIUS or TACACS+ server, and if the number dialed by the cable modem is being redirected to another number for authentication, Cisco IOS Release 12.1(1a)T1 can include the original number in the information sent to the authentication server. The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. This allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

This feature is enabled with the **aaa nas redirected-station** command and disabled with the **no aaa nas redirected-station** command; other AAA configuration commands also apply as appropriate. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the **non-standard** option to the **radius-server host** command.

Note This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

RFC 2233 Support

Cisco IOS Release 12.2 updates the IF-MIB MIB with support for RFC 2233, which makes the previous RFC 1573 obsolete. This change adds the "ifCounterDiscontinuityTime" attribute and changes the "ifTableLastChange attribute".

In addition, this feature adds support for RFC 2233-compliant link-up and link-down traps. By default, link-up and link-down traps are implemented as given in the CISCO-IF-CAPABILITY.my MIB. To generate link-up and link-down traps as defined by RFC 2233, use the **snmp-server trap link ietf** global configuration command.

This feature was tracked as caveats CSCdp41317 and CSCdp55546, and is introduced in Cisco IOS Release 12.1(2)T.

Router-Port Group Management Protocol

The Router-Port Group Management Protocol (RGMP) feature introduces a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s10/dtrgmp.htm

RSVP Support for Frame Relay

Queueing manages congestion on a router interface or a virtual circuit (VC). In a Frame Relay environment, the congestion point may not be the interface itself, but it may be the VC because of the committed information rate (CIR). For real-time traffic (voice flows) to be transmitted in a timely manner, the data rate must not exceed the CIR or packets might be dropped causing voice quality issues. Frame Relay traffic shaping (FRTS) is configured on the interfaces to control the outbound traffic rate by preventing the router from exceeding the CIR. This means that fancy queueing such as class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), and weighted fair queueing (WFQ), can run on the VC to provide the quality of service (QoS) guarantees for the traffic.

Previously, RSVP reservations were not constrained by the CIR of the flow's outbound VC. As a result, oversubscription could occur when the sum of the RSVP traffic and other traffic exceeded the CIR.

The RSVP support for Frame Relay feature allows RSVP to work with per VC (data link connection identifier (DLCI)) queueing for voice-like flows. Traffic shaping must be enabled in a Frame Relay environment for accurate admission control of resources (bandwidth and queues) at the congestion point; that is, the VC itself. Specifically, RSVP can work with VCs defined at the interface and subinterface levels. There is no limit to the number of VCs that can be configured per interface or subinterface. Refer to the following document for further information:

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

RSVP Support for Low Latency Queuing (LLQ)

RSVP Support for LLQ (low latency queueing) is a network-control protocol that provides a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across networks achieve the desired quality of service (QoS).

RSVP enables real-time traffic (which includes voice flows) to reserve resources necessary for low latency and bandwidth guarantees. RSVP uses weighted fair queuing (WFQ) to provide fairness among flows and to assign a low weight to a packet to attain priority. However, the preferential treatment provided by RSVP is insufficient to minimize the jitter because of the nature of the queuing algorithm itself. As a result, the low latency and jitter requirements of voice flows might not be met in the prior implementation of RSVP and WFQ.

Consequently, a new queuing implementation, referred to as LLQ, was put in place. However, this new queuing implementation, by itself, is not sufficient to provide QoS for VoIP calls. Since the priority queue (PQ) in the queuing system does not distinguish between a VoIP packet of an existing call and a new call (as the queue does not keep the flow state), the queue may drop the packet of the existing call and service the packet of the new call due to strict policing. This means that RSVP is needed to perform admission control to avoid oversubscription of the priority queues. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/rsvp_llq.htm

SDLC SNRM Timer and Window Size Enhancements

The SDLC SNRM Timer and Window Size Enhancements feature introduces a new window size setting for SDLC configurations, and a new timeout setting for the SNRM frame. These enhancements change the operation of SDLC processing on a multidrop line.

Window Size Setting

Prior to this feature, all SDLC addresses on the multidrop had the same window count. Now the window count can be configured on a Physical Unit (PU) or SDLC address level. This enhancement gives a controller a different window size than other devices on the interface, and allows devices attached to the multidrop to be sized individually.

Timeout Setting for SNRM frame

Cisco IOS software SDLC implementation currently utilizes a common response timer (T1) for all outstanding commands. Calculating the maximum frame size and line speed produces a minimum time of 3.5 seconds for receiving acknowledgments; thus, polling stations used for link activation utilize this 3.5-second timer. This is a problem on a multidrop, because stations that do not respond to the SNRM will have 3.5 seconds of downtime-waiting before the next station that is active is polled. This enhancement reduces the time to stations that are waiting idle, as opposed to those that are active. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_4sdlc.htm

Secure Shell Version 1 Integrated Client

Secure Shell (SSH) is a protocol that provides a secure remote connection to another router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The Secure Shell Version 1 Integrated Client feature is an application running over TCP/IP to provide strong authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication.

The SSH client functionality is available only when the SSH server is enabled. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/sshv1.htm

Service Assurance Agent Enhancements

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a mainframe host) by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss and application performance.This feature enables you to perform troubleshooting, problem analysis, and notifications based on the statistics collected by the SA Agent.

The SA Agent Enhancements feature introduces new performance measurement operations and enhancements to assist in the measurement of SLAs. With Cisco IOS Release 12.1(1)T, the SA Agent provides new capabilities that enable you to do the following:

- Measure FTP file download response time using the new FTP operation.
- Monitor one-way latency reporting through enhancements to the Jitter operation.
- Configure a new option for the DHCP operation.
- Manually enable a responder port.
- Verify data for the UDPEcho operation.
- Configure new options for the **rtr schedule** command.
- Restart an operation.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/1dt_saa.htm

Session Initiation Protocol (SIP)

Voice over Internet Protocol (VoIP) currently implements ITU's H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999.

The Cisco SIP functionality equips the Cisco AS5300 access server, and the Cisco 2600 and Cisco 3600 series routers to signal the setup of voice and multimedia calls over IP networks; therefore, the SIP feature, introduced in Cisco IOS Release 12.1(1) T, provides an alternative to H.323 within the VoIP internetworking software. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/0251clmb.htm

Session Initiation Protocol Gateway Call Flows

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks.

SIP uses six request methods:

- INVITE—Indicates a user or service is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server. Gateways do not support the REGISTER method.

The following types of responses are used by SIP and generated by the Cisco SIP gateway:

- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/sipcf.htm

Set ATM CLP Bit

The Cell Lost Priority (CLP) bit in the ATM header of a cell provides a method of controlling the discarding of cells in a congested ATM environment. A CLP bit contains two settings: 0 or 1. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0.

Before the introduction of the ATM CLP Setting feature, the CLP bit was automatically set to 0 when Cisco routers converted packets into ATM cells for ATM networks.

The ATM CLP Setting feature allows users to control the CLP bit setting on routers with the PA-A3 port adapter. The CLP bit is set on each packet individually, and the default CLP bit setting is 0. The application of the ATM CLP Setting feature changes the CLP bit setting to 1. Therefore, users have the option to leave each packet with the default CLP bit setting of 0 or to establish a new CLP bit setting of 1.

ATM CLP Setting is documented as part of the Class-Based Packet Marking feature.

Settlement for Packet Telephony with Roaming and Multiple Roots

This is the second release of Cisco's Open Settlement Protocol (OSP) features. Some settlement vendors have required roaming users to be authenticated and accounted for by the settlement clearinghouse. Therefore, this IOS Release 12.2 introduces two new features, roaming and multiple roots.

- Roaming—A user is roaming when s/he dials in a gateway which is not his/her home gateway. A home gateway belongs to the user's service provider. Usually, the subscriber is billed with additional charges when making roaming calls The settlement server and the service provider need to know when a user is roaming or not in order to create accurate billing statements. A roaming user has to be authenticated before the call can go through the gateway. Both AAA and the settlement server can authenticate a roaming user. If AAA fails to authenticate a roaming user, the roaming call has to be routed to a settlement server. If the settlement server can not authenticate the user, the call is terminated.

  The roaming feature is configured by:

  - Setting the roaming patterns to determine if a user is roaming.
  - Setting the roaming capability in the settlement provider.
  - Setting the roaming capability in the dial peer.
  - Forcing a call to be routed via a settlement server in a dial peer.
- Multiple Roots—The Multiple Roots feature is based on the Cisco security and public key infrastructure (PKI) technology. For in depth information about Security, refer to the *Cisco Security Configuration Guide*.

  The multiple roots feature allows a settlement server to use one certificate for a Secure Socket Layer (SSL) handshake and a different certificate for token signing.

Settlement Plus Roaming and PKI Multiple Roots on Cisco Access Platforms (Settlements for Packet Voice, Phase 2)

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. Two new features, Roaming and Multiple Roots have been added in Cisco IOS Release 12.2 to enhance the OSP. The VoIP/Open Settlement Protocol (OSP) feature offers the ability to authorize, route calls, and billings between two different ISPs via a trusted third party, the settlement clearing house, which is the OSP server. Cisco has built this OSP client on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms, and partnered with a few companies (TransNexus, GRIC, etc.) that provide OSP servers. The code for this feature is an encrypted image.

Note Before you can download 56-bit or 56i encryption images, you must first go through the entitlement process. This process makes sure your system is coming from a registered DNS address and that you're not coming from an encryption-restricted country (Iraq, Libya, etc.). You (and your customers) can entitle yourselves by filling out the forms located at the following URL: http://www.cisco.com/kobayashi/library/12.0/.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/0123box2.htm

SGCP Call Control Protocol Support on the Cisco MC3810 and 3600 series routers

Simple Gateway Control Protocol (SGCP) enables intelligent external call agents to control gateways in Voice over IP (VoIP) environments. Gateways include trunking and residential gateways. Call agents include Telecordia SM 1.5 and third-party products. This release supports SGCP Version 1.1+.

SGCP is used in large IP networks typical of competitive local exchange carriers (CLECs) and Internet exchange carriers (IXCs). Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/sgcp_2t.htm

SNMP Cable Modem Remote Query

The feature provides a new MIB, SNMP Cable Modem Remote Query, so that the cable modem termination system (CMTS) cable modem (CM) poller and the CMs' status polled from the CMTS CM poller can be configured and queried via SNMP.

A new CLI command has been implemented for turning on the trap:

snmp-server enable cable cm-remote-query

Note In the release notes for Cisco IOS Release 12.1(2), this feature was referred to as CISCO-DOCS-REMOTE-QUERY-MIB

SNMP Enhancements

Cisco IOS Release 12.2 adds support for RFC 2669 and RFC 2670 to the DOCS-CABLE-DEVICE-MIB and DOCS-IF-MIB MIBs, respectively.

SNMP Support for IOS vLAN Subinterfaces

This enhancement provides sparse table support for fastethernet subinterfaces similar to what is currently provided for frame-relay subinterfaces. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtsnmpvl.htm

Source Specific Multicast (SSM)

The Source Specific Multicast (SSM) feature is an extension of IP multicast, where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

Source specific multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast lite suite of solutions targeted for audio and video broadcast application environments.

This feature module introduces the following Cisco IOS components that support SSM:

- PIM SS (PIM Source Specific)
- Internet Group Management Protocol Version 3 lite (IGMPv3lite)
- URL Rendezvous Directory (URD)

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtssm.htm

SSH Version 1 Server Support

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

State-Refresh

The **state-refresh** command prevents the periodic timeout of prune state in routers, greatly reducing the reflooding of multicast traffic down the pruned branches that expire periodically. It also causes topology changes to be realized quicker than the traditional three-minute timeout.

T1/E1 Alarm Conditioning for Switched Calls and Permanent Connection Trunks

The T1/E1 Alarm Conditioning for Switched Calls and Permanent Connection Trunks feature provides status monitoring on T1/E1 PBX voice interfaces for permanent trunk connections created using the Cisco connection trunk command (private lines and tie-lines) and for switched calls. The feature supports operation with channel associated signaling (CAS) only; it does not support common channel signaling (CCS). Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtte1alm.htm

T.37/T.38 Fax Gateway

Previously, Store and Forward Fax was supported only on modem cards while voice applications ran on the C542 Digital Signal Processing Module (DSPM) and C549 DSPMs that populated Cisco AS5300 Voice Feature Cards (VFCs). Each type of call required different technologies. With this software release, a single DSPM technology will support:

- Voice, fax relay, and Store and Forward Fax on both the C542 and C549 DSPM and the same voice port.
- Dynamic switching from one application to another in the same call (IVR, voice, fax relay, and Store and Forward Fax).

When the Cisco AS5300 is equipped with VFCs, it supports carrier-class VoIP and fax over IP services. Since the Cisco AS5300 is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and voice activity detection (VAD)/silence suppression. There is an interactive voice response (IVR) application that provides voice prompts and digit collection in order to authenticate the user and identify the call destination.

The VFC is a coprocessor card with a powerful reduced instructions set computing (RISC) engine and dedicated, high-performance Digital Signal Processors (DSPs) to ensure predictable, real-time voice processing. The design enables streamlined packet forwarding. The Cisco AS5300 supports two VFCs, which are scalable up to 96 E1 or 120 T1 voice connections within a single chassis.

Refer to the following document for further information:

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

T.38 Fax Relay for VoIP H.323

T.38 Fax Relay for VoIP H.323 provides standards-based fax relay protocol support for H.323 gateways and gatekeepers. T.38 is an ITU-T recommended standard for fax relay and has been implemented on Cisco 2600, Cisco 3640, and Cisco MC3810 multiservice gateways. Since T.38 is a standards-based implementation for fax relay, Cisco gateways and gatekeepers are able to interwork with third-party H.323 devices that support T.38 protocol. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_t38fx.htm

TCP Clear Performance Optimization

This feature provides inbound and outbound performance optimization for America Online (AOL) users of wholesale dialing services.

First introduced in Cisco IOS Release 12.1(1)AA, this feature is designed to provide more efficiency in the data transfers for AOL users who are using a Cisco network access server (the Cisco AS5800) to communicate with a wholesale dial carrier. It permits the Cisco AS5800 platform to support the maximum number of connections provided by two T3 connections (that is, 1344 connections) running the TCP Clear protocol with typical traffic loads. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_tcpcl.htm

TN3270 Server Connectivity Enhancements

The TN3270 Server Connectivity Enhancements feature, an enhancement to the existing TN3270 Server feature, provides the following new functions:

- Dynamic LU naming
- Inverse DNS nailing
- TN3270 Server security enhancements

Refer to the following document for further information:

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

Traceroute Enhancement for MPLS

The Traceroute Enhancements for MPLS feature introduces two new commands that enable you to manage the time to live (TTL) field in an MPLS header.

- The **mpls ip ttl-expiration pop** command lets you specify how a packet with an expired time to live (TTL) value is forwarded. You can specify that the packet be forwarded by the global IP routing table or by the packet's original label stack. The forwarding method is determined by the number of labels in the packet. You specify the number of labels as part of the command. If the packet contains the same or fewer labels than you specified, it is forwarded through the use of the global IP routing table. If the packet contains more labels than you specified, the packet is forwarded through the use of the original label stack.

- The **mpls ip propagate-ttl** command controls the generation of the time to live (TTL) field in the MPLS header when labels are first added to an IP packet. By default, this command is enabled, which means the TTL field is copied from the IP header. The command allows a traceroute command to show all the hops in the network.

  Use the no form of the **mpls ip propagate-ttl** command to use a fixed TTL value (255) for the first label of the IP packet. This hides the structure of the MPLS network from a traceroute command. You can specify the types of packets to be hidden by using the forwarded and local arguments. Specifying **no mpls ip propagate-ttl forwarded** allows the structure of the MPLS network to be hidden from customers but not from the provider. This is the most common application of the command.

Transparent CCS and Frame Forwarding Enhancements on the Cisco MC3810

The Transparent CCS (T-CCS) feature provides a way to interconnect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) when the Private Integrated Services Network Exchange (PINX) does not support QSIG, or when the PINX uses a proprietary solution. Transparent CCS allows the connection of two PBXs with T1 or E1 interfaces that use one CCS protocol without the need for interpretation of CCS signaling for call processing. A PBX PRI group is transported transparently through the data network and the feature preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PINXs are not routed, but follow a preconfigured route to the destination. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_tccs.htm

Transparent Common Channel Signalling (T-CCS)

Transparent Common Channel Signalling (T-CCS) allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported CCS protocol without the need for interpretation of CCS signaling for call processing. T1/E1 traffic is transported transparently through the data network and the feature preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but follow a preconfigured route to the destination. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_tccs.htm

Trunk Conditioning Enhancements

Cisco MC3810 series concentrators support additional trunk-conditioning commands that specify various trunk-conditioning timing, signaling, and transmission options.

These additional commands provide enhanced control over rerouting of calls in cases of trunk failure, and increased bandwidth availability due to suppression of voice packets on out-of-service trunks. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dttnkcnd.htm

Trunk Conditioning for FRF.11 and Cisco Trunks

Trunk Conditioning for FRF.11 and Cisco Trunks is an enhancement that adds the following capabilities to the trunk conditioning feature on the Cisco 2600 and 3600 series routers and Cisco MC3810 series concentrators:

- Busyout of ports interfacing with a local PBX if a network trunk is out of service (OOS)
- Suppression of voice traffic when no calls are in progress or when the network trunk is OOS

This feature applies to analog telephony connections and digital T1/E1 using CAS/robbed-bit "ABCD" signaling. It does not apply to digital T1/E1 connections using CCS type signaling. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_tcond.htm

Turbo Access Control Lists

Access control lists (ACLs) are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include:

- For ACLs larger than 3 entries, the CPU load required to match the packet to the pre-determined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.
- The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

Refer to the following document for further information:

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

UDLR Tunnel ARP and IGMP Proxy

Most protocols in the Internet assume that links are bidirectional. In particular, routing protocols used by directly connected routers no longer behave properly in the presence of a unidirectional link, such as a satellite link. The Unidirectional Link Routing feature, introduced in Cisco IOS Release 12.0(3)T, enables a router to emulate the behavior of a bidirectional link for operation of IP over unidirectional links.

The unidirectional link routing (UDLR) enhancements introduced in Cisco IOS Release 12.1(5)T include enhancements to the existing UDLR tunnel mechanism and the addition of the Internet Group Management Protocol (IGMP) proxy mechanism. Refer to the following document for further information:

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

uOne (Unified Messaging) on Cisco 3660 Multiservice Platforms

Networks that use a Cisco 3660 Multiservice Platform as a VoIP gateway can now offer uOne, or unified messaging, service to subscribers. uOne consolidates voice and e-mail services on a single IP network, allowing subscribers to send, receive, and manage messages from any access device—whether telephone or PC—regardless of message type and independent of location or time. It allows the user to access, send, forward, and reply to messages, make calls, and provision options. Calls to uOne terminate on a PC called the Gateserver, which is the unified messaging application server. This server then interfaces with a message store and a directory. uOne is based on a standards-based, open-protocol infrastructure and is highly scalable. Note that fax messaging is not supported on the Cisco 3660 at this time.

Cable Subinterfaces and Interface Bundling

Cisco uBR7200 series software supports the definition of logical network layer interfaces over a cable physical interface or a bundle of cable interfaces. The system also supports subinterface creation on either a physical cable interface or a bundle of cable interfaces. This allows a service provider to share one IP subnet across multiple cable interfaces that are grouped into a cable interface bundle. All of the cable interfaces on a Cisco uBR7200 Series Universal Broadband Router can be grouped into a single bundle so that only one subnet is required for each router. This eliminates the requirement that a separate IP subnet be used for each individual cable interface. This in turn avoids the performance, memory, and security problems that result if a bridging solution is used to manage subnets, especially for a large number of subscribers.

Note Cable interface bundling is applicable only in two-way cable configurations. It is not supported in telco-return configurations.

The CMTS administrator can perform the following tasks:

- Define subinterfaces on a cable physical interface and assign Layer 3 configurations to each subinterface.
- Bundle a group of physical interfaces and define a bundle master Layer 3 configuration or define subinterfaces on the bundle master and give each subinterface Layer 3 configurations.

The command to create a subinterface over a cable interface is the same as that defined by Cisco IOS for other software applications:

interface cable *x/y.n*

where *x* is the slot number, *y* is the port number, and *n* is the subinterface number.

Two new commands implement the bundling feature:

- **[no] cable bundle** *number* [master] — Configures cable interfaces into bundles.
- **show cable bundle** *number* **forwarding table —** Displays all the currently known cable devices in the bundle.

Administrators can create subinterfaces on cable interfaces or cable interface bundles to support VPN. Each subinterface can be assigned to a specific pool of IP addresses, mapping that subinterface to a particular VPN customer network. A Generic Routing Encapsulation (GRE) tunnel can also be created between the Cisco uBR7200 series router and the router that serves as the VPN customer gateway.

When a cable modem registers with the Cisco uBR7200 Series Universal Broadband Router, its IP address is used to identify the subinterface being used by the cable modem; this information is used to associate the Service Identifier (SID) assigned to the modem to that subinterface (and thus the VPN customer network).

Note Cisco IOS Release 12.1(1a)T1 and Release 12.1(3)T do not include MPLS support as part of its VPN support on the cable subinterfaces. Cisco IOS Release 12.1(2)T and Release 12.1(5)T and higher releases do support MPLS over VPN.

A subinterface can be created on any cable interface that is not part of a cable interface bundle. A subinterface can also be created on the master cable interface bundle; subinterfaces cannot be created on non master bundles.

Subinterfaces support the following existing cable interface commands:

- **cable arp**
- **cable dhcp-giaddr**
- **cable helper-address**
- **cable ip-broadcast-echo**
- **cable ip-multicast-echo cable proxy-arp**
- **cable source-verify**

Caution Configure an IP address on the master interface only. An attempt to add an interface to a bundle will be rejected if an IP address is configured and the interface is not specified as a master interface.

When bundling cable interfaces, only the interface configured to be the bundle master is allowed to have subinterfaces. An interface that has subinterface(s) defined over it will not be allowed to be part of a bundle.

MIB objects on cable interface bundles are not supported as of the date of this publication.

For more information on cable bundling, refer to the chapter *Understanding System Operations* of the *Cisco uBR7200 Series Software Configuration Guide*.

V.110 Support for 3600 Digital Modems

This feature implements the V.110 protocol on the digital modem network modules. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtv110dm.htm

Virtual Profile CEF Switched

Using the Virtual Profile CEF Switched feature you can apply a per-user level configuration onto an Async and ISDN B-channel interface. VP CEF previously supported process switching and low-end system fast switching.

VP CEF switching provides improved performance by using Forwarding Information Base (FIB) to look up a route for a forwarding packet. FIB look-ups are superior to the cache tables used in fast switching because they are populated by routing topology rather than traffic and use the optimal switching decision.

VP CEF switching enables you to use VP in other new technologies that requires CEF switching, such as MPLS/BGP VPN, and dCEF with ISDN interfaces. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtvpcef.htm

VIC-2BRI-NT/TE, MC3810-BVM4-NT/TE

The ISDN BRI NT/TE voice interface card (VIC-2BRI-NT/TE) for the Cisco 2600 and Cisco 3600 series and the ISDN BRI Voice Module (BVM4-NT/TE) for the Cisco MC3810 enable Cisco IOS software to replicate the public switched network interface to a PBX that is compatible with European Telecommunications Standards Institute (ETSI) NET3 and QSIG switch types.

Before this feature, customers with PBXs that implement only the BRI TE interface, have had to make substantial hardware and software changes on the PBX to implement the NT interface. The implementation of an NT interface on the router allows the customer to connect ISDN PBXs and Key Systems to a multiservice network with a minimum of configuration changes on the PBX.

VIP-Based Distributed FRF.11/12

The Voice Over Frame Relay using FRF.11 and FRF.12 capabilities currently available in Cisco IOS Release 12.1 T are now available, with some modifications, on VIP-enabled Cisco 7500 series routers. The new feature is called VIP-Based Distributed FRF.11 and FRF.12 (VIP-Based FRF.11 and FRF.12).

Refer to the following document for further information:

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

VIP-Based WFQ Support for RSVP

In earlier software releases, Resource Reservation Protocol (RSVP) on Cisco 7500 series routers would leverage Route Switch Processor-based (RSP-based) weighted fair-queuing to guarantee bandwidth to RSVP flows.

RSVP now interoperates with distributed weighted fair-queuing (dWFQ), thus offloading the RSP of the overhead of the queueing function and improving RSVP scalability. RSVP support of dWFQ is transparent to the user.

Virtual Private Network (VPN) Module for the Cisco 1700 Series

The Cisco 1700 series routers, which includes the Cisco 1720 and 1750 models, are modular access routers for small and medium businesses and small branch offices. Cisco 1700 routers deliver routing, firewall, and VPN functions for Internet data and voice applications.

The VPN module, which fits into a slot inside the Cisco 1720 or 1750 chassis, assists the host processor by accelerating layer 3 IP Security (IPSec) data and voice encryption and decryption. The VPN module supports DES and 3DES encryption algorithms, MD5 and SHA-1 hashing, and Diffie-Hellman key generation.

The VPN module encrypts data using DES and 3DES algorithms at speeds suitable for full duplex T1/E1 serial connections (4 megabits per second for 1518-byte packets). Equipped with a VPN module, a Cisco 1700 router supports up to 100 encrypted tunnels for concurrent sessions with mobile users or other sites. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_vpn17.htm

Virtual Switch Interface Master MIB

The Virtual Switch Interface Master MIB provides a standardized vehicle for monitoring the operation of the VSI protocol within a Label Switch Controller (LSC). It also displays the results of the protocol operations. Specifically, with the VSI Master MIB you can monitor:

- Connections between an LSC and the switch it controls
- The status of the interfaces in the switch
- Virtual circuits (VCs) that are maintained across the interfaces

With the VSI Master MIB you can enlist Simple Network Management Protocol (SNMP) to monitor the status of the VSI protocol and the results of its operations.

This MIB is primarily oriented toward management of Multiprotocol Label Switching (MPLS) systems. As such, the MIB resides in routers that are also LSCs. These are routers that are VSI capable, and whose network control application is MPLS. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/mstrmib.htm

Voice Busyout Enhancements

The local voice busyout feature provides a way to busy out a voice port if a monitored network interface changes state. When a monitored interface changes to a specified state—to out-of-service or in-service—the voice port presents a seized/busyout condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route.

Local voice busyout is supported on analog and digital voice ports using channel associated signaling (CAS).

This feature allows you to perform the following tasks:

- Configure individual voice ports to enter the busyout state whenever specified network interfaces go out of service or come into service
- Force individual voice ports into the busyout state
- Define the voice-port actions for the busyout state
- Force one or more DS0 timeslots on a controller into the busyout state

Note This feature is different from busy-back, the signal sent from the network to the calling party to indicate a busy (or congested) state along the route.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_boenh.htm

Voice Over ATM

Voice over ATM on Cisco 3600 series routers extends support for Voice over ATM, previously available only on the Cisco MC3810 to the Cisco 3600 series routers. Voice over ATM enables a Cisco 3600 series router to carry voice traffic (for example, telephone calls and faxes) over an ATM network.

Voice over ATM enables a Cisco 3600 to carry voice traffic, (for example, telephone calls and faxes) over an ATM network by using ATM encapsulation AAL5.

Restrictions:

Voice over ATM on the Cisco 3600 series requires that you install one of the following modules:

- Multiport T1/E1 ATM network module with IMA

  The Multiport T1/E1 ATM network module with IMA supports up to 8 T1/E1 lines. For more information, refer to the Cisco IOS Release 12.0(5)T online document Configuring Multiport T1/E1 ATM Network Modules with Inverse Multiplexing over ATM on Cisco 2600 and 3600 Series Routers.

- OC3 ATM Network Module

  The OC3 ATM Network Module supports one OC3 line. For more information about the Digital T1 packet voice trunk network modules, refer to the Cisco IOS Release 12.0(3)T online document ATM OC-3 Network Module for the Cisco 3600 Series Routers.

- Voice over ATM on the Cisco 3600 series supports ATM encapsulation AAL5 only. AAL2 is not supported.
- Voice over ATM Switched Virtual Circuits (SVCs) are not supported in this release.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtvoatm.htm

Voice over ATM with AAL2 Trunking

Voice over ATM with AAL2 trunking enables the Cisco MC3810 series concentrators to carry voice traffic (for example, telephone calls and faxes) over ATM networks using AAL2.

This feature provides the following improvements to the Cisco MC3810 capabilities:

- Increased quality of service (QoS) capabilities
- Standards-based transport of voice over ATM
- Bandwidth-efficiency
- Robust architecture

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_aal2v.htm

Voice Over Frame Relay

Voice over Frame Relay (VoFR) enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. Configuration information is available in the “Cisco IOS Multiservice Applications Configuration Guide” and “Cisco IOS Multiservice Applications Command Reference” publications.

Before configuring VoFR on a router, you must configure your Frame Relay backbone network. As part of your Frame Relay configuration, you need to configure the map class, and the Local Management Interface (LMI) among other Frame Relay functionality. For more information about Frame Relay configuration, refer to the *Cisco IOS Wide-Area Networking Configuration Guide*.

The Cisco VoFR implementation allows the following types of VoFR calls:

- Static FRF.11 trunks
- Switched VoFR calls:
  - Dynamic switched calls
  - Cisco-trunk (private line) calls

Voice over Frame Relay Configuration Updates Using FRF.11 and FRF.12

Voice over Frame Relay functionality has been updated in this release, so that configuration on all supported platforms is nearly identical. In Cisco IOS Release 12.0(4)T, when support for Voice over Frame Relay Using FRF.11 and FRF.12 was introduced, configuration procedures were different depending on the router platform used.

Some commands introduced in earlier Cisco IOS releases have been removed or modified. This document describes the configuration procedures effective in this release.

In addition, this release provides support for digital voice calls for Voice over Frame Relay on the Cisco 2600 and 3600 series routers. In previous releases, the Cisco 2600 and 3600 series only supported analog voice calls for Voice over Frame Relay.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtvofr.htm

Voice over IP

Voice over IP (VoIP) enables a Cisco MC3810 concentrator to carry voice traffic (for example, telephone calls and faxes) over an IP network. Voice over IP is primarily a software feature; however, to support this feature, a Cisco MC3810 must be equipped with a digital voice module (DVM) or an analog voice module (AVM). The Cisco MC3810's LAN/WAN multiservice routing capabilities provide analog and digital (T1/E1) VoIP gateway capabilities for packetized voice traffic.

In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because it is a delay-sensitive application, you need to have a well-engineered network end-to-end to successfully use Voice over IP. Fine-tuning your network to adequately support Voice over IP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection. Refer to the following information for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtvoip38.htm

Voice Port Enhancements

The Cisco 2600 series and 3600 series routers and Cisco MC3810 series multiservice access concentrators support data, voice, and video transport to varying degrees. Numerous voice port commands and features that were previously limited to one or two of these product series have been extended to additional product series, and differences in configuration commands have been reduced or eliminated.

These enhancements provide the following improvements:

- Increase the voice capabilities of the product series gaining new features
- Increase the level of interoperability between the product series

- Simplify the configuration procedures

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtvoxprt.htm

Voice Port Testing Enhancements

Voice port testing enhancements expand the capabilities to analyze and troubleshoot voice ports on the Cisco 2600 and 3600 series routers and MC3810 series concentrators. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_tstvp.htm

VoIP Call Admission Control using RSVP

The VoIP Call Admission Control using the Resource Reservation Protocol (RSVP) feature synchronizes with H.323 Version 2 (Fast Connect) setup procedures to guarantee that the required QoS for VoIP calls is maintained across the IP network. Before Cisco IOS Release 12.1(3)XI, VoIP gateways used H.323 Version 1 (Slow Connect) procedures when initiating calls requiring bandwidth reservation. This feature, which is enabled by default, allows gateways to use H.323 Version 2 (Fast Connect) for all calls, including those requiring RSVP.

WCCP Redirection on Inbound Interfaces

The WCCP Redirection on Inbound Interfaces feature adds support to Cisco IOS software for the redirection of Web Cache Coordination Protocol (WCCP) traffic on inbound interfaces. Prior to this release, WCCP Version 2 was implemented as an output feature only, with packets classified by WCCP after a routing table lookup. With Cisco IOS release 12.1(3a)T1, you can now configure an interface for inbound redirection using CEF, dCEF, Fast forwarding, and Process forwarding paths. WCCP redirection on inbound interfaces avoids the processing overhead created by CEF on outbound interfaces. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_wccpi.htm

Wildcard Pre-Shared Key Enhancement

A wildcard pre-shared key allows a group of remote users with the same level of authentication to share an IKE pre-shared key. The remote peer's pre-shared key must match the local peer's pre-shared key for IKE authentication to occur. The term wildcard means that any remote peer with the pre-shared key can access the local peer, regardless of the remote peer's IP address assignment. The term pre-shared key is a shared secret key exchanged during IKE negotiation.

A wildcard pre-shared key is usually distributed through a secure out-of-band channel. In a remote peer-to-local peer scenario, any remote peer with the IKE pre-shared key configured can establish IKE security associations (SAs) with the local peer.

The wildcard pre-shared key feature is an enhancement to the crypto isakmp key global configuration command. With a wildcard IP address of 0.0.0.0 and pre-shared key authentication method configured on the local router, the local router can authenticate the IKE SA with any remote peer that has a matching wildcard pre-shared key. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/wcpsk.htm

New Hardware Features in Release 12.2(1)

The following features are supported in Cisco IOS Release 12.2.

- Advanced Integration Modules (AIM) and Network Module (NM)
- ATM OC-3 Network Modules with Circuit Emulation
- ATM T3 and E3 Network Modules
- Broadband Wireless—Point-to-Point
- Cable Modem Card (MC16E)
- Cisco 2650 and 2651 Routers
- Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers
- Cisco Cable Clock Card
- Cisco ICS 7750
- Digital E1 Packet Voice Trunk Network Module Interfaces
- Dynamic Packet Transport OC-12c Port Adapter for 7200
- High-Performance Compression Module
- MC3810-BVM4-NT/TE
- MIX-Enabled 2/4/8 Port Multichannel T1/E1 Port Adapter with CSU/DSU
- Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM
- Network Services Engine
- NPE-400
- OC-12 Dynamic Packet Transport Interface Processor
- One-Port Enhanced ESCON Channel Port Adapter
- PA-GE Gigabit Ethernet Port Adapter
- PA-MC-T3+
- PA-VXB and PA-VXC
- Spectrum Management Cable Modem Card (MC16S)
- Two-Port Moderate-Capacity T1 and E1 Digital Voice Port Adapter
- VIC-2BRI-NT/TE
- VIC-2FXO-M3 Support on the Cisco 1750

Advanced Integration Modules (AIM) and Network Module (NM)

The data encryption Advanced Integration Module (AIM) and Network Module (NM) are hardware Layer 3 (IPSec) encryption modules and provide DES (56-bit) and 3DES (168-bit) IPsec encryption for multiple T1s or E1s of bandwidth. This level of performance is a dramatic increase over that achievable when running IPSec in software on the main CPU of the Cisco 2600 or 3600. These products also have hardware support for DH, RSA, and DSA key generation.

In addition to encryption, the data encryption AIM is intended to increase the security of passwords and various encryption keys over that provided by IOS software and the platform hardware. Specifically, these products have been submitted for Level 2 of the Federal Information Processing Standard (FIPS)

140-1 in general, as well as more stringent levels for some parameters such as Level 3 tamper resistance. For more information see *Installing the Data Encryption AIM in Cisco 2600 Series and Cisco 3600 Series Routers* on Cisco.com.

ATM OC-3 Network Modules with Circuit Emulation

Circuit emulation is a service based on ATM Forum standards that allows communications to occur between AAL1 CES and ATM UNI interfaces, that is, between non-ATM telephony devices (such as classic PBXs or TDMs) and ATM devices (such as Cisco 2600 and 3600 series routers). Thus, a Cisco 2600 or 3600 series router equipped with an ATM OC-3 network module with circuit emulation service offers a migration path from classic T1/E1 data communications services to emulated CES T1/E1 unstructured (clear channel) services or structured (N x 64) services in an ATM network.

The following network modules are available:

- Single port ATM OC-3 multimode network module and circuit emulation service (NM-1A-OC3MM-1V)
- Single port ATM OC-3 single-mode, intermediate reach network module and circuit emulation service (NM-1A-OC3SMI-1V)
- Single port ATM OC-3 single-mode, long reach network module and circuit emulation service (NM-1A-OC3SML-1V)

ATM T3 and E3 Network Modules

Two new ATM network modules are supported on the Cisco 2600 Series and Cisco 3600 Series routers in this release. These network modules support ATM Adaptation Layer 5 (AAL5) and will provide North American 44.736 Mbps ATM T3 services, and European 34.368 Mbps E3 services.

These network modules provide DS3 and E3 ATM connectivity for the Cisco 2600 and 3600 Series routers. These network modules can be used to provide connectivity with campus networks and LAN switches, and long-haul WAN applications. These network modules include support for ATM LANE, RFC1577, RFC1483, TAG switching, and PPP over ATM with full support for both client and server functions. The modules support up to 1,024 simultaneous virtual circuits (VCs) and provide extensive traffic shaping and rate queueing capabilities on a per- VC basis. Use of these modules requires using one of the Cisco IOS Plus feature sets.

The following modules are available:

- Single port ATM T3 network module (NM-1A-T3)
- Single port ATM E3 network module (NM-1A-E3)

Broadband Wireless—Point-to-Point

The Cisco high-speed point-to-point broadband fixed wireless system provides a fixed, dedicated wireless link from one site to another. This link delivers full-duplex data in the Unlicensed National Information Infrastructure (U-NII) band (5.725 to 5.825 GHz).

The broadband fixed wireless system consists of a Cisco uBR7200 Series Universal Broadband Router (Cisco uBR7246 or Cisco uBR7223) and one or more point-to-point wireless modem cards, each with a power feed panel and one or two wireless transverters.

The point-to-point wireless modem cards are installed in a Cisco uBR7200 series router. Each modem card is cabled to a power feed panel installed either in the same equipment rack as the router or mounted on a wall. Cables from the power feed panel are attached to one or two wireless transverters, which are installed on antenna masts. The system is managed using a command-line interface (CLI) or CiscoView.

The Cisco IOS software has a number of new and enhanced commands to support the point-to-point wireless modem card. The point-to-point wireless modem card is also one component of a complete fixed wireless subsystem. For more information about the new commands and additional wireless hardware, refer to the *Cisco uBR7200 Series Wireless Modem Card and Subsystem Installation and Configuration* publication.

Note Not all port adapters are supported with the point-to-point wireless modem card. The HSSI, 10BaseT Ethernet, 100BaseT Ethernet, and serial Frame Relay interfaces are fully supported. The ATM, POS, and Gigabit Ethernet port adapters were not supported with the point-to-point wireless modem card at the time Release 12.1(1a)T1 was released.

Cable Modem Card (MC16E)

The MC16E Cable Modem Card provides one downstream and six upstream connections to the cable network, similar to the MC16C Cable Modem Card, except that it supports the ITU J.83 Annex A physical layer and the proposed EuroDOCSIS (Annex A) standard (Cable Labs ECR RFI-R-98036). The MC16E card has the following differences with the current MC16C card:

- Downstream 36.125 MHz interface, with an 8-MHz DAVIC/DVB channel width and interleave factor of I=12, J=17
- Downstream symbol rate of 6.592 Msymbols/sec at 64 and 256 QAM
- Downstream channel range of 85 to 860 MHz
- Upstream channel range from 5 to 65 MHz
- Supported in the Cisco uBR7200 series MIBs
- Supports EuroDOCSIS-compliant cable modems and set top boxes (STBs)

All cable interface commands have been updated to support the MC16E Cable Modem Card. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtmc16e.htm

Cisco 2650 and 2651 Routers

The Cisco 2650 and Cisco 2651 modular multiservice routers, extend the range of performance options in the widely deployed Cisco 2600 family. These high performance models enable customers to support multiple bandwidth-intensive and latency-sensitive applications concurrently, such as new web applications, broadband WAN services, and converged voice and data infrastructures.

The Cisco 2650 provides a single auto-sensing 10/100Mbps Ethernet port. The Cisco 2651 features dual 10/100 Mbps ports. Both platforms offer increased Flash capacity (up to 32MB) and DRAM capacity (up to 128MB) memory support for extensive access control lists, routing tables and the flexibility of dual software-image back-up support for even the most feature-rich versions of Cisco IOS®.

All current hardware and software features supported on the Cisco 261x and 262x routers will be supported on the Cisco 2650 and 2651 routers.

Note The new Cisco 2650 and Cisco 2651 DRAM DIMMs are NOT COMPATIBLE WITH OTHER CISCO 2600 FAMILY MEMBERS (Cisco 261x and Cisco 262x)! The Cisco 2650 and Cisco2651 use Synchronous DRAM only as opposed to the Cisco 261x, and Cisco 262x which use EDO type DRAM only. DRAM memory for the Cisco 265x models are identified with part numbers starting with MEM2650-xxxxxD as opposed to MEM2600-xxxxxD.

Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000 megabits per second (Mbps) operation and an RJ-45 receptacle for 10 Mbps operation.

The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100 Mbps operation.

I/O controllers support the following features:

- Dual EIA/TIA-232 channels for local console and auxiliary ports
- NVRAM for storing the system configuration and environmental monitoring logs
- Two PC card slots that hold Flash Disks or Flash memory cards for storing the default Cisco IOS software image
- Flash memory for storing the boot helper image
- Two environmental sensors for monitoring the cooling air as it enters and leaves the chassis

Refer to the following document for further information:

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

Cisco Cable Clock Card

The Cisco Cable Clock Card enables the uBR7246 VXR to synchronize to an external T1 timing source and propagate the clock to the downstream DOCSIS-based cable access routers. It is designed for cable networks running VoIP applications.

When installed in the Cisco uBR7246 VXR chassis, the Cisco Cable Clock Card can propagate a national clock signal throughout the router's midplane by locking onto an external T1 signal originating over the PSTN, locking onto a T1 clock signal originating from a port adapter installed in the same chassis, or connecting to a GPS receiver generating a T1 clock signal.

Cisco ICS 7750

The Cisco Integrated Communications System (ICS) 7750 is an IP telephony system that provides managed Web-based communications applications for transforming branch-office and mid-sized business environments into Internet e-businesses. The system is built on the open and scalable Cisco AVVID (Architecture for Voice, Video and Integrated Data).

The Cisco ICS 7750 integrates the functionality of the following voice and data network components:

- Internet Protocol (IP) routing
- Switched Ethernet local area network (LAN) interface
- IP telephony

- Call processing and computer telephony applications

The Cisco ICS 7750 incorporates all of the following elements needed to deliver converged data, voice and video:

- Multiservice router and voice gateways based on Cisco IOS technology
- Application servers running core voice applications
- CallManager software
- Integrated web-based system management in the Cisco ICS System Manager
- A data switching interface for seamless connectivity to recommended Cisco Catalyst quality of service (QoS)-enabled switches

The Cisco ICS 7750 is a six-slot system, which houses any combination of Cisco IOS-based MRPs and/or SPEs. Various combinations of MRP and SPE cards allow a network administrator to customize the configuration to meet voice and data processing needs, such as telephony, in one integrated system. The SAP card provides fault management and events-driven alarms through electronic mail or paging and the SSP card provides Ethernet switching.

The MRP supports both digital and analog voice-trunk gateways and WAN interfaces. The MRP enables businesses to use virtual private network (VPN), firewall, IP Security (IPSec), and QoS for voice and data transmission. The Cisco ICS 7750 system uses the MRP to link to the Public Switched Telephone Network (PSTN) and existing private branch exchanges (PBXs), as well as other common analog devices, such as fax machines and teleconferencing stations. Each MRP card has two slots that accept existing Cisco Voice interface cards (VICs) and WAN interface cards (WICs).

The SPE is a single-board computer that can run Cisco CallManager for intelligent call processing and other core voice applications such as voice mail and auto-attendant, as well as interactive voice response (IVR), unified messaging, automated call distributor (ACD), and Web-based contact center applications.

A Cisco ICS 7750 network includes peripheral hardware components, such as the following:

- Ethernet switches
- Digital Cisco IP Phones
- Analog telephony devices, such as telephones and fax machines

Digital E1 Packet Voice Trunk Network Module Interfaces

Digital E1 packet voice trunk network modules for the Cisco 2600 series routers allow enterprises or service providers, using the equipped routers as customer premises equipment, to deploy digital voice and fax relay. These modules receive constant bit-rate telephony information over E1 interfaces and can convert that information to a compressed format, so that it can be transmitted as Voice over IP (VoIP) and Voice over Frame Relay (VoFR).

Cisco IOS software configuration allows you to set up a variety of applications. Here are a few examples:

- Compressed voice over WANs
- Routing of dialed variable-length digits collected from the Public Switched Telephone Network or PBX for VoIP or VoFR.
- Support for FRF.12 fragmentation and queueing in a VoIP over Frame-Relay network
- Drop and Insert of E1 channels on a E1 trunk to allow some PBX channels to be directed to the PSTN while others are used for compressed VoIP

The following network modules are available:

- Single-Port 30 Channel E1 High-Density Voice Network Module (NM-HDV-1E1-30)

- Single-Port Enhanced 30 Channel E1 High-Density Voice Network Module (NM-HDV-1E130E)
- Dual-Port 60 Channel High-Density Voice Network Module (NM-HDV-2E1-60)

Restrictions

The following restrictions apply to digital E1 packet voice trunk network module configuration:

- Group 4 fax is not supported.
- The high-density voice network module has one slot for a voice/WAN interface card (VWIC); VWICs supply one or two ports. Only the dual-mode (voice/WAN) multiflex trunk cards are supported in the digital E1 packet voice trunk network module, not older VICs.
- Drop-and-Insert capability is supported only between two ports on the same multiflex card.
- Common-channel signaling (CCS) and Primary Rate Interface (PRI) are not supported.
- R2 signaling is not supported.
- Voice over ATM—including AAL5 encapsulation, circuit emulation service (CES), and AAL2—is not supported for VoATM on the Cisco 2600 series router.
- Digital E1 voice is manageable through Simple Network Management Protocol (SNMP) using Release 2.0 of Cisco Voice Manager.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dte1_vo.htm

Dynamic Packet Transport OC-12c Port Adapter for 7200

The dual-width OC-12c Dynamic Packet Transport (DPT) port adapter is available on Cisco 7200 series routers and Cisco 7200 VXR series routers. The DPT is an OC-12c interface used in Cisco 7200 series and Cisco 7200 VXR routers to provide a shared IP-over-SONET capability.

The following benefits are offered by the DPT for the Cisco 7200 and Cisco 7200 VXR series routers:

- Accommodates large-scale network topology
- Applicable IEEE 802.3 standards
- Supports Intelligent Protection Switching (IPS)

High-Performance Compression Module

The high-performance compression module (HCM) enables the Cisco MC3810 to provide greater density for voice calls. There are two types of high-performance compression modules, the HCM2 and the HCM6, and each provides voice compression according to the codec specified when the Cisco MC3810 is configured. Table 7 shows the number of voice channels each type of compression module can support.

Table 24 HCM Voice Call Density

Type	Codec Packaging Complexity	Voice Channels per HCM
HCM2	High complexity	4
	Medium complexity	8
HCM6	High complexity	12
	Medium complexity	24

MC3810-BVM4-NT/TE

The ISDN BRI Voice Module (BVM4-NT/TE) for the Cisco MC3810 enables Cisco IOS software to replicate the public switched network interface to a PBX that is compatible with European Telecommunications Standards Institute (ETSI) NET3 and QSIG switch types.

MIX-Enabled 2/4/8 Port Multichannel T1/E1 Port Adapter with CSU/DSU

The Multiservice Interchange (MIX) port adapter adds time-division multiplexing (TDM) connection capabilities that enable you to combine types of traffic traveling through Cisco 7200 VXR series routers. On the Cisco 7200 VXR series router, MIX enables TDM connections between two ports on the same MIX-enabled port adapter.

MIX functions permit connection of TDM streams to support applications that are sensitive to time delay, such as voice and video, and provide customers the flexibility to manage this traffic through the router as traditional TDM connections or in a packet-based format. In addition, Extended Availability Drop and Insert (EADI) capabilities have been added, which allow MIX connections to stay up through a router reload.

The 2/4/8 Port Multichannel T1/E1 port adapters are now enabled with a Multiservice Interchange (MIX) card. The MIX card enables the connection of TDM traffic from any port on a MIX-enabled port adapter to any other port on the same MIX-enabled port adapter on the Cisco 7200 VXR platform.

The following port adapters are currently MIX-enabled:

- PA-MCX-2TE1
- PA-MCX-4TE1
- PA-MCX-8TE1

Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM

The inverse multiplexing over ATM (IMA) port adapter is a single-width port adapter that allows Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers to support inverse multiplexing over ATM. These port adapters support WAN uplinks at speeds ranging from 1.544 Mbps to 12.288 Mbps for T1 connections and from 2.048 Mbps to 16.384 Mbps for E1 connections.

With the scalable Cisco ATM IMA solution, network designers and managers can deploy only the bandwidth they need, using multiple T1 or E1 connections instead of more expensive T3 or OC-3 lines to bridge LANs and ATM WAN applications. Enterprises and branch offices can aggregate traffic from multiple lower-bandwidth physical transmission media, such as T1 or E1 pipes, to transmit voice and data at high-bandwidth connection speeds.

Network Services Engine

The Network Services Engine (NSE) is the latest processor engine for Cisco 7200 VXR routers. The NSE delivers wire rate OC-3 throughput while running concurrent high-touch WAN edge services. It is the first Cisco processing engine to offer integrated hardware acceleration increasing Cisco 7200 VXR series system performance by 50 to 300% for combined “high touch” edge services. NSE takes advantage of a new technology called Parallel eXpress Forwarding (PXF).

NPE-400

NPE-400 is a new version of network processing engine for Cisco 7200 series routers with the following enhancements:

- RM7000 microprocessor that operates at an internal clock speed of 350 MHz
- Up to 512 MB ECC SDRAM
- 100 MHz SysAD and memory bus speed
- 4 MB Layer 3 cache

The NPE-400 leverages technology from the NPE-225 and NSE-1 to provide a higher performance NPE card.

OC-12 Dynamic Packet Transport Interface Processor

The OC-12c Dynamic Packet Transport (DPT) Interface Processor is available on Cisco 7500 series routers. The DPT is an OC-12c interface that uses second-generation Versatile Interface Processor (VIP2) technology to provide a shared IP-over-SONET capability and it complies with IEEE 802.3 specifications for multicast and broadcast media. The DPTIP assembly consists of a VIP2 with a dual-width DPT interface processor permanently attached to it.

One-Port Enhanced ESCON Channel Port Adapter

The High Performance Enterprise Systems Connection (ESCON) port adapter provides a single channel interface for Cisco 7200-series routers. In some situations, this interface can eliminate the need for a separate front-end processor (FEP). The HP ESCON PA contains one ESCON I/O connector.

The HP ESCON PA is a high-speed port adapter. A Fast Ethernet port adapter is an example of another type of high-speed port adapter. A single Cisco 7200-series router can support up to three high-speed port adapters.

The HP ESCON PA provides a single channel attachment interface for connecting Cisco 7200 series routers to an ESCON director or to a mainframe channel.

A mainframe channel (referred to as a channel) is an intelligent processor that manages the protocol on the communications media and controls the data transfer to and from the main central processing unit (CPU) storage. Devices called input/output processors (IOPs) communicate between the host CPU and the channel. One IOP controls multiple channels. There is no relationship between the number of CPUs and the number of IOPs.

The channel relieves the mainframe CPU of direct communication with input/output (I/O) devices, which saves processing cycles and allows data processing and communications tasks to run concurrently. Channels use one or more channel paths as the links between mainframes and I/O devices. I/O devices are connected directly to control units, which provide the logical capabilities required to operate and control the I/O devices.

For more information refer to the *PA-4C-E 1-Port High-Performance ESCON Channel Port Adapter* Installation and Configuration guide.

PA-GE Gigabit Ethernet Port Adapter

The single port Gigabit Ethernet Port Adapter (PA-GE) provides a Gigabit Ethernet connection for the Cisco 7200 series router. This port adapter, which offers moderate performance, is suitable for campus, enterprise edge and wide-area network (WAN) aggregation applications. When used on the campus, the

Cisco 7200 series router with the PA-GE connects the enterprise WAN to the Gigabit Ethernet campus backbone. At the enterprise edge, the PA-GE connects the WAN to the Gigabit Ethernet campus backbone. When the Cisco 7200 series router is used for WAN aggregation, the PA-GE provides intra-pop connectivity between the router and high-speed WAN core devices, such as the Cisco 12000 series router. The PA-GE may be inserted into any open port adapter slot on Cisco 7200VXR routers.

PA-MC-T3+

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections using BNC connectors. Each T3 interface can be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

An unchannelized T3 provides a single serial interface data channel that may be configured to use all of the T3 bandwidth or a fractional portion of it. This mode is compatible with several vendors of fractional (subrate) DS3 data service units (DSUs).

The PA-MC-2T3+ has the following features and physical characteristics:

- Supports both channelized and unchannelized operations.
- Transmits and receives data bidirectionally at the T3 rate of 44.736 Mbps.
- Conforms to relevant specifications for DS3 (Digital Signal Level 3) circuits.
- Supports RFC 1406 and RFC 1407 (CISCO-RFC-1407-CAPABILITY.my). For RFC 1406, Cisco supports all tables except the FarEnd table.

For more information refer to the *PA-MC-2T3+ Multichannel T3 Port Adapter Installation and Configuration* guide.

PA-VXB and PA-VXC

The PA-VXB and the PA-VXC are multichannel packet voice port adapters that allow Cisco 7200 series, Cisco 7200 VXR, and Cisco 7500 series routers to become dedicated packet voice hubs or packet voice gateways that connect to both private branch exchanges (PBXs) and the Public Switched Telephone Network (PSTN). This allows packet voice and packet fax calls to be placed over the wide-area network (WAN) and sent through the gateway into the traditional circuit-switched voice infrastructure.

The PA-VXB and the PA-VXC are single-width port adapters with two universal ports that are configurable for either T1 or E1 connection. The PA-VXB contains 12 high-performance digital signal processors (DSPs) that support up to 48 medium-complexity or 24 high-complexity channels of compressed voice. The PA-VXC contains 30 high-performance DSPs that support up to 60 medium-complexity or 120 high-complexity channels of compressed voice.

In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because Voice over IP is a delay-sensitive application, you must have a well-engineered network end-to-end to use it successfully. Fine-tuning your network to adequately support Voice over IP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

Spectrum Management Cable Modem Card (MC16S)

The software for the MC16S Spectrum Management Cable Modem Cards is a driver running on the Cisco uBR7200 Series Universal Broadband Routers. Using a Peripheral Component Interconnect (PCI) interface, the Universal Broadband Router line card software interacts with the cable modem card. Data is passed back and forth, as direct memory access (DMA) transfers, from the Cisco uBR7200's memory to the cable modem card.

Additionally, the MC16S Cable Modem Cards support Universal Broadband Router line card management and control with the modem card Management Information Bases (MIBs), Media Access Control (MAC) control software, and logical link management software based on DOCSIS standards.

In addition to its cable modem card, the MC16S provides dedicated hardware support for advanced spectrum management through a daughter spectrum management card. This card contains a spectrum analyzer that samples the 5- to 42-MHz upstream frequency spectrum in real-time, analyzing the number of offline cable modems. If a user-defined threshold value is reached, the spectrum management card takes a snapshot of the available upstream spectrum and passes that information to the IOS software, which analyzes it for possible significant ingress and impulse noise.

Using this analysis, the IOS software evaluates the upstream frequency spectrum and, if necessary automatically hops to a frequency that can provide a clean upstream channel. This eliminates "blind" frequency hops and can improve response time to ingress noise impairments.

The **cable upstream** interface command now includes a new parameter when used to configure an interface on the MC16S Cable Modem Card, to allow the creation of a range of channel width. The new syntax is **cable upstream** *port* **channel-width** *channel-width-1 channel-width-2* where the possible channel width values are 200000, 400000, 800000, 1600000, 3200000.

The **cable upstream** *port* **modulation-profile** *modulation-number* command configures the upstream modulation profile.

Note The MC16S Spectrum Management Card is calibrated using a 24.016 MHz, 0 dBmV reference signal injected into the card's front F-connector. The worst case accuracy is specified as +/- 3 dB over the DOCSIS upstream frequency band (5-45 MHz) and operating temperature range (0 to 40 degrees Centigrade).

Two-Port Moderate-Capacity T1 and E1 Digital Voice Port Adapter

Cisco digital voice port adapters for the Cisco 7200 series routers provide large-scale voice and fax termination for PBXs, and the Public Switched Telephone Network (PSTN) using Voice over IP (VoIP) or Voice over Frame Relay (VoFR).

The digital voice port adapter is a highly integrated solution offering a leap forward in voice-channel density and application flexibility. This single-width port adapter incorporates two universal ports that can be configured for either T1 or E1 connections with high-performance digital signal processors that support up to 48 channels of compressed voice. Integrated channel service units/digital service units (CSU/DSU) echo cancellation, and digital signal level 0 (DS-0) drop and insert functionality eliminate the need for external line-termination devices and multiplexers, simplifying network design and management.

VIC-2BRI-NT/TE

The ISDN BRI NT/TE voice interface card (VIC-2BRI-NT/TE) for the Cisco 2600 series enables Cisco IOS software to replicate the public switched network interface to a PBX that is compatible with European Telecommunications Standards Institute (ETSI) NET3 and QSIG switch types.

In the past, customers with PBXs that implement only the BRI TE interface have had to make substantial hardware and software changes on the PBX to implement the NT interface. The implementation of an NT interface on the router allows the customer to connect ISDN PBXs and key systems to a multiservice network with a minimum of configuration changes on the PBX.

VIC-2FXO-M3 Support on the Cisco 1750

The Australian version of the two-port Foreign Exchange Office (FXO) voice/fax interface card for the voice/fax network module (VIC-2FXO-M3) is supported by the Cisco 1750 in Cisco IOS Release 12.1(5)T.

MIBs

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

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 25.

Table 25 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined

Table 25 Deprecated and Replacement MIBs (Continued)

Deprecated MIB	Replacement
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Limitations and Restrictions

SNMP Version 1 BGP4-MIB Limitations

When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

Important Notes

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

For general information, refer to the following documents:

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Important Notes for Cisco IOS Release 12.2(19)

The following information applies to Cisco IOS Release 12.2(19).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(19) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz

- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(17a)

The following information applies to Cisco IOS Release 12.2(17a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(17a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(17a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(17)

The following information applies to Cisco IOS Release 12.2(17).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(17) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(17) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(16c)

The following information applies to Cisco IOS Release 12.2(16c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(16c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(16c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(16b)

The following information applies to Cisco IOS Release 12.2(16b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(16b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(16b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(16a)

The following information applies to Cisco IOS Release 12.2(16a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(16a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(16a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(16)

The following information applies to Cisco IOS Release 12.2(16).

atm bandwidth dynamic Command for ATM IMA Interfaces

When a link within an ATM Inverse Multiplexing over ATM (IMA) group goes down, traffic disruptions can occur because the total available bandwidth of the IMA interface is reduced. Before the introduction of the **atm bandwidth dynamic** command, the bandwidth could not be recovered until the IMA group was manually taken down and brought back up. This command enables permanent virtual circuit (PVC) bandwidth to change dynamically in proportion to IMA interface bandwidth changes. At least one link on the IMA group interface must be active for ATM PVC dynamic bandwidth changes to take effect.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(16) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(16) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

threshold noise Command

The **threshold noise** {*value*} command is introduced and configured in voice-port configuration mode. The value argument has a valid range from –30 to –90 dB. There is no default.

The command enables users to adjust the threshold for noise so that the voice activity detection (VAD) API layer will not classify the incoming signal as “unknown” or “silence.” For example, when there is no speech input and the noise level is near the static noise threshold (in the case of the hoot-n-holler application), you could have noise that creates unwanted spurious packets and takes up bandwidth.

The supported platforms are: Cisco 1700, Cisco 1751, Cisco 2600 (with and without the NM-HDA), Cisco 3600 (with and without the NM-HDA), Cisco 7200 (with and without the NM-HDA), Cisco AS5300, Cisco AS5800, and Cisco MC3810.

Important Notes for Cisco IOS Release 12.2(13c)

The following information applies to Cisco IOS Release 12.2(13c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(13c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(13b)

The following information applies to Cisco IOS Release 12.2(13b).

atm bandwidth dynamic Command for ATM IMA Interfaces

When a link within an ATM Inverse Multiplexing over ATM (IMA) group goes down, traffic disruptions can occur because the total available bandwidth of the IMA interface is reduced. Before the introduction of the **atm bandwidth dynamic** command, the bandwidth could not be recovered until the IMA group was manually taken down and brought back up. This command enables permanent virtual circuit (PVC) bandwidth to change dynamically in proportion to IMA interface bandwidth changes. At least one link on the IMA group interface must be active for ATM PVC dynamic bandwidth changes to take effect.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(13b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(13b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

threshold noise Command

The **threshold noise** {*value*} command is introduced and configured in voice-port configuration mode. The value argument has a valid range from –30 to –90 dB. There is no default.

The command enables users to adjust the threshold for noise so that the voice activity detection (VAD) API layer will not classify the incoming signal as “unknown” or “silence.” For example, when there is no speech input and the noise level is near the static noise threshold (in the case of the hoot-n-holler application), you could have noise that creates unwanted spurious packets and takes up bandwidth.

The supported platforms are: Cisco 1700, Cisco 1751, Cisco 2600 (with and without the NM-HDA), Cisco 3600 (with and without the NM-HDA), Cisco 7200 (with and without the NM-HDA), Cisco AS5300, Cisco AS5800, and Cisco MC3810.

Important Notes for Cisco IOS Release 12.2(13a)

The following information applies to Cisco IOS Release 12.2(13a).

atm bandwidth dynamic command for ATM IMA interfaces

When a link within an ATM IMA group goes down, traffic disruptions can occur because the total available bandwidth of the IMA interface is reduced. Before the introduction of this command, the bandwidth could not be recovered until the IMA group was manually taken down and brought back up. The **atm bandwidth dynamic** command enables PVC bandwidth to change dynamically in proportion to IMA interface bandwidth changes. At least one link on the IMA group interface must be active for ATM PVC dynamic bandwidth changes to take effect.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(13a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(13a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(13)

The following information applies to Cisco IOS Release 12.2(13).

Configuring MD5 Authentication for BGP Peering Sessions

This document provides general information about deploying MD5 authentication for a BGP session. You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, then an error message will be displayed in the console.

Old Behavior

In previous versions of Cisco IOS software, configuring MD5 authentication for a BGP peering session was generally considered to be difficult because the initial configuration and any subsequent MD5 configuration changes required the BGP neighbor to be reset.

New Behavior

This behavior has been changed in current versions of Cisco IOS software. CSCdx23494 (integrated in Cisco IOS release 12.2(13)) introduced a change to MD5 authentication for BGP peering sessions. The BGP peering session does not need to be reset to maintain or establish the peering session for initial configuration or after the MD5 configuration has been changed. However, the configuration must be completed on both the local and remote BGP peer before the BGP hold timer expires. If the hold down timer expires before the MD5 configuration has been completed on both BGP peers, the BGP session will time out.

The following example enables the authentication feature between this router and the BGP neighbor at 10.108.1.1. The password that must also be configured for the neighbor is *bla4u00=2nkq*. The remote peer must be configured before the holddown timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

When the password has been configured, the MD5 key is applied to the tcp session immediately. If one peer is configured before the other, the TCP segments will be discarded on both the local and remote peers due to an authentication failure. The peer that is configured with the password will print an error message in the console similar to the following:

```
  00:03:07: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.2(179) to 10.0.0.1(11000)
```

The time period in which the password must changed is typically the life time of a stale BGP session. When the password or MD5 key is configured, incoming TCP segments will only be accepted if the key is known. If the key is unknown on both the remote and local peer, the TCP segments will be dropped, and the BGP session will time out when the holddown timer expires.

If the BGP session has been preconfigured with a hold time of 0 seconds, no keepalive messages will be sent. The BGP session will stay up until one of the peers, on either side, tries to transmit a message (For example, a prefix update).

Note Configuring a new timer value for the holddown timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the holddown timer to avoid resetting the BGP session.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(13) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12f)

The following information applies to Cisco IOS Release 12.2(12f).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12e)

The following information applies to Cisco IOS Release 12.2(12e).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12d)

The following information applies to Cisco IOS Release 12.2(12d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12c)

The following information applies to Cisco IOS Release 12.2(12c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12b)

The following information applies to Cisco IOS Release 12.2(12b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12a)

The following information applies to Cisco IOS Release 12.2(12a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(12)

The following information applies to Cisco IOS Release 12.2(12).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(12) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(12) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(10d)

The following information applies to Cisco IOS Release 12.2(10d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(10d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(10d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(10c)

The following information applies to Cisco IOS Release 12.2(10c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(10c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(10c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(10b)

The following information applies to Cisco IOS Release 12.2(10b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(10b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(10b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(10a)

The following information applies to Cisco IOS Release 12.2(10a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(10a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz

- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(10a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(10)

The following information applies to Cisco IOS Release 12.2(10).

Cisco AS5400 Universal Gateway Images Deferred Due to Caveat CSCdx82069

Two images in Cisco IOS Release 12.2(10) to 12.2(10a) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdx82069. This caveat affects the following images:

- c5400-is-mz
- c5400-js-mz

The software solution for these deferred images is Cisco IOS Release 12.2(6f), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco AS5800 Universal Access Server Images Deferred Due to Caveats CSCdx25471 and CSCdw67688

Three images in Cisco IOS Release 12.2(10) to 12.2(10a) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdx25471 and CSCdw67688. These caveats affect the following images:

- c5800-p4-mz
- dsc-c5800-mz
- c5800-k8p4-mz

The software solution for these deferred images is Cisco IOS Release 12.2(7c), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(10) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(10) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Codec Preference Order When Using H.323 Signaling

Cisco gateways do not support a codec preference order when using H.323 signaling. All codecs listed are given equal preference.

Important Notes for Cisco IOS Release 12.2(7g)

The following information applies to Cisco IOS Release 12.2(7g).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7g) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7g) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7f)

The following information applies to Cisco IOS Release 12.2(7f).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7e)

The following information applies to Cisco IOS Release 12.2(7e).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7d)

The following information applies to Cisco IOS Release 12.2(7d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7c)

The following information applies to Cisco IOS Release 12.2(7c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7b)

The following information applies to Cisco IOS Release 12.2(7b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7a)

The following information applies to Cisco IOS Release 12.2(7a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(7)

The following information applies to Cisco IOS Release 12.2(7).

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(7) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(7) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Images Deferred Because of Caveat CSCdw29595

In Cisco IOS Release 12.2(7), 152 images have been deferred because of a severe defect. The affected images are as follows:

• c800-k8nosy6-mw	• c2600-ik9o3s-mz	• mc3810-a2ik8sv5-mz	• c7100-jk8o3s-mz
• c800-k8osy6-mw	• c2600-ik9s-mz	• mc3810-a2ik9s-mz	• c7100-jk8s-mz
• c805-k8nosy6-mw	• c2600-jk8o3s-mz	• mc3810-a2ik9sv5-mz	• c7100-jk9o3s-mz
• c805-k8osy6-mw	• c2600-jk8s-mz	• mc3810-ik8s-mz	• c7100-jk9s-mz
• ubr920-k8o3v6y5-mz	• c2600-jk9o3s-mz	• mc3810-a2jk8sv5-mz	• c7200-ik9o3s-mz
• ubr920-k8o3v7y5-mz	• c3620-a3jk8s-mz	• mc3810-a2jk9s-mz	• c7200-ik9s-mz
• ubr920-k8v6y5-mz	• c3620-a3jk9s-mz	• mc3810-a2jk9sv5-mz	• c7200-jk8o3s-mz
• ubr920-k8v7y5-mz	• c3620-ik8o3s-mz	• mc3810-i5k8s-mz	• c7200-jk8s-mz
• ubr920-k9o3v6y5-mz	• c3620-ik8s-mz	• mc3810-i5k9s-mz	• c7200-jk9o3s-mz
• ubr920-k9o3v7y5-mz	• c3620-ik9o3s-mz	• mc3810-ik9s-mz	• c7200-jk9s-mz

• ubr920-k9v6y5-mz	• c3620-ik9s-mz	• mc3810-jk8s-mz	• c7200-a3jk8s-mz
• ubr920-k9v7y5-mz	• c3620-jk8o3s-mz	• mc3810-jk9s-mz	• c7200-a3jk9s-mz
• c1400-k8osy-mz	• c3620-jk8s-mz	• c4500-a3jk9s-mz	• c7200-dk8o3s-mz
• c1600-bk8nor2sy-l	• c3620-jk9o3s-mz	• c4500-a3jk8s-mz	• c7200-dk8s-mz
• c1600-bk8nor2sy-mz	• c3620-jk9s-mz	• c4500-ik8s-mz	• c7200-dk9o3s-mz
• c1600-k8osy-l	• c3640-a3jk8s-mz	• c4500-ik9s-mz	• c7200-g5jk8s-mz
• c1600-k8osy-mz	• c3640-a3jk9s-mz	• c4500-jk8s-mz	• c7200-ik8o3s-mz
• c1600-k8sy-l	• c3640-ik8o3s-mz	• c4500-jk9s-mz	• c7200-ik8s-mz
• c1600-k8sy-mz	• c3640-ik8s-mz	• c5rsm-ik9o3sv-mz	• rsp-a3jk8sv-mz
• c1700-bk8no3r2sv3y-mz	• c3640-ik9o3s-mz	• c5rsm-jk8o3sv-mz	• rsp-a3jk9sv-mz
• c1700-bk8no3r2sy-mz	• c3640-ik9s-mz	• c5rsm-jk8sv-mz	• rsp-dk8o3sv-mz
• c1700-bk9no3r2sv3y-mz	• c3640-jk8o3s-mz	• c5rsm-jk9o3sv-mz	• rsp-dk8sv-mz
• c1700-bk9no3r2sy-mz	• c3640-jk8s-mz	• c5rsm-jk9sv-mz	• rsp-dk9o3sv-mz
• c1700-k8o3sv3y-mz	• c3640-jk9o3s-mz	• c5rsm-ik9sv-mz	• rsp-ik8o3sv-mz
• c1700-k8o3sy-mz	• c3640-jk9s-mz	• c5rsm-a3jk8sv-mz	• rsp-ik8sv-mz
• c1700-k8sv3y-mz	• c3660-a3jk8s-mz	• c5rsm-a3jk9sv-mz	• rsp-ik9o3sv-mz
• c1700-k8sy-mz	• c3660-a3jk9s-mz	• c5rsm-dk8o3sv-mz	• rsp-ik9sv-mz
• c1700-k9o3sv3y-mz	• c3660-ik8o3s-mz	• c5rsm-dk8sv-mz	• rsp-jk8o3sv-mz
• c1700-k9o3sy-mz	• c3660-ik8s-mz	• c5rsm-ik8o3sv-mz	• rsp-jk8sv-mz
• c1700-k9sv3y-mz	• c3660-ik9o3s-mz	• c5rsm-ik8sv-mz	• rsp-jk9o3sv-mz
• c1700-k9sy-mz	• c3660-ik9s-mz	• c5300-ik8s-mz	• rsp-jk9sv-mz
• c2500-ik8os-l	• c3660-jk9s-mz	• c5300-ik9s-mz	• ubr7200-ik8s-mz
• c2500-ik8s-l	• c3660-telcoentk9-mz	• c5300-jk8s-mz	• ubr7200-ik8st-mz
• c2600-jk9s-mz	• c3660-jk8s-mz	• c5300-jk9s-mz	• ubr7200-k8p-mz
• c2600-a3jk9s-mz	• c3660-jk9o3s-mz	• c7100-ik8o3s-mz	• ics7700-bk8no3r2sv3y-mz
• c2600-a3jk8s-mz	• c3660-jk8o3s-mz	• c7100-ik8s-mz	• ics7700-bk9no3r2sv3y-mz
• c2600-ik8o3s-mz	• mc3810-a2i5k8s-mz	• c7100-ik9o3s-mz	• ics7700-k8o3sv3y-mz
• c2600-ik8s-mz	• mc3810-a2i5k9s-mz	• c7100-ik9s-mz	• ics7700-k9o3sv3y-mz

The software solution for these deferred images is Cisco IOS Release 12.2(7c), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6j)

The following information applies to Cisco IOS Release 12.2(6j).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6j) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6j) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6i)

The following information applies to Cisco IOS Release 12.2(6i).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6i) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6i) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6h)

The following information applies to Cisco IOS Release 12.2(6h).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6h) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6h) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6g)

The following information applies to Cisco IOS Release 12.2(6g).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6g) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6g) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6f)

The following information applies to Cisco IOS Release 12.2(6f).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6e)

The following information applies to Cisco IOS Release 12.2(6e).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6d)

The following information applies to Cisco IOS Release 12.2(6d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6c)

The following information applies to Cisco IOS Release 12.2(6c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6b)

The following information applies to Cisco IOS Release 12.2(6b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6a)

The following information applies to Cisco IOS Release 12.2(6a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(6)

The following information applies to Cisco IOS Release 12.2(6).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(6) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(6) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(5d)

The following information applies to Cisco IOS Release 12.2(5d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(5d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(5d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(5c)

The following information applies to Cisco IOS Release 12.2(5c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(5c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(5c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(5a)

The following information applies to Cisco IOS Release 12.2(5a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(5a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(5a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(5)

The following information applies to Cisco IOS Release 12.2(5).

Cisco 7500 Series Images Deferred Because of Caveat CSCdu01272

Twenty-one images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), 12.2(3) and 12.2(5) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu01272. This caveat affects the following images:

- rsp-pv-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-a3jsv-mz
- rsp-dk8o3sv-mz
- rsp-dk8sv-mz
- rsp-dk9o3sv-mz
- rsp-do3sv-mz
- rsp-dsv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-io3sv-mz
- rsp-isv-mz
- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jo3sv-mz
- rsp-jsv-mz

With caveat CSCdu01272, a Cisco 7500 series with a PA-MC-T3 port adapter may experience a Versatile Interface Processor (VIP) reload. The software solution for these deferred images is Cisco IOS Release 12.2(1), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco Catalyst 4000 Gateway Images Deferred Because of Caveats CSCdu59093 and CSCdu63022

Three images in Cisco IOS Release 12.2(1) through Cisco IOS Release 12.2(5) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdu59093 and CSCdu63022. These caveats affect the following images:

- c4gwy-cboot-mz
- c4gwy-io3s-mz
- c4gwy-io3sx3-mz

With caveat CSCdu59093, a Catalyst 4000 Gateway may reload when a conference call is made. With caveat CSCdu63022, a Cisco Catalyst 4000 Gateway may not be able to be used as a conference bridge. The software solution for these deferred images is Cisco IOS Release 12.1(5)T9, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(5) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(5) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

MPLS VPN with TE and MPLS InterAS Advisory on Cisco IOS Software

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) functionality is compromised for the following platforms in Cisco IOS Release 12.2(4)T:

- Cisco 3660 series and 3640 series
- Cisco 7200 series and 7500 series
- Cisco UBR7000 series
- Cisco RPM series

Refer to the advisory notice at the following location:

http://www-tac.cisco.com/Support_Library/field_alerts/fn15911.html

Output of show dialplan Command Does not Show Dial-peers With Variable Length Patterns

The **show dialplan** command does not match the user entered *dialstring* with dial-peers that have variable length patterns (i.e., patterns which have a terminating 'T' character). The condition happens when the *dialstring* is used to match the dial-peers as in the following examples:

- **show dialplan number** <*dialstring*>

- **show dialplan dialpeer** <*inbound peer tag*> **number** <*dialstring*>
- **show dialplan incall** *port* **number <***dialstring*>

This condition does not affect actual call routing.

As a workaround, the *dialstring* can be terminated with the configured dialstring terminator, which is by default, the # character, to match with the variable length patterns.

Important Notes for Cisco IOS Release 12.2(3g)

The following information applies to Cisco IOS Release 12.2(3g).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3g) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3f)

The following information applies to Cisco IOS Release 12.2(3f).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3f) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3e)

The following information applies to Cisco IOS Release 12.2(3e).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3e) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3d)

The following information applies to Cisco IOS Release 12.2(3d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3c)

The following information applies to Cisco IOS Release 12.2(3c).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3b)

The following information applies to Cisco IOS Release 12.2(3b).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3a)

The following information applies to Cisco IOS Release 12.2(3a).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz

- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(3)

The following information applies to Cisco IOS Release 12.2(3).

Cisco 1700 Series Images Deferred Because of Caveat CSCdu59975

Five images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), and 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. This caveat affects the following images:

- c1700-k8o3sv3y-mz
- c1700-k8sv3y-mz
- c1700-no3sv3y-mz

- c1700-o3sv3y-mz
- c1700-sv3y-mz

With caveat CSCdu59975, a glare condition may occur randomly and undetected on the Cisco 1700 series router. The software solution for these deferred images is Cisco IOS Release 12.2(5), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco 7500 Series Images Deferred Because of Caveat CSCdu01272

Twenty-one images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), 12.2(3) and 12.2(5) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu01272. This caveat affects the following images:

- rsp-pv-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-a3jsv-mz
- rsp-dk8o3sv-mz
- rsp-dk8sv-mz
- rsp-dk9o3sv-mz
- rsp-do3sv-mz
- rsp-dsv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-io3sv-mz
- rsp-isv-mz
- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jo3sv-mz
- rsp-jsv-mz

With caveat CSCdu01272, a Cisco 7500 series with a PA-MC-T3 port adapter may experience a Versatile Interface Processor (VIP) reload. The software solution for these deferred images is Cisco IOS Release 12.2(1), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco Catalyst 4000 Gateway Images Deferred Because of Caveats CSCdu59093 and CSCdu63022

Three images in Cisco IOS Release 12.2(1) through Cisco IOS Release 12.2(5) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdu59093 and CSCdu63022. These caveats affect the following images:

- c4gwy-cboot-mz
- c4gwy-io3s-mz
- c4gwy-io3sx3-mz

With caveat CSCdu59093, a Catalyst 4000 Gateway may reload when a conference call is made. With caveat CSCdu63022, a Cisco Catalyst 4000 Gateway may not be able to be used as a conference bridge. The software solution for these deferred images is Cisco IOS Release 12.1(5)T9, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco IOS Release 12.2(1) and Cisco IOS Release 12.2(3) Images Deferred Because of Recall, End of Sales, End of Engineering and End of Life for Cisco uBR914 Cable Data Service Unit

Four images in Cisco IOS Release 12.2(1) and Cisco IOS Release 12.2(3) have been deferred because of the recall, end of sales, end of engineering, and end of life for the Cisco uBR914 Cable Data Service Unit (DSU). This deferral affects the following images:

- ubr910-rboot-mz
- ubr910-k8y5-mz
- ubr910-k8-mz
- ubr910-k8y5-mz

Refer to the following document for additional information:

http://www.cisco.com/en/US/products/hw/cable/ps2221/prod_eol_notice09186a00800a44c6.html

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco Voice Gateway 200 Image Deferred Because of Caveat CSCdu59975

The vg200-i6s-mz image in Cisco IOS Release 12.2(1), 12.2(1a), and 12.2(1c) has been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. With CSCdu59975, glare conditions are not detected by the voice telephony service provider (VTSP). The software solution for the deferred image is Cisco IOS Release 12.2(6), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(1d)

The following information applies to Cisco IOS Release 12.2(1d).

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(1d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(1d) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(1c)

The following information applies to Cisco IOS Release 12.2(1c).

Cisco 1700 Series Images Deferred Because of Caveat CSCdu59975

Five images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), and 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. This caveat affects the following images:

- c1700-k8o3sv3y-mz
- c1700-k8sv3y-mz
- c1700-no3sv3y-mz
- c1700-o3sv3y-mz
- c1700-sv3y-mz

With caveat CSCdu59975, a glare condition may occur randomly and undetected on the Cisco 1700 series router. The software solution for these deferred images is Cisco IOS Release 12.2(5), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(1c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(1c) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(1b)

The following information applies to Cisco IOS Release 12.2(1b).

Cisco 1700 Series Images Deferred Because of Caveat CSCdu59975

Five images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), and 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. This caveat affects the following images:

- c1700-k8o3sv3y-mz
- c1700-k8sv3y-mz
- c1700-no3sv3y-mz
- c1700-o3sv3y-mz
- c1700-sv3y-mz

With caveat CSCdu59975, a glare condition may occur randomly and undetected on the Cisco 1700 series router. The software solution for these deferred images is Cisco IOS Release 12.2(5), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(1b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco IOS Release 12.2(1b) Images Deferred Because of Caveat CSCdu54754

Seventy-nine images in Cisco IOS Release 12.2(1b) were deferred because of a severe defect. This defect has been assigned Cisco Caveat ID CSCdu54754. This caveat affects the following images:

- c3640-p7-mz
- c3660-telcoent-mz
- mc3810-a2i5k8s-mz
- mc3810-a2i5k9s-mz
- mc3810-a2i5s-mz
- mc3810-a2ik8sv5-mz
- mc3810-a2ik9s-mz
- mc3810-a2jk8sv5-mz
- mc3810-a2isv5-mz
- mc3810-a2jk8sv5-mz
- mc3810-a2jk9s-mz
- mc3810-a2jk9sv5-mz
- c3810-a2jsv5-mz
- mc3810-aa2jsv5x-mz
- mc3810-i5k8s-mz
- mc3810-i5k9s-mz
- mc3810-i5s-mz
- mc3810-is-mz
- mc3810-ik8s-mz
- mc3810-jk8s-mz
- c3660-p-mz
- mc3810-jk9s-mz
- mc3810-js-mz
- c1700-bk8no3r2sv3y-mz
- c1700-bk9no3r2sv3y-mz
- c1700-k8o3sv3y-mz
- c1700-k800-k8svy-mz
- c1700-k9o3sv3y-mz
- c1700-k9sv3y-mz
- c1700-no3sv3y-mz
- c1700-o3sv3y-mz
- c1700-sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bk9no3r2sv3y-mz

- ics7700-bnr2sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-sv3y-mz
- c2600-ik8o3s-mz
- c2600-ik8s-mz
- c2600-ik9o3s-mz
- c2600-jk9s-mz
- c2600-ipss7-mz
- c2600-is-mz
- c2600-jk8o3s-mz
- c2600-jk9o3s-mz
- c2600-jk9s-mz
- c2600-js-mz
- c2600-jsx-mz
- c7200-a3jk8s-mz
- c7200-a3jk9s-mz
- c7200-a3js-mz
- c7200-ik8o3s-mz
- c7200-jk8s-mz
- c7200-ik8o3s-mz
- c7200-ik9s-mz
- c7200-jk9s-mz
- c7200-js-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-ik9o3sv-mz
- rsp-jk9sv-mz
- rsp-isv-mz
- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jsv-mz

- c7200-ik8o3s-mz
- c7200-ik9s-mz
- c7200-jk9s-mz
- c7200-js-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-ik8o3sv-mz

With Caveat CSCdu54754, call failures, DSP alarms, and DSP timeouts are generated when G723 codecs are configured.

This release has been replaced with Cisco IOS Release 12.2(1a) which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Caution Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(1b) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(1a)

The following information applies to Cisco IOS Release 12.2(1a).

Cisco 1700 Series Images Deferred Because of Caveat CSCdu59975

Five images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), and 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. This caveat affects the following images:

- c1700-k8o3sv3y-mz
- c1700-k8sv3y-mz
- c1700-no3sv3y-mz
- c1700-o3sv3y-mz
- c1700-sv3y-mz

With caveat CSCdu59975, a glare condition may occur randomly and undetected on the Cisco 1700 series router. The software solution for these deferred images is Cisco IOS Release 12.2(5), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(1a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(1a) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(1)

The following information applies to Cisco IOS Release 12.2(1).

Addition of squeeze Command for Cisco 2600 and Cisco 3600 Series Routers

The **squeeze** command, which is used to erase all files marked for deletion on a Flash file system, is now available on Cisco 2600 and Cisco 3600 series routers.

Access Server Commands Removed From Parser in Cisco IOS Release 12.2

The following commands have been removed from the parser in Cisco IOS Release 12.2 for the Cisco AS5350, AS5400, AS5800 and AS5850:

- **port modem autotest**
- **port modem startup-test**

The following commands have been removed from the parser in Cisco IOS Release 12.2 for the Cisco AS5300:

- **modem startup-test**
- **modem autotest**

Changes to output attenuation Command

In Cisco IOS Release 12.2(1), the range of the **output attenuation** command for voice ports has changed from *0-14* to *-6-14*.

Cisco 1700 Series Images Deferred Because of Caveat CSCdu59975

Five images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), and 12.2(3) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. This caveat affects the following images:

- c1700-k8o3sv3y-mz
- c1700-k8sv3y-mz
- c1700-no3sv3y-mz
- c1700-o3sv3y-mz
- c1700-sv3y-mz

With caveat CSCdu59975, a glare condition may occur randomly and undetected on the Cisco 1700 series router. The software solution for these deferred images is Cisco IOS Release 12.2(5), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco 7500 Series Images Deferred Because of Caveat CSCdu01272

Twenty-one images in Cisco IOS Release 12.2(1a), 12.2(1b), 12.2(1c), 12.2(3) and 12.2(5) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu01272. This caveat affects the following images:

- rsp-pv-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-a3jsv-mz
- rsp-dk8o3sv-mz
- rsp-dk8sv-mz
- rsp-dk9o3sv-mz
- rsp-do3sv-mz
- rsp-dsv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-io3sv-mz
- rsp-isv-mz

- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jo3sv-mz
- rsp-jsv-mz

With caveat CSCdu01272, a Cisco 7500 series with a PA-MC-T3 port adapter may experience a Versatile Interface Processor (VIP) reload. The software solution for these deferred images is Cisco IOS Release 12.2(1), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco AS5800 Universal Access Server Images Deferred Because of Caveats CSCdu18348, CSCdv06104, CSCdu64551, and CSCdv04970

Three images in Cisco IOS Release 12.2(1) to 12.2(1a) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdu18348, CSCdv06104, CSCdu64551, and CSCdv04970. These caveats affect the following images:

- c5800-p4-mz
- dsc-c5800-mz
- c5800-k8p4-mz

The software solution for these deferred images is Cisco IOS Release 12.2(1)XS, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco Catalyst 4000 Gateway Images Deferred Because of Caveats CSCdu59093 and CSCdu63022

Three images in Cisco IOS Release 12.2(1) through Cisco IOS Release 12.2(5) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdu59093 and CSCdu63022. These caveats affect the following images:

- c4gwy-cboot-mz
- c4gwy-io3s-mz
- c4gwy-io3sx3-mz

With caveat CSCdu59093, a Catalyst 4000 Gateway may reload when a conference call is made. With caveat CSCdu63022, a Cisco Catalyst 4000 Gateway may not be able to be used as a conference bridge. The software solution for these deferred images is Cisco IOS Release 12.1(5)T9, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Cisco ICS7700 Images Deferred Because of Caveat CSCdy01600

Six images in Cisco IOS Release 12.2(1) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy01600. This caveat affects the following images:

- ics7700-sv3y-mz
- ics7700-k8o3sv3y-mz
- ics7700-k9o3sv3y-mz
- ics7700-bk9no3r2sv3y-mz
- ics7700-bk8no3r2sv3y-mz
- ics7700-bnr2sv3y-mz

With caveat CSCdy01600, router fails to recognize voice cards or load running configuration. The software solution for these deferred images is Cisco IOS Release 12.3(2)XA.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco IOS Release 12.2(1) Images Deferred Because of Recall, End of Sales, End of Engineering and End of Life for Cisco uBR914 Cable Data Service Unit

Four images in Cisco IOS Release 12.2(1) and Cisco IOS Release 12.2(3) have been deferred because of the recall, end of sales, end of engineering, and end of life for the Cisco uBR914 Cable Data Service Unit (DSU). This deferral affects the following images:

- ubr910-rboot-mz
- ubr910-k8y5-mz
- ubr910-k8-mz
- ubr910-k8y5-mz

Refer to the following document for additional information:

http://www.cisco.com/en/US/products/hw/cable/ps2221/prod_eol_notice09186a00800a44c6.html

Cisco MGX 8850 Route Processor Module Images Deferred Because of Caveat CSCeb31735

Two images in Cisco IOS Release 12.2(1) were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-js-mz

With caveat CSCeb31735, there is a deferral of unsupported RPM-PR and RPM-XF images. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5, which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Cisco Voice Gateway 200 Image Deferred Because of Caveat CSCdu59975

The vg200-i6s-mz image in Cisco IOS Release 12.2(1), 12.2(1a), and 12.2(1c) has been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu59975. With CSCdu59975, glare conditions are not detected by the voice telephony service provider (VTSP). The software solution for the deferred image is Cisco IOS Release 12.2(6), which is available on Cisco.com.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Deferral of AS5300 Boot Image

The c5300-boot-mz image has been deferred in Cisco IOS Release 12.2(1) because of a severe defect. This defect has been assigned Cisco Caveat ID CSCdu10569. The software solution for this defect is the c5300-boot-mz image in Cisco IOS Release 12.0(4)T1.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Caution Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

PBR and NAT

If an incoming packet hits both Policy-based Routing (PBR) and NAT-inside with process switching configured, the packet will undergo PBR again for the second time. Workarounds: 1) Avoid configuring any features that can make the packets process switched. Or, 2) Permit the translated addresses in the PBR access list to be policy routed.

Caveats for Cisco IOS Release 12.2

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.

For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.2 and is located on Cisco.com.

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

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, log 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 of 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.)

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page* at:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions* at:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- *Why Does My Router Lose Its Configuration During Reboot?* at:

  http://www.cisco.com/warp/public/63/lose_config_6201.html

- *Troubleshooting Router Hangs* at:

  http://www.cisco.com/warp/public/63/why_hang.html

- *Troubleshooting Memory Problems - SYS-2-MALLOCFAIL* at:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers* at:

  http://www.cisco.com/warp/public/63/highcpu.html

- *Troubleshooting Router Crashes* at:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

- *Using CAR During DOS Attacks* at:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html