

# Cisco IOS Software 12.2 T Early Deployment Release Series

*Last Updated: October 10, 2001*

A stylized graphic of a globe with white grid lines on a blue background, positioned on the left side of the page.

## New Features Overview

The Cisco IOS<sup>®</sup> Software Release 12.2 T series is an Early Deployment (ED) release delivering the latest Cisco IOS Software functionality and platform support. Cisco IOS Software ED Release 12.2 T series, unlike the 12.2 Major Release series, will integrate new features with every maintenance release.

This Early Deployment Technology (T) release will reach End of Engineering when the next Cisco IOS Software major release becomes available. Ongoing support for the functionality introduced in Release 12.2 T series will be carried forward into the next ED release.

Use the matrix below to quickly locate a feature of interest.

Feature Matrix

Connectivity and Scalability	Content Delivery	Dial	Hardware Support
PPP Over Ethernet Client <i>12.2(2)T</i>	DNS Server Support for NS Records <i>12.2(2)T</i>	ACL Default Direction <i>12.2(4)T</i>	1-Port ADSL WAN Interface Card <i>12.2(2)T</i>
PPPoA/PPPoE Autosense for ATM PVCs <i>12.2(4)T</i>		Asynchronous Line Monitoring <i>12.2(4)T</i>	Small Office Home Office ADSL Router <i>12.2(2)T</i>
PPPoE Session Limit <i>12.2(4)T</i>		Dialer Persistent <i>12.2(4)T</i>	uBR905 Cable Access Router <i>12.2(2)T</i>
		Interesting Traffic PPP and Customer Profile Idle Timer <i>12.2(4)T</i>	
		L2TP and L2F Timer and Retry Enhancement <i>12.2(4)T</i>	
		L2TP Large-Scale Dial-Out <i>12.2(4)T</i>	
IP & Routing	Management	Mobile Networks	MPLS
IPv6 for Cisco IOS Software <i>12.2(2)T</i>	Circuit Interface Identification Persistence for SNMP <i>12.2(2)T</i>	Cisco Mobile Networks <i>12.2(4)T</i>	MPLS Label Distribution Protocol MIB <i>12.2(2)T</i>
NAT Support of H.323v2 RAS <i>12.2(2)T</i>	CNS Event Agent and CNS Configuration Agent <i>12.2(2)T</i>		DiffServ Aware MPLS Traffic Engineering <i>12.2(4)T</i>
BGP Conditional Route Injection <i>12.2(4)T</i>	Interface Index Display <i>12.2(2)T</i>		MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels <i>12.2(4)T</i>
BGP Multipath Load Sharing for eBGP and iBGP in an MPLS-VPN <i>12.2(4)T</i>	Interface Alias Long Name Support <i>12.2(2)T</i>		
BGP Prefix-Based Outbound Route Filtering <i>12.2(4)T</i>	MPLS Label Distribution Protocol MIB <i>12.2(2)T</i>		
Distributed Director <i>12.2(4)T</i>	MPLS Label Switching Router MIB <i>12.2(2)T</i>		
IPSec MIB Support for Cisco IPSec VPN Management <i>12.2(4)T</i>	NetFlow Multiple Export Destinations <i>12.2(2)T</i>		
OSPF ABR Type 3 LSA Filtering <i>12.2(4)T</i>	SIP User Agent MIB <i>12.2(2)T</i>		
OSPF Stub Router Advertisement <i>12.2(4)T</i>	SNMP Trap Support for VSI Master MIB <i>12.2(2)T</i>		
OSPF Update Packet-Pacing Configurable Timers <i>12.2(4)T</i>	ATM SNMP Trap and OAM Enhancements <i>12.2(4)T</i>		
	PIM MIB Extension for IP Multicast <i>12.2(4)T</i>		

QoS	Security	Voice	WAN Services
Class-Based Frame-Relay DE-Bit Matching and Marking <i>12.2(2)T</i>	DF Bit Override Functionality with IPsec Tunnels <i>12.2(2)T</i>	56K CSU Support for Cisco Signaling Link Terminal (SLT) <i>12.2(2)T</i>	ADSL Over ISDN <i>12.2(2)T</i>
Control Plane DSCP Support for RSVP <i>12.2(2)T</i>	Firewall Feature Set <i>12.2(2)T</i>	FXO Answer and Disconnect Supervision <i>12.2(2)T</i>	DHCP Option 82 Support for Routed Bridged Encapsulation <i>12.2(2)T</i>
Low Latency Queuing Enhancement—Priority Percentage Support <i>12.2(2)T</i>	IPsec Triple DES <i>12.2(2)T</i>	H.323 Version 2 Phase 2 <i>12.2(2)T</i>	X.25 Annex G Session Status Change Reporting <i>12.2(2)T</i>
MPLS QoS Multi-VC Mode for PA-A3 <i>12.2(2)T</i>	Secure Copy <i>12.2(2)T</i>	MGCP CAS PBX and AAL2 PVC <i>12.2(2)T</i>	Adaptive Frame Relay Traffic Shaping for Interface Congestion <i>12.2(4)T</i>
RSVP Scalability Enhancements <i>12.2(2)T</i>	Secure Terminal-Line Access <i>12.2(2)T</i>	SIP Gateway Support for Third Party Call Control <i>12.2(2)T</i>	Cisco Modem User Interface Option <i>12.2(4)T</i>
RSVP Support for ATM PVCs <i>12.2(2)T</i>	Ability to Disable Xauth for Static IPsec Peers <i>12.2(4)T</i>	SLT Dual Ethernet <i>12.2(2)T</i>	Frame Relay 64-Bit Counters <i>12.2(4)T</i>
Call Admission Control for H.323 VoIP Gateways <i>12.2(4)T</i>	Distinguished Name Based Crypto Maps <i>12.2(4)T</i>	SLT G.732 Support <i>12.2(2)T</i>	Leased/Switched BRI Interfaces for ETSI NET3 <i>12.2(4)T</i>
IP to ATM Class of Service Mapping for SVC Bundles <i>12.2(4)T</i>	Enhanced Test Command <i>12.2(4)T</i>	Voice over ATM with AAL2 Trunking <i>12.2(2)T</i>	Hardware <i>12.2(4)T</i>
Two-Rate Policer <i>12.2(4)T</i>	Inter-Domain Gatekeeper Security Enhancement <i>12.2(4)T</i>	Cisco H.323 Scalability and Interoperability Enhancements <i>12.2(4)T</i>	
	L2TP Security <i>12.2(4)T</i>	Location Confirmation (LCF) Enhancements for Alternate Endpoints <i>12.2(4)T</i>	
	Offload Server Accounting Enhancement <i>12.2(4)T</i>	MGCP 1.0 with NCS 1.0 and TGCP 1.0 Profiles <i>12.2(4)T</i>	
	RADIUS Attribute Screening <i>12.2(4)T</i>	PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer <i>12.2(4)T</i>	
	RADIUS Tunnel Preference for Load Balancing and Fail-Over <i>12.2(4)T</i>	PSTN Fallback <i>12.2(4)T</i>	
		Sequential LRQ Enhancement <i>12.2(4)T</i>	

## Connectivity and Scalability

### PPP Over Ethernet Client

#### Description

Several service providers (SPs) have moved to use PPPoE as the architecture to connect to the PPP termination device on the network.

PPPoE allows SPs to leverage their experience and existing RADIUS server to define users and their properties. Traditionally PPPoE meant that the ADSL CPE provided a bridged access carrying Ethernet frames over the ATM segment into and over the Ethernet, delivering it to a client on the customer's PC. This solution had some inherent weaknesses that the integrated PPPoE client on the CPE router solves, including multi-user access, support issues and multi-platform access.

For details on how to configure the PPPoE client, please refer to the Cisco IOS documentation or to the Cisco SOHO series documentation page at: [http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_fix/soho/sciront.htm#xtocid2671616](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/soho/sciront.htm#xtocid2671616)

#### Benefits

- Multi-user access over one account. Using NAT allows many users to share an account, which provides a seamless integration for the SP from an infrastructure point of view.
- Platform independent implementation. When providing a client, the SP needs to make assumptions about the platform that is used by the customer. PPPoE clients used by SPs commercially typically only support PC's running Windows platforms. However customers who have Apple Macintosh computers and Linux-based systems installed still expect the service to work. By supporting straight Ethernet using a PPPoE client in the router, support becomes much easier.

#### Platforms/Considerations

---

Routers	SOHO 70, C820, C827, C1600, C1700
---------	-----------------------------------

---

First appearance in a Cisco IOS Software release: 12.1(3)XG (special release) and in 12.2(2)T.

#### Marketing Contact

Geir Leirvik  
geir@cisco.com

PPPoA/PPPoE Autosense for ATM PVCs

#### Description

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

This new feature also adds support for precloning of virtual-access interfaces for PPPoA. Precloning enables virtual-access interfaces to be allocated at system start. This functionality significantly reduces the load on the system during call setup. When precloning is used, the virtual-access interface is attached to the session upon receipt of the first session-initiation packet from the client. The virtual-access interface is detached upon termination of the PPP session.

#### Benefits

The PPPoA/PPPoE Autosense for ATM PVCs feature provides resource allocation on demand. For each permanent virtual circuit (PVC) configured for both PPPoA and PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoA or PPPoE session on that PVC. With the PPPoA/PPPoE Autosense for ATM PVCs feature, resources are allocated for PPPoA and PPPoE sessions only when a client initiates a session, thus reducing overhead on the network access server (NAS).

#### Platforms/Considerations

---

Routers	C3660, C72xx, C75xx
---------	---------------------

---

#### PPPoE Session Limit

##### Description

The PPPoE Session Limit feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions that can be created on a router or on an ATM permanent virtual circuit (PVC), PVC range, or virtual circuit (VC) class.

Before the introduction of this feature, there was no way to limit the number of PPPoE sessions that could be created on a router. Not having a limit was potentially a problem because it was possible that the router could create so many PPPoE sessions that it would run out of memory.

To prevent the router from using too much memory for virtual access, the PPPoE Session Limit feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. The new `pppoe limit max-sessions` command limits the number of PPPoE sessions that can be created on the router. The modified `pppoe max-sessions` command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

#### Benefits

The PPPoE Session Limit feature prevents the router from using too much memory for virtual access by enabling you to limit the number of PPPoE sessions that can be created on a router or on a PVC, ATM PVC range, or VC class.

#### Platforms/Considerations

---

Routers	C45xx, C63xx, C72xx, C75xx
---------	----------------------------

---

## Content Delivery

DNS Server Support for NS Records

#### Description

DNS server support for NS records adds support for NS records to the Cisco IOS DNS server. This feature allows the distribution of the server-selection process to multiple Distributed Directors, improving overall capacity.

This feature provides additional support for RFC 1035, RFC 2131.

#### Benefits

- Improves server load-balancing capacity—server selection process is distributed to multiple Distributed Directors
- Improves fault tolerance—because the distributed server selection process eliminates single point of failure compare to a centralized Distributed Director service

#### Platforms/Considerations

---

Routers	C4500
---------	-------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact

Karen Cui

kcu@cisco.com

## Dial

ACL Default Direction

#### Description

The ACL Default Direction feature allows you to change the filter direction (where filter direction is not specified) to inbound packets only; that is, you can configure your server to filter packets that are coming toward the network.

This feature introduces the `radius-server attribute 11 direction default` command, which allows you to change the default direction of filters for your access control lists (ACL) via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router, thereby reducing resource consumption—rather than the outbound default direction, which waits until the traffic is about to leave the network before filtering.

### Benefits

The ACL Default Direction feature allows you to change the default direction, which is outbound, of filters for your access control lists to inbound via the radius-server attribute 11 direction default command.

### Platforms/Considerations

Routers	C7200
Access Servers (AS)	5300, 5400, 5800, 5850

## Asynchronous Line Monitoring

### Description

Before Cisco IOS Release 12.2(4)T, Cisco IOS software did not provide a method for displaying character mode asynchronous traffic flowing out of an asynchronous line. Therefore, when a user tried to troubleshoot difficult asynchronous traffic problems, the user needed to use EIA/TIA-232 datascopes in order to examine the data stream. This method is very detailed and cumbersome. The Asynchronous Line Monitoring feature available in Cisco IOS Release 12.2(4)T allows the monitoring of inbound and outbound asynchronous character mode traffic on another terminal line.

### Benefits

This feature increases the efficiency of the user that performs troubleshooting on character mode asynchronous traffic problems.

### Platforms/Considerations

Routers	C25xx, C26xx, C3620, C3640, C3660, C54xx, C58xx
Access Servers (AS)	5300, 5800

## Dialer Persistent

### Description

A new interface configuration command introduced in Cisco IOS Release 12.2(4)T, dialer persistent, allows a dial-on-demand routing (DDR) dialer profile connection to be brought up without being triggered by *interesting* traffic. When configured, the dialer persistent command starts a timer when the dialer interface starts up and starts the connection when the timer expires. If interesting traffic arrives before the timer expires, the connection is still brought up and set as persistent. The command provides a default timer interval, or you can set a custom timer interval.

The connection is not brought down until the shutdown interface command is entered on the dialer interface. If the persistent connection is torn down for some other reason, such as the ISDN line goes down, the system immediately tries to bring the connection back up, and will use any other settings configured for dialing on the dialer interface. If the dialer redial interface configuration command is configured, for example, the dialer connection is started again as persistent only after all redials have been attempted.

### Benefits

The Dialer Persistent feature allows the connection settings in the dialer profile to be configured as persistent, that is, the connection is not torn down until the shutdown interface command is entered on the dialer interface.

Until Cisco IOS Release 12.2(4)T, interesting traffic was used to bring up a DDR link. If there was no interesting traffic and the idle timeout interval was reached, the link was torn down. However, there are situations where a link needs to be up all the time. The Dialer Persistent feature provides the option to ignore idle timers and interesting traffic, thereby keeping the link up and maintaining DDR dialed calls indefinitely. The Dialer Persistent feature allows you to configure the intervals to be used for dial attempts, both initially on startup and when a persistent link is brought down due to external failures.

#### Platforms/Considerations

---

Routers	8xx, 16xx, 26xx, 3620, 3640, 71xx, 72xx, 75xx
---------	---

---

### Interesting Traffic PPP and Customer Profile Idle Timer

#### Description

Before Cisco IOS Release 12.2(4)T, only the dialer idle timer could be reset for *interesting* traffic on a dialer interface. The Customer Profile Idle Timer Enhancements for Interesting Traffic feature available in Cisco IOS Release 12.2(4)T supports a PPP idle timer based on interesting traffic for dialer interfaces. (Existing PPP idle timer behavior is not changed when traffic is not classified.) New commands and functionality provided with this feature also address idle timer issues for virtual access dialup network (VPDN) sessions, which use virtual access (projected) interfaces and rely on the PPP idle timer mechanism.

The Resource Pool Manager (RPM) per-customer profile dialer idle timer function works with Multilink PPP (MLP) and Multichassis Multilink PPP (MMP), providing that the master bundle interface is not a virtual access (projected) interface. For virtual access interfaces such as those used in a VPDN or with MMP where the dialer idle timer cannot be used, you can now classify the IP traffic that resets the PPP idle timer. A named access list is also supported.

Additionally, because RPM customer profiles are applied on a per-Dialed Number Identification Service (DNIS) basis and allow for configuring a per-customer profile dialer idle timer, the Customer Profile Idle Timer Enhancements for Interesting Traffic feature associates idle timers based on call type and DNIS.

The idle timer implementation in the Customer Profile Idle Timer Enhancements for Interesting Traffic feature specifies that for calls terminated on a network access server, a virtual access interface is cloned from the virtual template. This virtual access interface is linked to a physical interface on which is running a dialer timer. If the PPP idle timer is configured on the virtual template or provided by an authentication, authorization, and accounting (AAA) per-user interface configuration, the result is two idle timers, as follows:

- A PPP idle timer on the virtual access interface.
- A dialer idle timer on the physical interface.

Neither the dialer idle timer nor the PPP idle timer will run when the idle timer set in the per-user configuration is set to 0. When the per-user idle timer is set to some value besides 0, that value overrides all local idle timer configurations.

#### Benefits

The Customer Profile Idle Timer Enhancements for Interesting Traffic feature provides the following system idle timer benefits:

- Resets the PPP idle-timer based on interesting inbound or outbound IP traffic for virtual access interfaces on L2TP access concentrators (LACs) and L2TP network servers (LNSs).
- Associates the dialer timer with interesting traffic within RPM customer profiles.
- Applies the user idle-timer value RADIUS attribute 28 across all interfaces associated with the call.

#### Platforms/Considerations

---

Routers	8xx, 1xxx, 16xx, 17xx, 25xx, 26xx, 36xx, 38xx, 4xxx, 71xx, 72xx
---------	---

---

## L2TP and L2F Timer and Retry Enhancement

### Description

The L2TP and L2F Timer and Retry Enhancement feature allows the user to configure certain adjustable timers for Layer Two Transport Protocol (L2TP) and Layer Two Forwarding Protocol (L2F). For L2F, the settings for control packet retries and control packet timeouts are now both configurable. Initial tunnel packet retries and initial tunnel packet timeouts are now configurable for both the L2F and L2TP protocols.

### Benefits

Adjustments to timers made using the L2TP and L2F Timer and Retry Enhancement feature will impact the amount of time that a router will attempt to wait for a reply while establishing a virtual private dialup network (VPDN) tunnel, and the amount of time that a router will wait before trying to contact an alternate VPDN peer. These customizable timers will allow fine-tuning of router performance to suit the particular needs of the user.

### Platforms/Considerations

---

Routers	8xx, 16xx, 17xx, 26xx, 3620, 3640, 3660, 64xx, 72xx
---------	---

---

## L2TP Large-Scale Dial-Out

### Description

The L2TP Large-Scale Dial-Out feature enables the router to dial multiple Layer 2 Tunnel Protocol (L2TP) access concentrators (LACs) from a single L2TP network server (LNS). The LACs are signaled through the LNS and use L2TP to establish the dial sessions. User-defined profiles can be configured on an authentication, authorization, and accounting (AAA) server and retrieved by the LNS when dial-out occurs. The L2TP Large-Scale Dial-Out feature also supports multiple LACs bound into one stack group, call traffic load balancing, and outbound call congestion management.

1. The IP packets arrive at the LNS and are forwarded to the dialer interface by the routing protocol. (A virtual access interface has not been created yet.)
2. A dialer session is created and placed in a pending state while the dialer interface sends a Dial Out Request message to the AAA server requesting the user profile. The AAA server sends the user profile, and the LNS builds a dynamic map based on the reply.
3. The dialer interface looks for its dial resources and finds the virtual private dialup network (VPDN) group. The dialer interface then issues a dial call request to the VPDN group, which creates a virtual access interface. The virtual access interface becomes a member of a rotary group.
4. If there is no existing L2TP tunnel between the LNS and the primary LAC, the LNS would establish one; otherwise, it uses the existing tunnel. The LNS sends an Outgoing Call ReQuest (OCRQ) message, inside of which is the dynamic dialer map, to the primary LAC.
5. Upon receiving the OCRQ message, the primary LAC determines whether it is congested. If the primary LAC is congested, it sends a Stack Group Bidding Protocol (SGBP) Discover message through a new tunnel to the secondary LAC in the scenario depicted in Figure 1, but it could send the message to any other LAC configured in the SGBP stack group. After the secondary LAC receives the SGBP Discover message from the LNS, it responds with an SGBP Offer message describing available resources.
6. If neither LAC has resources to dial out, the primary LAC would send a Call Disconnect Notification (CDN) message to the LNS. The LNS would then tear down the tunnel.

If the secondary LAC has more resources, the primary LAC can choose to dial through the secondary LAC. The primary LAC sends a CDN message to the LNS with error code 7, which means “Try another” as defined in RFC 2661. Inside this message, the LNS learns that its dial-out request should be redirected to the secondary LAC, and the LNS clears the session to the primary LAC.

7. The LNS creates a new tunnel to the secondary LAC if one does not exist. The dial-out LAC creates a VPDN session and sets it in a pending state. It then places a call to the PPP client. Once the call is connected, the LAC determines to which pending VPDN session the connected interface belongs and binds the connected interface with the session. The secondary LAC sends an Outgoing Call Connected (OCCN) message to the LNS. The LNS determines for which pending virtual access interface and VPDN session this OCCN is meant, and then the LNS brings up the virtual access interface.

#### Benefits

#### Large-Scale Dial-Out Integrated with L2TP

Before Cisco IOS Release 12.2(4)T, L2TP required that requests for tunneled dial-out calls be from a single LNS to a single LAC, and that configurations be available on the local server. The L2TP Large-Scale Dial-Out feature introduced in Cisco IOS Release 12.2(4)T allows dialing multiple LACs from a single LNS. The LACs are signaled through the LNS using L2TP to establish the dial sessions. User-defined profiles can also be configured on a AAA server and retrieved by the LNS when dial-out occurs.

#### Enhanced Dial Management

The L2TP Large-Scale Dial-Out feature also provides the following benefits:

- Multiple LACs bound into one stack group
- Call traffic load balancing
- Outbound call congestion management

#### Platforms/Considerations

---

Routers	26xx, 36xx, 71xx, 72xx, 75xx
---------	------------------------------

---

#### Marketing Contact

Neil Abogado

nabog@cisco.com

#### Hardware

##### 1-Port ADSL WAN Interface Card

#### Description

The asymmetric digital subscriber line WAN interface card (ADSL WIC) enables business-class broadband service with voice integration, scalable performance, flexibility, and security for small and medium-sized businesses, and small branch offices, using the Cisco 1700 series routers; and for enterprise branch offices using the Cisco 2600, and 3600 series modular routers. These products are ideal for businesses inclined to aggregate both ADSL and other transport options into a single box.

The one-port ADSL WIC, which fits into the VIC/WIC slot on Cisco modular access platforms, provides both plain old telephone service (POTS) and ADSL high-speed digital data transmissions between customer premise equipment and central offices.

The Cisco platforms along with the ADSL WIC are ideal for small to medium-sized businesses, or small and enterprise branch offices that require a modular DSL access router platform with business-class functionality supporting scalable, secure, quality, and proven business solutions such as:

- Business-class security
- Dual WAN ports for back up and load sharing
- Intranet toll-quality voice
- ATM and IP based quality of service (QoS)
- Support for scalable routing and Web caching protocols

For more information, please see [http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/ads17\\_ds.htm](http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/ads17_ds.htm).

#### Benefits

- Modular platform that provides flexibility and investment protection for businesses and service providers
- Dual WIC support enables WAN back-up and load sharing
- Enhanced security, optional integrated firewall and VPNs with hardware-based encryption
- ATM and IP QoS
- The Cisco 1700 DSL solution can be upgraded with future DSL technologies

#### Platforms/Considerations

---

Routers	C1700
---------	-------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact  
smahadev@cisco.com

Small Office Home Office ADSL Router

#### Description

Cisco IOS Software now supports the Cisco SOHO 77 ADSL router.

#### Benefits

- Provides affordable Internet access
- Enables security with packet filtering firewall
- Enables Cisco IOS manageability and reliability features
- For users with no plans to upgrade to value-added services

#### Platforms/Considerations

---

Router	SOHO 77
--------	---------

---

First appearance in a Cisco IOS Software release: 12.1(3)XP (special release) and 12.2(2)T.

Marketing Contact  
Geir Leirvik  
geir@cisco.com

## uBR905 Cable Access Router

### Description

The Cisco uBR905 Cable Access Router delivers feature-rich broadband access to telecommuter, small office, and small branch-office customers. A fully integrated Cisco IOS Software router and CableLabs<sup>®</sup>-Certified<sup>™</sup> cable modem, it interoperates with any bidirectional, CableLabs-Qualified cable modem termination system (CMTS). This compact device includes the familiar features and programming interface of other routers in the extensive line of Cisco small and medium-sized business product offerings.

The Cisco uBR905 supports hardware-accelerated IP security (IPsec) virtual private networks (VPNs), making it ideal for users that require high-speed, secure remote tunneling. It also provides Cisco IOS Firewall protection capabilities. A data-only device, it is suitable for applications not requiring voice, or for applications that support voice through an Ethernet port.

The Cisco uBR905 leverages many design elements from the award-winning Cisco uBR924, providing a reliable, stable platform. In addition, its use of common software used by all Cisco cable customer premises equipment (CPE) devices offers a dependable and proven operating environment as well as investment protection through ongoing enhancement of the operating system.

Please access additional information on the Cisco uBR905 Cable Access Router at:

[http://www.cisco.com/warp/public/cc/pd/rt/900/prodlit/u905\\_ds.pdf](http://www.cisco.com/warp/public/cc/pd/rt/900/prodlit/u905_ds.pdf)

### Benefits

- Integrated Cable Modem, Cisco IOS Router, and Four-Port Ethernet Hub: Simplifies and reduces costs of operations with an integrated, one-box solution
- Address Management through Cisco Easy IP (NAT/PAT, Multi-NAT and DHCP Server): Preserves precious and finite public address space and provides basic security for small offices
- Integrated Cisco IOS Firewall (Optional): Provides full-featured, business-class firewall, in contrast to partial security solutions such as NAT or packet filtering
- Hardware-Accelerated Ipsec VPN—3DES (Optional) and 56 bit (Included): Supports high-speed, secure IPsec VPN technology; ideal for telecommuters or LAN extension applications
- DOCSIS 1.1 Ready: Supports BPI+ certificates and SNMP v3 at FCS, which simplifies transition to DOCSIS 1.1

### Platforms/Consideration

---

Universal Broadband Routers (UBR)

uBR900

---

First appearance in a Cisco IOS Software release: 12.1(3)XL, 12.2(2)T.

### Marketing Contact

Gwen Byard

[gbyard@cisco.com](mailto:gbyard@cisco.com)

### IP & Routing

IPv6 for Cisco IOS Software

### Description

The continuous growth of the global Internet requires that the Internet architecture evolve to accommodate new technologies as well as increasing numbers of users, applications, and services.

IP version 6 (IPv6) is designed to enable ongoing Internet expansion to accommodate the continuous growth of the Internet. Fundamental to the successful market adoption of the new Internet protocol version is its smooth integration into existing networks and its coexistence with IP version 4 who is the current foundation of the Internet.

Release 12.2(2)T is the first one to integrate support of the new IPv6 protocol into Cisco IOS Software. Thus, IPv4 and IPv6 versions will coexist for the foreseeable future and will be included in Cisco IOS Software upgrades at no extra charge.

Please refer to additional information on Cisco IOS IPv6 at: [www.cisco.com/ipv6](http://www.cisco.com/ipv6) Cisco IPv6. Statement of Direction is available at the URL above.

#### Benefits

- IPv6 protocol support (RFC 2460, RFC 2374)
  - IPv6 Addressing Architecture (RFC 2373)
  - IPv6 Stateless Address Auto-configuration (RFC 2462)
  - ICMPv6 (RFC 2463)
  - Neighbor Discovery (RFC 2461)
- IPv6 Routing Protocols
  - Static Route
  - RIPng (RFC 2080)
  - Multi-Protocol Extensions for BGP4 (RFC 2545 & 2858)
- IPv6 over Data Link Layers
  - Ethernet 10/100/1000Mb/s (RFC 2464)
  - FDDI (RFC 2467)
  - Cisco HDLC
  - ATM PVC
  - Frame Relay PVC (RFC 2590)
  - PPP (RFC 2472), including Serial Link, ISDN and POSIP
- IPv6 Transition Tools
  - Configured IPv6 over IPv4 Tunnels
  - Automatic IPv6 over IPv4 Tunnels
  - 6to4 Tunnels
- IPv6 Management Tools
  - Standard Access Control List (ACL)
  - Route Map
  - Ping for IPv6
  - Traceroute for IPv6
  - Telnet over an IPv6 transport
  - TFTP over an IPv6 transport

#### Platforms/Considerations

---

Routers	C800, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500, uBR7200
---------	--

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact  
 Patrick Grossetete  
 pgrosset@cisco.com

NAT Support of H.323v2 RAS

**Description**

Voice over IP (VoIP) solutions in the marketplace make use of a number of protocols, one of these is H.323 Registration, Admission and Status (RAS).

RAS provides a number of messages that are used by software clients and VoIP devices to register their location, request assistance in call set-up, controlling bandwidth and so on. These RAS messages are directed towards something called an H.323 Gatekeeper.

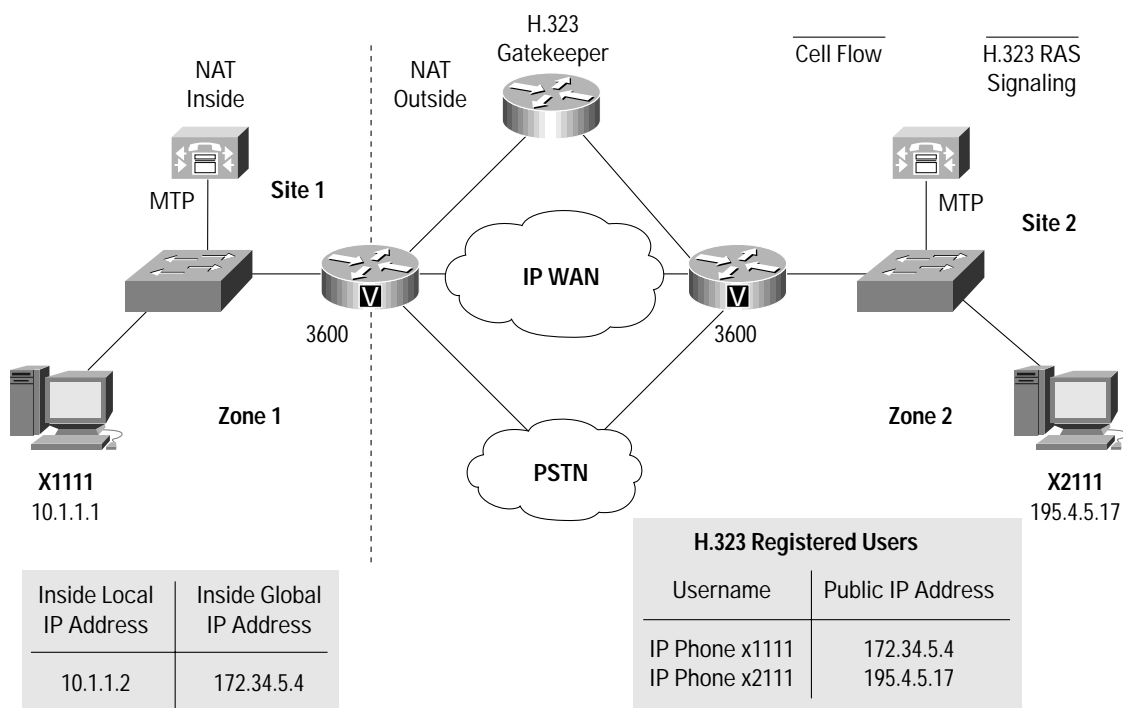
Some of the RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or find out about another user already registered. If these messages are not known to NAT they cannot be translated to an IP address which will be visible to the “public”.

As of 12.2(2)T the Cisco IOS Software feature Network Address Translation (NAT) now understands H.323 RAS messages and can inspect any embedded IP addresses for potential address translation. This enables a user to maintain control over their IP addressing schemes and still deploy a number of Cisco VoIP solutions.

Cisco has several products that have support for RAS

- Voice Gateway
- Cisco Multimedia Conference Manager
- Cisco CallManager

Figure 1 Cisco IOS NAT Support for H.323 RAS



### Benefits

- Customers can control their IP address scheme and include complete support for H.323 Gatekeeper designs.
- Network Address Translation (NAT) enables customers to deploy private IP addresses within their network and perform translation to public IP addresses when connecting to the Internet or interconnecting with another corporate network.

### Platforms/Considerations

---

Routers	C800, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Mark Denny

mdenny@cisco.com

### BGP Conditional Route Injection

#### Description

Routes that are advertised through the Border Gateway Protocol (BGP) are commonly aggregated to minimize the number of routes that are used and reduce the size of global routing tables. However, common route aggregation can obscure more specific routing information that is more accurate but not necessary to forward packets to their destinations. Routing accuracy is obscured by common route aggregation because a prefix that represents multiple addresses or hosts over a large topological area cannot be accurately reflected in a single route. Cisco IOS software provides several methods in which you can originate a prefix into BGP. The existing methods include redistribution and using the network or aggregate-address commands. These methods assume the existence of more specific routing information (matching the route to be originated) in either the routing table or the BGP table.

The BGP Conditional Route Injection feature allows you to originate a prefix into a BGP routing table without the corresponding match. This feature allows more specific routes to be generated based on administrative policy or traffic engineering information in order to provide more specific control over the forwarding of packets to these more specific routes, which are injected into the BGP routing table only if the configured conditions are met. Enabling this feature will allow you to improve the accuracy of common route aggregation by conditionally injecting or replacing less specific prefixes with more specific prefixes. Only prefixes that are equal to or more specific than the original prefix may be injected. The BGP Conditional Route Injection feature is enabled with the `bgp inject-map exist map` command. This command uses two route maps (`inject-map` and `exist-map`) to install one (or more) more specific prefixes into a BGP routing table. The `exist-map` specifies the prefixes that the BGP speaker will track. The `inject-map` defines the prefixes that will be created and installed into the local BGP table.

#### Benefits

The BGP Conditional Route Injection feature allows you to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.

### Platforms/Considerations

---

Routers	14xx, 16xx, 17xx, 26xx, 28xx, 362x, 364x, 366x, 38xx, 45xx, 71xx, 72xx, 75xx
Node Switch Processor	6400
Universal Broadband Routers (UBR)	UBR7200

---

## BGP Multipath Load Sharing for eBGP and iBGP in an MPLS-VPN

### Description

The BGP Multipath Load Sharing for eBGP and iBGP feature allows you to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol (BGP) networks that are configured to use Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multi-homed and stub networks.

BGP will install up to the maximum number of paths allowed (configured using the maximum-paths command). BGP uses the best path algorithm to select one multipath as the best path, insert the best path into the RIB, and advertise the best path to BGP peers. Other multipaths may be inserted into the RIB, but only one path will be selected as the best path

The multipaths are used by Cisco Express Forwarding (CEF) to perform load balancing, which can be performed on a per-packet or per-source/destination pair basis. The BGP Multipath Load Sharing for eBGP and iBGP feature performs unequal cost load balancing by default by selecting BGP paths that do not have an equal cost of the Interior Gateway Protocol (IGP). In order to enable the BGP Multipath Load Sharing for eBGP and iBGP feature, the router must be configured with MPLS VPNs that contain VPN routing and forwarding instances (VRFs) that import both eBGP and iBGP paths. The number of multipaths can be configured separately for each VRF.

### Benefits

#### Improved Load Balancing

The BGP Multipath Load Sharing for eBGP and iBGP feature allows multi-homed autonomous systems and Provider Edge (PE) routers to be configured to distribute traffic across both eBGP and iBGP paths.

### Platforms/Considerations

Routers	14xx, 16xx, 17xx, 26xx, 28xx, 362x, 364x, 366x, 38xx, 45xx, 71xx, 72xx, 75xx
Universal Broadband Routers (UBR)	UBR7200
Catalyst Switches	Catalyst 4000 Access Gateway Module, Catalyst 5000 Route Switch Feature Card, Catalyst 6000 Multilayer Switch Feature Card
Node Switch Processor	6400

### Marketing Contact

Pepe Garcia  
pepe@cisco.com

### BGP Prefix-Based Outbound Route Filtering

#### Description

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

The BGP Prefix-Based Outbound Route Filtering feature is enabled through the advertisement of ORF capabilities to peer routers. The advertisement of the ORF capability indicates that a BGP speaking router will accept a prefix list from a neighbor and apply the prefix list to locally configured ORFs (if any exist). When this capability is enabled, the BGP speaker can install the inbound prefix list filter to the remote peer as an outbound filter, which reduces unwanted routing updates.

The BGP Prefix-Based Outbound Route Filtering feature can be configured with send, receive, or send and receive ORF capabilities. The local peer advertises the ORF capability in send mode. The remote peer receives the ORF capability in receive mode and applies the filter as outbound policy. The local and remote peers exchange updates to maintain the ORF for each router. Updates are exchanged between peer routers by address family depending on the ORF prefix list capability that is advertised. The remote peer starts sending updates to the local peer after a route refresh request or an ORF prefix list with immediate status has been received. The BGP speaker will continue to apply the inbound prefix list to received updates after the speaker pushes the inbound prefix list to the remote peer.

#### Benefits

The BGP Prefix-Based Outbound Route Filtering feature can limit the number of unwanted routing updates, which will reduce the amount of resources required for routing update generation and processing. This feature also reduces the amount of resources required to receive and discard routes that would otherwise be filtered out.

#### Platforms/Considerations

Routers	14xx, 16xx, 17xx, 26xx, 28xx, 362x, 364x, 366x, 38xx, 45xx, 6400 NSP, 71xx, 72xx, 75xx
Universal Broadband Routers (UBR)	UBR7200

#### Distributed Director

##### Description

Cisco Distributed Director can use all of its decision-making metrics to determine the best server for a client request. From the configured metrics, Distributed Director chooses the best distributed server and returns its IP address to the local Domain Name System (DNS) server for the client.

The new ip director default priorities command specifies the default priorities for each type of metric. The default priorities will take effect if no host-specific priorities are specified in the ip director host priority command or in the corresponding DNS text record. If a metric does not have a priority or a weight specified, the metric is ignored.

The new ip director drp rttprobe command sets the protocol used by Director Response Protocol (DRP) agents for round trip time (RTT) probing. The protocols to be set are the Transmission Control Protocol (TCP) and the Internet Control Message Protocol (ICMP). Both protocols can be activated, in which case DistributedDirector will instruct DRP agents to return the RTT collected from either the TCP or the ICMP, whichever becomes available first. Using the no form of the command causes DistributedDirector to stop using a specified protocol for RTT probing. At any time, one of the protocols must be activated, and both protocols can be activated if desired. The default protocol is TCP.

The new ip dns server command enables the DNS server on the router.

The new show ip director default priority command is used to verify the default priority for any metric.

The ip director default-weights command name has been modified slightly in this release. The command name is now ip director default weights.

#### Benefits

The ip director default priorities command sets defaults for DistributedDirector metrics.

The ip director drp rttprobe command allows users to select the protocol for RTT probing that works best for your system.

The ip dns server command allows users to activate and use the DNS server on the router.

The show ip director default priority command allows user to verify the default priority for any metric.

#### Platforms/Considerations

---

Routers

26xx, 3620, 3640, 3660, 72xx

---

### IPSec MIB Support for Cisco IPSec VPN Management

#### Description

The IP Security (IPSec) MIB Support for Virtual Private Network (VPN) Management feature introduces Cisco IOS-software specific IPSec MIBs for use in VPN Management. The IPSec MIBs allow Cisco IPSec configuration monitoring, and can be integrated in a variety of VPN management solutions.

This feature allows users to specify the desired size of a tunnel history table or a tunnel failure table using the Cisco IOS CLI. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also provides IPSec SNMP notifications for use with network management systems.

#### Benefits

By allowing the user to adjust tunnel tables and enable IPSec trap notifications using the Cisco IOS CLI, the IPSec MIB Support feature provides additional VPN security monitoring capabilities.

#### Platforms/Considerations

---

Routers

8xx, 17xx, 26xx, 3620, 3640, 3660, 71xx, 72xx

---

### Marketing Contact

Mika Loukola

mloukola@cisco.com

### OSPF ABR Type 3 LSA Filtering

#### Description

The ABR Type 3 link-state advertisement (LSA) Filtering feature extends the ability of an ABR that is running the OSPF protocol to filter type 3 LSAs between different OSPF areas. This feature allows only specified prefixes to be sent from one area to another area and restricts all other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time. This feature is supported by the addition of the area filter-list command.

#### Benefits

The ABR Type 3 Lsa Filtering feature gives the administrator improved control of route distribution between OSPF areas.

## Platforms/Considerations

Routers	1xxx, 14xx, 16xx, 17xx, 26xx, 362x, 364x, 366x, 45xx, 6400 NSP, 7xxx RSP, 71xx, 72xx, 75xx, 77xx
Universal Broadband Routers (UBR)	UBR7200
Multiservice Access Concentrator	MC3810
Catalyst Switches (CAT)	4000

### OSPF Stub Router Advertisement

#### Description

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shutdown or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors.

When any of these three configuration options are enabled on a router, the router will originate link-state advertisements (LSAs) with a maximum metric (LSInfinity: 0xFFFF) through all non-stub links. The advertisement of a maximum metric causes other routers to assign a cost to this router that is higher than the cost of using an alternate path. Because of the high cost assigned to paths that pass through this router, other routers will not use a path through this router as a transit path to forward traffic that is destined for other networks, which allows switching and routing functions to be up and running and routing tables to converge before transit traffic is routed through this router.

#### Allowing Routing Tables to Converge

Two configuration options that are introduced by the OSPF Stub Router Advertisement feature allow you to bring a new router into a network without immediately routing traffic through the new router. These configuration options are useful because Interior Gateway Protocols (IGPs) converge very quickly upon a router during startup or after a reload, often before Border Gateway Protocol (BGP) routing tables have completely converged. If neighbor routers forward traffic through a router while that router is building BGP routing tables, packets that have been received for other destinations may be dropped. Advertising an maximum metric during startup will allow routing tables to converge before traffic that is destined for other networks is sent through the router. The following two configuration options enable a router to advertise a maximum metric at startup:

- You can configure a timer to advertise a maximum metric when the router is started or reloaded. When this option is configured, the router will advertise a maximum metric, which forces neighbor routers to select alternate paths until the timer expires. When the timer expires, the router will advertise accurate (normal) metrics, and other routers will send traffic to this router depending on the cost. The configurable range of the timer is from 5 to 86,400 seconds.
- You can configure a router to advertise a maximum metric at startup until BGP routing tables converge or until the default timer expires (600 seconds). Once BGP routing tables converge or the default timer expires, the router will advertise accurate (normal) metrics and other routers will send traffic to this router depending on the cost.

#### Configuring a Graceful Shutdown

The third configuration option that is introduced by the OSPF Stub Router Advertisement feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down. There are many situations where you may need to remove a router from the network. If a router is removed from a network and neighbor routers cannot detect that the physical interface is down, neighbors will need to wait for dead timers to expire before the neighbors will remove the adjacency and

routing tables will reconverge. This situation may occur when there is a switch between other routers and the router that is shut down. Packets may be dropped while the neighbor routing tables reconverge. When this third option is configured, the router advertises a maximum metric, which allows neighbor routers to select alternate paths before the router is shut down. This configuration option could also be used to remove a router that is in a critical condition from the network without affecting traffic that is destined for other networks.

#### Benefits

##### Improved Stability and Availability

Advertising a maximum metric through all links at startup or during a reload will prevent neighbor routers from using a path through the router as a transit path, thereby reducing the number of packets that are dropped and improving the stability and availability of the network.

##### Graceful Removal From the Network

Advertising a maximum metric before shutdown allows other routers to select alternate paths before the transit path through a router becomes inaccessible.

#### Platforms/Considerations

Routers	1xxx, 14xx, 16xx, 17xx, 26xx, 3620, 3640, 3660, 38xx, 45xx, 6400 NSP, 71xx, 72xx, 75xx, 77xx, 10xxx
Universal Broadband Routers (UBR)	UBR7200
Multiservice Access Concentrator	MC3810

#### OSPF Update Packet-Pacing Configurable Timers

##### Description

The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which Open Shortest Path First (OSPF) link-state advertisement (LSA) flood pacing, group pacing and retransmission pacing updates occur.

#### Platforms/Considerations

Routers	26xx, 3620, 3640, 3660, 45xx, 53xx, 58xx, 64xx, 72xx, 75xx, 10xxx, 12xxx
Universal Broadband Routers (UBR)	UBR7200
Catalyst Switches (CAT)	5000, 6000, 8510, 8540

## Management

#### Circuit Interface Identification Persistence for SNMP

##### Description

In current Cisco IOS Software releases, circuit description is not kept in non-volatile RAM, therefore when a device is rebooted, all circuit description is lost and user has to re-enter all the detail information.

With Circuit description MIB persistence, users can be certain that when the device is rebooted, the circuit description stays intact.

#### Benefits

- Eliminates the need to repeatedly re-enter circuit information when the device is rebooted.

## Platforms/Considerations

---

Routers

C1600, C2600, C3620, C3640, C3660, C7500, uBR7200

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Michael Lin

mhelin@cisco.com

CNS Event Agent and CNS Configuration Agent

### Description

The Cisco Networking Services (CNS) Event Agent and CNS Configuration Agent in Cisco IOS Software work with the Intelligence Engine 2100 series (IE2100) network device to form the larger CNS programmable network solution. This exposes the Cisco IOS XML interface via a shared communications bus.

The CNS Event Agent provides a general—purpose publish-subscribe eventing service to agents residing in Cisco IOS (such as CNS Configuration Agent).

The CNS Configuration Agent provides “plug and play” capability for initial configuration as well as incremental configuration update and introduces on-box validation, two-stage commit, and synchronized commit across multiple devices.

### Benefits

- Single programmable XML-based interface to multiple devices
- Plug-and-play initial configuration
- Two-stage synchronized commit across multiple devices
- Easy integration into existing OSS and process workflow applications

## Platform/Considerations

---

Routers

C800, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500

Multiservice Access Concentrator (MC)

MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T

### Marketing Contact

Sairaj Pakkam

spakkam@cisco.com

Interface Index Display

### Description

In current Cisco IOS Software releases, there are no command to show SNMP index assigned to an interface. This new command now offers the capability for users to easily see SNMP indices assigned.

### Benefits

- This feature makes it easy to view SNMP indices assigned to an interface.

### Platforms/Considerations

---

Routers	C800, C820, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500, uBR7200
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Michael Lin  
mhelin@cisco.com

Interface Alias Long Name Support

#### Description

In current Cisco IOS Software releases, the alias field is too short. This feature extends the alias field to 256 characters.

#### Benefits

- Offers the capability to place long alias names in large networks.

### Platforms/Considerations

---

Routers	C800, C805, C820, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500, vg200
---------	--

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Michael Lin  
mhelin@cisco.com

MPLS Label Distribution Protocol MIB

#### Description

This feature provides MPLS Label Distribution Protocol (LDP) MIB support for management and monitoring purposes for network administrators. This MIB support is compliant with the IETF definition of MPLS LDP MIB.

The MIB support allows any SNMP-capable network management stations to monitor the status of LDP sessions by polling the managed objects that define LDP entities, LDP peers and LDP sessions. It enables network administrators to monitor and control network devices that are running LDP in an MPLS network.

#### Benefits

- Better Network Management—Any SNMP-capable network management station can be used to monitor the status of the MPLS capable routers.
- Better Debugging—Allows Network Administrators to look at LDP session and peers and co-relate information to do better debugging during outages or problems
- Standards support—MPLS LDP MIB is based on the IETF MPLS LDP MIB allowing an interoperable solution based on standards.

### Platforms/Considerations

---

Routers	C7200, C7500
---------	--------------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

## Marketing Contact

Azhar Sayeed

asayeed@cisco.com

## MPLS Label Switching Router MIB

### Description

The MPLS Label Switch Router MIB support was added in Cisco IOS Software Release 12.2(2)T. It contains the managed objects required to support MPLS Label Switch routers and is compliant with IETF MPLS-LSR-MIB-0.5 version.

Network administrators can now determine the status and monitor MPLS-capable interfaces on the Label Switch Router by looking at the incoming and outgoing labels and their associated parameters via an SNMP capable Network management station. Network management station can also retrieve cross connect information that shows the association of incoming labels with outgoing labels.

### Benefits

- Better Status and Monitoring—Any SNMP-capable device can now poll the router for the MPLS information.
- Standards Based MIB—This MIB is based on IETF MPLS-LSR MIB revision 05.
- Easier debugging—Using the cross connect information obtained from the MIB the network manager can easily associate the incoming MPLS segments with outgoing MPLS segments.

### Platforms/Considerations

---

Routers	C3640, C7200, C7500
---------	---------------------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

## Marketing Contact

Azhar Sayeed

asayeed@cisco.com

## NetFlow Multiple Export Destinations

### Description

Currently, Cisco devices export NetFlow data to a single collection server and there is no backup mechanism. This feature offers the capability to export to multiple destination so NetFlow data can be exported to two different destinations (servers) and enables the ability to back up the NetFlow data on a separate server.

### Benefits

- Fail safe Netflow data export—Multiple data export offers the security of providing a backup in the event of server failure.

### Platforms/Considerations

---

Routers	C1400, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7200, C7500
---------	--

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

## Marketing Contact

Michael Lin

mhelin@cisco.com

## SIP User Agent MIB

### Description

The SIP User Agent MIB addresses the need for SIP specific gateway information to be made available by SNMP. The implementation of this capability is based upon the current IETF draft 'draft-ietf-sip-mib-01.txt'.

The implementation of the SIP MIB in the Cisco SIP gateway supports configuration objects related to SIP such as the configured SIP server, SIP timers, and number of retry attempts allowed for requests and responses.

The SIP MIB also supports SIP specific statistical information objects. This includes information on numbers of provisional responses, success responses, redirection responses, client error responses, server error responses, and global error responses. In addition, The SIP MIB includes information regarding SIP Requests initiated and received as well as information about retries associated with each SIP Request type.

### Benefits

- Provides SIP specific information via SNMP—this information allows customers to have SIP specific information available to evaluate the performance of gateways in conjunction with their SIP networks

### Platforms/Considerations

---

Routers	C2600, C3620, C3640, C3660
---------	----------------------------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Steve Levy

stlevy@cisco.com

SNMP Trap Support for VSI Master MIB

### Description

VSI Master is the software that resides on the router that controls the operation of an ATM switch for MPLS LSP setup. VSI Master MIB provides support for management and monitoring of the VSI master and its associated parameters for better control of network elements.

Each VSI master can connect to one or multiple VSI slaves (ATM switches). Monitoring information needs to be polled via SNMP GETs to obtain information about the switches or the routers.

SNMP trap support adds speedy notification of the changes/failures in the network element by sending an SNMP trap to the management or monitoring stations that can alert the network administrators of a possible problem which requires corrective/preventive action.

Traps can be set on threshold values in the managed objects of the VSI master MIB.

### Benefits

- Speedy notification—This feature allows speedy notification of failure or trouble conditions to network administrators by sending SNMP trap messages to the network management stations.
- Simpler management—Provides alarm capability so that network managers can focus on the critical things.
- Better network resource usage—Provides better usage of network resources as network managers can now take corrective action before the failure conditions thereby reducing down time and improving network performance.

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Azhar Sayeed

asayeed@cisco.com

#### ATM SNMP Trap and OAM Enhancements

##### Description

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to Operation, Administration, and Maintenance (OAM) functionality:

- ATM PVC traps will now be generated when the operational state of a PVC changes from the DOWN to UP state.
- ATM PVC traps will now be generated when OAM loopback fails. Additionally, when OAM loopback fails, the PVC will now remain in the UP state, rather than going down.
- The ATM PVC traps are now extended to include virtual path identifier/virtual channel identifier (VPI/ VCI) information, the number of state transitions a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

The ATM SNMP trap and OAM enhancements are described in the following sections:

- ATM PVC UP Trap
- ATM PVC OAM Failure Trap
- Extended ATM PVC Traps
- Supported MIB Objects and Tables

#### ATM PVC UP Trap

Before the introduction of the ATM SNMP trap and OAM enhancements, the only SNMP notifications for ATM PVCs were the ATM PVC DOWN traps, which were generated when a PVC failed or left the UP operational state. The ATM SNMP trap and OAM enhancements introduce ATM PVC UP traps, which are generated when a PVC changes from the DOWN to the UP state.

#### ATM PVC OAM Failure Trap

The ATM SNMP trap and OAM enhancements introduce the ATM PVC OAM failure trap. OAM loopback is a mechanism that detects whether a connection is UP or DOWN by sending OAM end-to-end loopback command/response cells. An OAM loopback failure indicates that the PVC has lost connectivity. The ATM PVC OAM failure trap is generated when OAM loopback for a PVC fails and is sent at the end of the notification interval.

When OAM loopback for a PVC fails, the PVC is included in the atmStatusChangePvcIRangeTable or atmCurrentStatusChangePvcITable and in the ATM PVC OAM failure trap.

Before the introduction of this feature, if OAM loopback failed, the PVC would be placed in the DOWN state. When the ATM PVC OAM failure trap is enabled, the PVC remains UP when OAM loopback fails so that the flow of data will still be possible.

## Extended ATM PVC Traps

The ATM SNMP Trap and OAM Enhancements feature introduces extended ATM PVC traps. The extended traps include VPI/VCI information for affected PVCs, the number of UP-to-DOWN and DOWN-to-UP state transitions a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

## Supported MIB Objects and Tables

The ATM PVC trap is defined in the ATM PVC trap MIB. The ATM SNMP trap and OAM enhancements introduce the following MIB objects and tables:

- The table atmInterfaceExt2Table displays the status of ATM PVCs and is indexed by ifIndex. This table contains the following objects:
  - atmIntfCurrentlyDownToUpPVcls
  - atmIntfOAMFailedPVcls
  - atmIntfCurrentlyOAMFailingPVcls
- The table atmCurrentStatusChangePvcTable displays information about ATM PVCs that have gone through an operational state change and is indexed by ifIndex, atmVclVpi, and atmVclVci. This table contains the following objects:
  - atmPvcStatusTransition
  - atmPvcStatusChangeStart
  - atmPvcStatusChangeEnd
- The table atmStatusChangePvcRangeTable displays information about ATM PVC ranges and is indexed by ifIndex, atmVclVpi, and rangeIndex. This table contains the following objects:
  - atmPvcLowerRangeValue
  - atmPvcHigherRangeValue
  - atmPvcRangeStatusChangeStart
  - atmPvcRangeStatusChangeEnd
- The ATM PVC UP Trap “atmIntfPvcUpTrap” contains the following objects:
  - ifIndex
  - atmIntfCurrentlyDownToUpPVcls
- The ATM PVC OAM Failure Trap “atmIntfPvcOAMFailureTrap” contains the following objects:
  - ifIndex
  - atmIntfOAMFailedPVcls
  - atmIntfCurrentlyOAMFailingPVcls

For a complete description of the extended ATM PVC MIB, see the MIB file called CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my, available through Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### Benefits

The ATM SNMP Trap and OAM enhancements

- Enable you to use SNMP to detect the recovery of PVCs that have gone DOWN.
- Enable you to use SNMP to detect when OAM loopback for a PVC has failed.
- Keep the PVC in the UP state when OAM loopback has failed, allowing for the continued flow of data.

- Provide VPI/VCI information in the ATM PVC traps, letting you know which PVC has changed operational state or has had an OAM loopback failure.
- Provide statistics on the number of state transitions a PVC goes through.

#### Platforms/Considerations

---

Routers	17xx, 26xx, 36xx, 38xx, 45xx, 64xx, 72xx, 75xx
---------	--

---

#### Marketing Contact

Michael Lin

mhelin@cisco.com

#### PIM MIB Extension for IP Multicast

##### Description

Protocol Independent Multicast (PIM) is an IP Multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the Protocol Independent Multicast for IPv4 MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

The PIM MIB Extension for IP Multicast feature introduces support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the existing Cisco implementation of the PIM MIB (PIM-MIB). This feature introduces the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - when a router’s PIM interface is disabled or enabled (using the ip pim command in interface configuration mode).
  - when a router’s PIM neighbor adjacency expires or is established (defined in RFC 2934).
- rp-mapping-change—This notification results from a change in RP mapping information due to either Auto-RP or bootstrap router (BSR) messages.
- invalid-pim-message—This notification results from the following conditions:
  - when an invalid (\*, G) join or prune message is received by the device (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group).
  - when an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP).

##### Benefits

- Allows users to identify changes in the multicast topology of their network by detecting changes in the RP mapping.
- Provides traps to monitor the PIM protocol on PIM-enabled interfaces.
- Helps users identify routing issues when multicast neighbor adjacencies expire or are established on a multicast interface.
- Enables users to monitor RP configuration errors (for example, errors due to flapping in dynamic RP allocation protocols like Auto-RP).

#### Platforms/Considerations

---

Routers	16xx, 3620, 3640, 45xx, 58xx, 64xx NPR, 71xx, 72xx, 75xx
Universal Broadband Routers (UBR)	UBR7200

---

## Mobile Networks

### Cisco Mobile Networks

#### Description

The Cisco Mobile Networks feature enables a Mobile Router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this Mobile Router.

Mobile IP, as defined in standard RFC 2002, provides the architecture that enables the Mobile Router to connect back to its home network. Mobile IP allows a device to roam while appearing to a user to be at its home network. Such a device is called a mobile node. A mobile node is a node—for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone—that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain ongoing communications while using the same IP address.

The Mobile Router functions similarly to the mobile node with one key difference—the Mobile Router allows entire networks to roam. For example, a plane with a Mobile Router can fly around the world while passengers stay connected to the Internet. This communication is accomplished by Mobile IP aware routers tunneling packets, which are destined to hosts on the mobile networks, to the location where the Mobile Router is visiting. The Mobile Router then forwards the packets to the destination device.

These devices can be mobile nodes running mobile IP client software or nodes without the software. The Mobile Router eliminates the need for a mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The Mobile Router “hides” the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

The Cisco Mobile Networks feature is a static network implementation that supports stub routers only. The Mobile Router avoids convergence problems by statically defining which networks it can address. The Mobile Router can do the following:

- Perform agent solicitation
- Perform registration and reregistration
- Decapsulate information for its attached devices

#### Cisco Mobile Network Components

The Cisco Mobile Networks feature comprises three components described in the following sections:

- Home Agent
- Foreign Agent
- Mobile Router

#### *Home Agent*

A Home Agent is a router on the home network of the Mobile Router that maintains an association between the home IP address of the Mobile Router and its care-of address, which is the current location of the Mobile Router on a foreign or visited network.

The Home Agent provides the anchoring point for the mobile networks on the Mobile Router. Once the Mobile Router has registered with the Home Agent, the Home Agent adds the mobile networks to its routing table and redistributes these routes. Traffic to the mobile networks arrives at the Home Agent, which tunnels it to the Foreign Agent, which in turn forwards it to the Mobile Router for forwarding to the destination device on the mobile network.

The Home Agent supplies the static network definitions for the mobile networks. As the Mobile Router moves from one Foreign Agent to another, the Mobile Router continuously reconfigures the default gateway definition to point to its new path. Although the Mobile Router can register through different Foreign Agents, the most recently contacted Foreign Agent provides the active connection.

### *Foreign Agent*

A Foreign Agent is a router on a foreign network that assists the Mobile Router in informing its Home Agent of its current care-of address. The Foreign Agent is a fixed router with a direct logical connection to the Mobile Router. That direct logical connection is not expected to be on the same subnet as the Foreign Agent interface.

However, the Foreign Agent needs a route to the Home Agent to accommodate a Mobile Router tunnel. The interface that is directly connected to the Mobile Router uses ICMP Router Discovery Protocol (IRDP). The Foreign Agent sends out advertisements using IRDP to allow the Mobile Router to attach to a foreign network. The Foreign Agent relays registrations between the Home Agent and the Mobile Router in order for the Mobile Router to notify the Home Agent of its whereabouts. For traffic to the Mobile Router, the Foreign Agent detunnels packets from the Home Agent before forwarding them to the Mobile Router. The Foreign Agent will then forward traffic from the Mobile Router using normal routing.

### *Mobile Router*

Any of the Cisco 2600, 3600, 7200, or 7500 series routers can serve as the Mobile Router. Deployed on a mobile platform (such as a car, plane, train, or emergency medical services vehicle), the Mobile Router functions as a roaming router that provides connectivity for its mobile network. A device connected to the Mobile Router need not be a mobile node because the Mobile Router is providing the roaming capabilities.

The Mobile Router is configured with the IP address of its Home Agent. The interfaces on the Mobile Router can be configured for preferred path or priority service, which allows IP traffic to quickly switch paths based upon bandwidth or priority.

There is a shared key between the Mobile Router and the Home Agent for authentication, as discussed in the “Security for Mobile Networks” section later in this document.

### How the Mobile Router Process Works

The Mobile Router process is created when configured. The process is responsible for processing incoming packets (such as agent advertisements and registration replies) and timers (such as solicitations, advertisements, and registrations).

The Mobile Router process has three main phases, which are described in the following sections:

- Agent Discovery
- Registration
- Routing

### *Agent Discovery*

During the agent discovery phase, Home Agents and Foreign Agents advertise their presence on their attached links by periodically multicasting or broadcasting messages called agent advertisements. Agent advertisements are IRDP messages that convey Mobile IP information. The advertisement contains the IRDP lifetime, which is the number of seconds the agent is considered valid. The advertisement also contains the care-of address, the point of attachment on the foreign network, as well as registration lifetime allowed and supported services such as generic routing encapsulation (GRE), and reverse tunnel.

The Mobile Router receives these advertisements on its interfaces that are configured for roaming and determines if it is connected to its home link or a foreign link.

Rather than waiting for agent advertisements, a Mobile Router can send an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.

The Mobile Router prefers a particular agent based on the received interface. If more than one interface receives agent advertisements, the one with higher roaming priority value is preferred. In the case that multiple interfaces have the same priority, the highest bandwidth is preferred. If interfaces have the same bandwidth, the highest interface IP address is preferred. The Mobile Router sends registration requests to the preferred Foreign Agent and deregistration to the preferred Home Agent.

### *Registration*

After receiving a care-of address, the Mobile Router registers this address with its Home Agent through an exchange of messages. The Home Agent creates a mobility binding table that maps the home IP address of the Mobile Router to the current care-of address of the Mobile Router. An entry in this table is called a mobility binding. The main purpose of registration is to create, modify, or delete the mobility binding of a Mobile Router (or mobile node) at its Home Agent.

After determining the preferred path, the Mobile Router sends a registration request to the Home Agent. Because the Mobile Router is attached to a foreign network, the registration request is sent first to the active Foreign Agent.

The Home Agent advertises reachability to the home IP address of the Mobile Router, thereby attracting packets that are destined for that address. When a device on the Internet, called a correspondent node, sends a packet to the Mobile Router, the packet is routed to the home network of the Mobile Router. The Home Agent intercepts the packet and performs two encapsulations of the packet and forwards it to the Foreign Agent. The Foreign Agent performs one decapsulation and forwards the packet to the Mobile Router. The Mobile Router performs the second decapsulation and forwards the packet to the devices on its networks. As the Mobile Router moves, it registers with its Home Agent on its whereabouts through various Foreign Agents.

When the Mobile Router powers down or determines that it is reconnected to its home link, it deregisters by sending a deregistration request to the Home Agent.

### *Routing*

Because the major function of a Layer 3 protocol is routing, the major features of Mobile IP deal with how to route packets to users that are mobile.

Mobile IP is a tunneling-based solution that takes advantage of the Cisco-created GRE tunneling technology and simpler IP-in-IP tunneling protocol. For more information on routing in a Mobile IP environment, refer to the “Configuring Mobile IP” chapter of the Cisco IOS IP Configuration Guide, Release 12.2.

Packets are routed through tunnels to the devices on the mobile networks. The Home Agent creates the following two tunnels:

- Between the Home Agent and care-of address
- Between the Home Agent and Mobile Router

When a correspondent node sends a packet to a device on the mobile network, it arrives on the Home Agent. The packet destined for the mobile network is encapsulated twice. It arrives at the Foreign Agent, which decapsulates the Home Agent and care-of address tunnel header and forwards the packet to the Mobile Router, which performs another decapsulation to deliver the packet to the destination device on the mobile network.

By default, packets from devices on the mobile network arrive at the Mobile Router, which forwards them to the Foreign Agent, which routes them normally.

In the case of reverse tunnel, packets from devices arrive at the Mobile Router, which encapsulates them before sending them to the Foreign Agent, which encapsulates the packets and forwards them to the Home Agent. The Home Agent decapsulates the packets and routes them.

#### Security for Mobile Networks

The Home Agent of the Mobile Router is configured with the home IP address of the Mobile Router and the mobile networks of the Mobile Router. The Message Digest 5 (MD5) hex key is also defined here. MD5 is an algorithm that takes the registration message and a key to compute the smaller chunk of data called a message digest, plus a secret key. The Mobile Router and Home Agent both have a copy of the key, called a symmetric key, and authenticate each other by comparing the results of the computation. If both yield the same result, it confirms that nothing in the packet has changed during transit.

#### Cisco Mobile Networks Redundancy

The Cisco Mobile Networks feature uses the Hot Standby Router Protocol (HSRP) to provide a full redundancy capability for the Home Agent, Foreign Agent, and Mobile Router.

HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic will immediately and transparently recover from failures. An HSRP group is composed of two or more routers that share an IP address and a MAC (Layer 2) address and act as a single virtual router. For example, your Mobile IP topology can include one or more standby Home Agents that the rest of the topology view as a single virtual Home Agent.

You must define certain HSRP group attributes on the interfaces of the Home Agents and Mobile Routers so that Mobile IP can implement the redundancy. For more information on Mobile Router redundancy see the “Enabling Mobile Router Redundancy” section later in this document. For more information on Home Agent redundancy, refer to the “Configuring Mobile IP” chapter of the Cisco IOS IP Configuration Guide, Release 12.2.

#### Benefits

##### Mobility Solution at the Network Layer

With the Mobile Router deployed in a moving vehicle, repeated reconfiguration of the various devices attached to that router as the vehicle travels to different locations is no longer necessary. Because the Mobile Router operates at the network layer and is independent of the physical layer, it operates transparently over cellular, satellite, and other media.

##### Always-On Connection to the Internet

Supports an always-on connection to the Internet, providing access to current information that enables people to stay informed and fully functional at all times. For example, aircraft pilots can access weather updates while flying and EMS vehicles can communicate with emergency room technicians while on the way to the hospital.

##### Versatile

Any IP-enabled device can be connected to the Mobile Router Local Area Network ports and achieve mobility. Applications that are not specifically designed for mobility can now be accessed and deployed.

##### Preferred Path

By using the preferred path, a network designer can specify the primary link, based upon bandwidth or priority, to reduce costs or to use a specific carrier.

## Platforms/Considerations

---

Routers

26xx, 3620, 3640, 3660, 45xx, 64xx, 72xx, 75xx

---

### Marketing Contact

Vinay Anand

vanand@cisco.com

## MPLS

### MPLS Label Distribution Protocol

#### Description

Label Distribution Protocol (LDP) is an IETF standard for Label Distribution in an MPLS Network. LDP provides a means to request and distribute labels for setting up Label switched paths in an MPLS network.

LDP is a superset of pre-standard TDP, which also supports MPLS tag distribution and binding. TDP is also supported along with LDP in Release 12.2T.

Both LDP and TDP can be configurable to run simultaneously on a router on a per link (interface) basis for directly connected neighbors and on a per-target basis for non-directly connected neighbors. The Cisco router sets up Label Switched Path transparently when one neighbor is running TDP and another running LDP. This provides backward compatibility with existing routers running tag switching and allows smooth migration to MPLS network.

#### Benefits

- Interoperability—IETF Standards based way of distributing labels provides an interoperable implementation of MPLS with other routers.
- Easy Migration—By running both TDP and LDP on a per target basis simultaneously on the same router migration of TDP environments can be done with relative ease.
- More features—LDP provides more features as it is a super set of TDP and provides important features like message header authentication using MD5 etc.

## Platforms/Considerations

---

Routers

C3620, C3640, C4500, C7200, C7500

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Azhar Sayeed

asayeed@cisco.com

DiffServ Aware MPLS Traffic Engineering

#### Description

MPLS traffic engineering allows constraint-based routing of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of “guaranteed” traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a sub-pool, while the

regular TE tunnel bandwidth is called the global pool. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate “overbooking” ratios for guaranteed and regular traffic. (In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.)

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements (such as real-time voice, virtual IP leased line, and bandwidth trading), where over-engineering cannot be assumed everywhere in the network.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

#### Benefits

Diff-Serv-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on signaled rather than provisioned QoS
- Build the higher-revenue generating “strict-commitment” QoS services, without over-provisioning
- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS

#### Platforms/Considerations

---

Routers

72xx

---

#### Marketing Contact

Amrit Hanspal

ahanspal@cisco.com

MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels

#### Description

Traffic engineering automatic bandwidth adjustment provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel’s allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

#### Benefits

The automatic bandwidth feature makes it easy to configure and monitor the bandwidth for MPLS traffic engineering tunnels. If automatic bandwidth is configured for a tunnel, traffic engineering automatically adjusts the tunnel's bandwidth.

#### Platforms/Considerations

---

Routers	36xx, 4xxx, 72xx, 75xx
---------	------------------------

---

#### Marketing Contact

Amrit Hanspal  
ahanspal@cisco.com

#### QoS

##### Class-Based Frame-Relay DE-Bit Matching and Marking

#### Description

Cisco IOS Quality of Service (QoS) provides the tools necessary to allocate network resources to the appropriate application traffic. Bandwidth, delay, jitter (delay variation), and packet loss are the critical resources to be managed. The Modular QoS CLI (MQC) framework, introduced in 12.0(5)T is the foundation upon which features such as Class-Based Weighted Fair Queuing (CBWFQ), Low-Latency Queuing (LLQ), Class-Based Policing, Class-Based Shaping, and Class-Based Marking are provisioned within Cisco IOS Software.

While most of these mechanisms deal with QoS at the packet level, and are independent of the underlying link layer, it is important to take into account the underlying Class of Service (CoS) capabilities of the link layer (such as Ethernet, frame-relay, and ATM). As an example, the IEEE 802.1Q/p standard, on Ethernet networks, allows up to 8 priority levels for Layer2 Ethernet frames (L2 CoS). Thus, a frame marked with CoS 1 will be given lower priority (for forwarding & dropping), compared to a frame marked with CoS 5.

Similarly, in frame-relay networks, the Discard-Eligible (DE) bit is used to indicate to the frame-relay switches the discard priority of a frame. Thus, frames marked with a DE-bit setting of 1 will be dropped before frames with DE 0. This Cisco IOS Release 12.2(2)T allows you to classify packets on the basis of the DE-bit being set, in addition to the capability of setting the DE-bit. This can be done using the Class-Based Policer, as well as through the match & set actions with the MQC framework.

For more information on Class-Based Marking:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/cbpmark2.htm>

For more information on the Modular QoS CLI:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5/mqc/mcli.htm>

#### Benefits

- For a given Class of Traffic (Premium, Gold, Silver, Bronze, Best Effort, etc.), this feature allows you to set the DE-bit to 1, thereby indicating (signaling) that the packets of the specified class are of less importance in the case of congestion in a Frame Relay network. The Service Provider frame-relay switch can then make the appropriate dropping decision when congestion occurs. As a real-world example, this can help protect voice packets over other data packets during times of congestion (in addition to the priority queueing & forwarding that voice packets should receive in a network).

- If a certain Class of Traffic exceeds the maximum allowed rate, packets that are over the limit can be marked with a DE-bit setting of 1. This implies, that when congestion occurs in the Service Provider frame-relay network, these packets are dropped ahead of the conforming (DE-bit 0) ones.
- On a frame-relay interface (or sub-interface), you can now classify incoming packets, based on the DE-bit being set. This technique can be used to identify low-priority packets (or out of contract packets, from a Service Provider perspective), and thereby provide the appropriate queueing and dropping behavior.

**Platforms/Considerations**

---

Routers	C2600, C3620, C3640, C3660, C4500, C7200, C7500
---------	---

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

**Marketing Contact**

Vijay Krishnamoorthy  
 kvijay@cisco.com

**Control Plane DSCP Support for RSVP**

**Description**

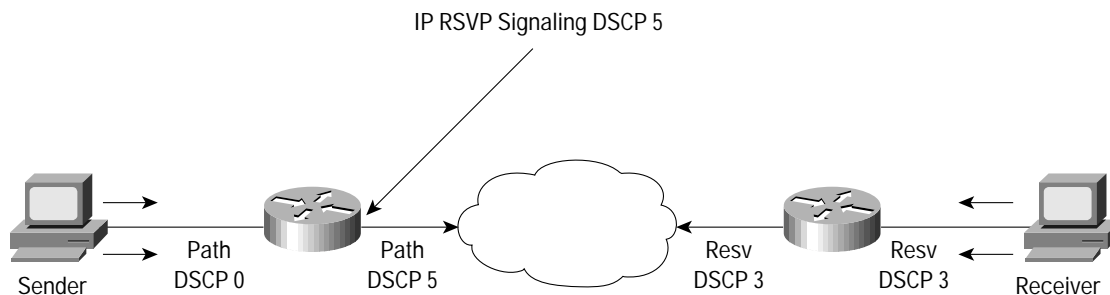
Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

The control plane DSCP support for RSVP feature allows network administrators to set the priority value in the type of service (ToS) byte/differentiated services (DiffServ) field in the IP header for RSVP signaling messages. The IP header functions with resource providers such as Weighted Fair Queuing (WFQ), so that voice frames have priority over data fragments and data frames. When packets arrive in a router’s output queue, the voice packets are placed ahead of the data frames.

Figure 3 shows a path message originating from a sender with a DSCP value of 0 (the default) that is changed to 5 and a reservation (resv) message originating from a receiver with a DSCP of 3.

Raising the DSCP value reduces the possibility of packets being dropped and improves call setup time in VoIP solutions.

Figure 2 Control Plane DSCP Support for RSVP



**Benefits**

- **Faster Call Setup Time**—The control plane DSCP support for RSVP feature allows a network administrator to set the priority for RSVP control messages. In a DiffServ QoS environment, higher priority packets get serviced before lower priority packets, thereby improving the call setup times for RSVP sessions.

- Improved Reliability of Control Messages—During periods of congestion, routers drop lower priority traffic before they drop higher priority traffic. Since RSVP control messages can now be marked with higher priority, the likelihood of these messages being dropped is significantly reduced.
- Faster Recovery after Failure Conditions—Congestion Management may have a snowballing effect in some instances. With the help of Control Plane DSCP support for RSVP feature, RSVP control messages are likely to be dropped later thereby providing faster recovery of RSVP reservations.

#### Platforms/Considerations

Routers	C2600, C3640, C3660, C7200
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Amrit Hanspal  
ahanspal@cisco.com

Low Latency Queuing Enhancement—Priority Percentage Support

#### Description

Cisco IOS Quality of Service (QoS) provides the tools necessary to allocate network resources to the appropriate application traffic. Bandwidth, delay, jitter (delay variation), and packet loss are the critical resources to be managed. The Modular QoS CLI (MQC) framework, introduced in 12.0(5)T is the foundation upon which features such as Class-Based Weighted Fair Queuing (CBWFQ), Low-Latency Queuing (LLQ), Class-Based Policing, Class-Based Shaping, and Class-Based Marking are provisioned within Cisco IOS Software.

LLQ is the complete queueing solution, comprising of CBWFQ and a Strict Priority queueing system. Prior to this release, you could specify bandwidth for a 'bandwidth' (CBWFQ class) class as a percentage of the available bandwidth on the interface/sub-interface. In this release, the functionality has been extended to the strict priority class.

Thus, you can specify bandwidth for all classes as either a percentage of the absolute available bandwidth, or (for the CBWFQ classes) as a percentage of the remaining/relative bandwidth, assuming the priority classes have been specified in kbps.

For more information on LLQ:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/pqcbwfq.htm>

For more information on the Modular QoS CLI:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5/mqc/mcli.htm>

#### Benefits

- You can now specify the priority class within LLQ using either a kbps measure, or as a percentage of the available bandwidth on the interface / sub-interface. This allows you to define generic QoS policies, and apply them on various interfaces, without having to adjust the QoS policies (provided all the bandwidth allocations of the LLQ classes are specified as a percentage of the available bandwidth).
- This enhancement gives you the flexibility to specify bandwidth for all classes as a percentage of the absolute available b/w on the interface/sub-interface.
- This enhancement also allows you to specify the priority classes in absolute kbps, and the remaining CBWFQ classes as a percentage of the remaining/relative bandwidth.

### Platforms/Considerations

---

Routers	C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Vijay Krishnamoorthy  
kvijay@cisco.com

MPLS QoS Multi-VC Mode for PA-A3

#### Description

In MPLS ATM QoS the EXP value of a MPLS Label can be mapped to an ATM Virtual Circuit (VC).

Multi-VC Mode is used to create Labeled Virtual Circuit (LVC) bundles, which consist of multiple LVCs (each LVC is referred to as bundle members), that have different QoS characteristics between any pair of ATM-connected routers. Using VC bundles, you can create differentiated services by flexibly distributing MPLS EXP values over different VC bundle members. Thus, you can apply EXP values to each bundle member or collectively at the bundle level.

MPLS QoS Multi-VC Mode for PA-A3 adds the above-mentioned feature to Cisco Enhanced ATM port adapter (PA-A3) on Cisco 7200 and Cisco 7500 routers.

#### Benefits

- Ensures effective deployment of differentiated service classes in an MPLS enabled ATM network
- Leverages existing ATM infrastructure
- Multiple low speed Virtual Circuits can be bundled to provide a single adjacency connection

### Platforms/Considerations

---

Routers	C7200
---------	-------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Amrit Hanspal  
ahanspal@cisco.com

RSVP Scalability Enhancements

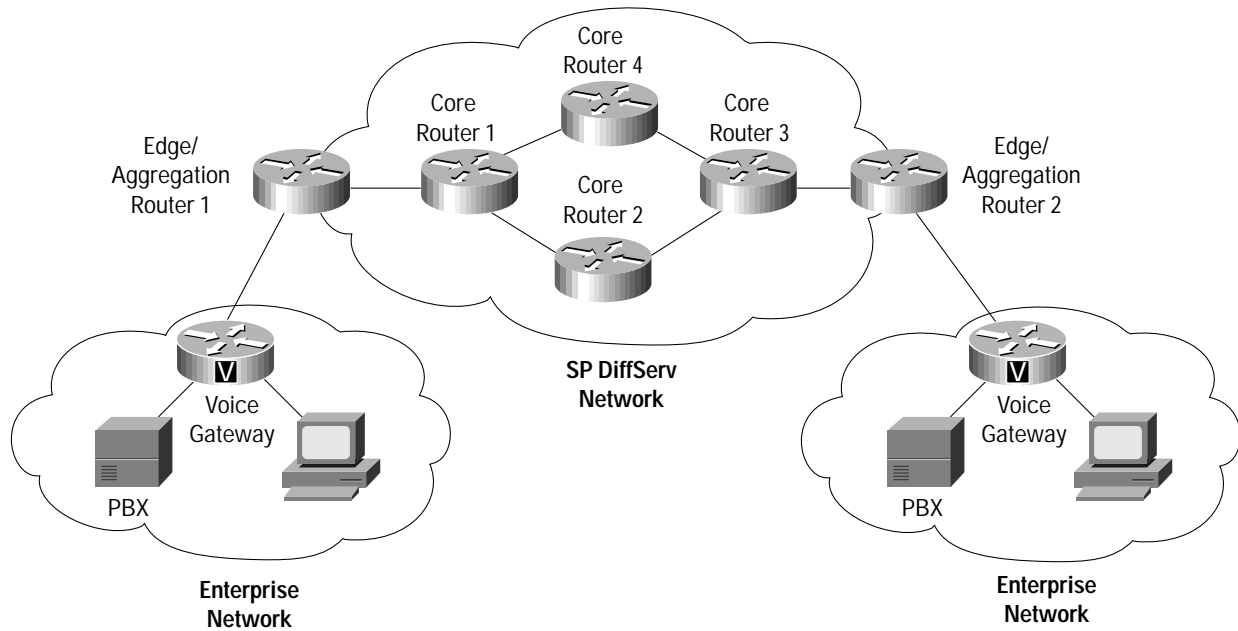
#### Description

RSVP is a signaling protocol that permits end systems to request Quality of Service (QoS) guarantees from the network. To achieve QoS, RSVP reserves bandwidth on each of a router's interfaces along the path. RSVP, currently, performs admission control, classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow. In a network in which the number of flows that RSVP maintains is relatively small, these processes function well together. However a per-flow processing model does not scale well.

RSVP Scalability Enhancements facilitate integration with service provider (differentiated services [DiffServ]) networks and to enable scalability. This feature enables RSVP to perform admission control and work with DiffServ QoS Mechanism such as classification, policing and scheduling (like CBWFQ) based on the Differentiated Services Code Point (DSCP) value in the packet's IP header, thereby eliminating the need for per-flow state and per-flow processing.

Figure 5 shows two enterprise networks interconnected through a service provider (SP) network. The SP network has an IP backbone configured as a DiffServ network. The enterprise voice gateways are running classic RSVP, while the SP Edge Router uses RSVP for admission control only on the interface connected to the SP Core Router. DiffServ QoS provides the classification, policing and scheduling functionality. The Core Routers, which run DiffServ, do not run RSVP but forward RSVP messages to the next hop.

Figure 3 RSVP/DiffServ Topology



**Benefits**

- **Enhanced Scalability:** This feature allows similar RSVP flows to be treated on a per-class basis. The resources needed to maintain per-class QoS is significantly lesser than those needed to maintain per-flow QoS. This allows for a larger number of flows to be established.
- **Improved Router Performance:** RSVP scalability enhancements improve router performance by allowing users to disable data packet classification and scheduling, which decrease central processing unit (CPU) resource consumption. The saved resources can then be used for other network management functions.

**Platforms/Considerations**

Routers	C2600, C3640, C3660, C7200
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact  
 Amrit Hanspal  
 ahanspal@cisco.com

## RSVP Support for ATM PVCs

### Description

Network administrators use queuing to manage congestion on a router interface or a permanent virtual circuit (PVC). In an ATM environment, the congestion point might not be the interface itself, but the PVC because of the traffic parameters, including the available bit rate (ABR), the constant bit rate (CBR), the unspecified bit rate (UBR), and the variable bit rate (VBR), associated with the PVC. For real-time traffic (voice flows) to be transmitted in a timely manner the data rate must not exceed the traffic parameters or packets might be dropped thereby affecting voice quality. This means that fancy queuing such as class-based weighted fair queuing (CBWFQ), low latency queuing (LLQ), or weighted fair queuing (WFQ), can run on the PVC to provide the quality of service (QoS) guarantees for the traffic.

Previously, RSVP reservations were not constrained by the traffic parameters of the flow's outbound PVC. As a result, over subscription could occur when the sum of the RSVP traffic and other traffic exceeded the PVC's capacity.

The RSVP support for ATM/PVCs feature allows RSVP to function with per-PVC queuing for voice-like flows. Specifically, RSVP can function with PVCs defined at the interface and subinterface levels. There is no limit to the number of PVCs that can be configured per interface or subinterface.

### Benefits

- Accurate Admission Control—RSVP now provides admission control based on the PVC's average cell rate, sustainable cell rate, or minimum cell rate, depending on the type of PVC that is configured, instead of the amount of bandwidth available on the interface.
- Improved QoS—RSVP provides QoS guarantees for high-priority traffic by reserving resources at the point of congestion; that is, the ATM PVC instead of the interface.
- Flexible Configurations—RSVP provides support for point-to-point and multipoint interface configurations, thus enabling deployment of services such as voice over IP (VoIP) in ATM environments with QoS guarantees.

### Platforms/Considerations

---

Routers	C2600, C3640, C3660, C7200
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Amrit Hanspal  
ahanspal@cisco.com

Call Admission Control for H.323 VoIP Gateways

### Description

#### Call Admission Control, Call Treatment, and Busyout Components

Before the call admission control feature, gateways did not have a mechanism to gracefully prevent calls from entering when certain resources were not available to process the call. This causes the new call to fail with unreported behavior, and could potentially cause the calls that are in progress to have quality related problems.

This feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume, and interface resources such as call volume.

If system resources are not available to admit the call, two kinds of actions are provided: system denial (which busyouts all of T1 or E1) or per call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

For further information on busyout, please refer to *Advanced Voicebusyout*, Cisco IOS Release 12.2(2)XA. For further information on the call denial aspects of this feature, please refer to Call Admission Control Based on CPU Utilization.

#### User Selected Threshold

This feature allows a user to configure call admission thresholds for local resources as well as memory and CPU resources. The list of local resources that are configured for call admission are described in the command description of “call threshold poll-interval”.

With the call threshold command, a user is allowed to configure two thresholds, high and low, for each resource. Call treatment is triggered when the current value of a resource goes beyond the configured high. The call treatment remains in effect until current resource value falls below the configured low. Having high and low thresholds prevents call admission flapping and provides hysteresis in call admission decision making.

With the call spike command, a user is allowed to configure the limit for incoming calls during a specified time period. A call spike is the term for when a large number of incoming calls arrive from the PSTN in a very short period of time (for example:100 incoming calls in 10 milliseconds).

#### Configurable Call Treatment

With the call treatment command, users are allowed to select how the call should be treated when local resources are not available to handle the call. For example, when the current resource value for any one of the configured triggers for call threshold has reached beyond the configured threshold, the call treatment choices are as follows:

- TDM hairpinning—Hairpins the calls through the POTS dial peer.
- Reject—Disconnects the call.
- Play message or tone—Plays a configured message or tone to the user.

#### Resource Unavailable Signaling

This feature set supports the autobusyout feature where channels are busied out when local resources are not available to handle the call. Autobusyout is supported on both channel associated signaling (CAS) and Primary Rate Interface (PRI) channels.

- CAS—Uses busyout to signal “local resources are unavailable.”
- PRI—Uses either service messages or disconnect with correct cause-code to signal “resources are unavailable.”

#### PSTN Fallback

The goal of PSTN fallback is to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion. Calls can be re-routed to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. The user defines the congestion thresholds based on the configured network. This functionality enables the service provider to give a reasonable guarantee about the quality of the conversation to their VoIP users at the time of call admission.

PSTN fallback includes the following features:

- Offers flexibility to define the congestion thresholds based on the network.
  - Defines a threshold based on Calculated Planning Impairment Factor (ICPIF), which is derived as part of International Telecommunication Union (ITU) G.113.

- Defines a threshold based solely on packet delay and loss measurements.
- Uses Service Assurance Agent (SAA) probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay and loss values are calculated.
- Is supported by calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

#### Benefits

##### Call Admission Control, Call Treatment, and Busyout

- Configurable call treatment—Allows ISP to configure how the call is supposed to be treated when local resources to process the call are not available.
  - TDM hairpinning—Hairpins the calls through the POTS dial peer.
  - Reject—Disconnects the call.
  - Play message—Plays a configured tone to the user.
- Resource unavailable signalling — Allows user to automatically busyout channels when local resources are not available to handle the call.
  - CAS—Uses busyout to signal “resources are unavailable”.
  - PRI—Uses either service messages or disconnects with correct cause code to signal “resources are unavailable”.
- User selected threshold—Allows user to configure thresholds for each of the local resources.

##### PSTN Fallback

- A call is automatically routed to any alternate destination when the data network is congested at the time of the call setup.
- PSTN fallback provides delay, jitter, and packet loss information for the configured IP addresses.
- PSTN fallback contains a network traffic cache used to maintain ICPIF and delay, loss, and jitter values which increase performance. A new call does not have to wait for probe results before it is admitted. The value is cached from a previous call.

#### Platforms/Considerations

Routers	26xx, 36xx
Multiservice Access Concentrator	MC3810
Access Servers	AS5300, AS5350, AS5400

##### IP to ATM Class of Service Mapping for SVC Bundles

#### Description

The IP to ATM Class of Service Mapping for SVC Bundles feature supports multiple SVCs to the same NSAP destination for different types of service (ToS). This feature is an extension to the feature described in the chapter “Configuring IP to ATM Class of Service” in the *Cisco IOS Quality of Service Solutions Configuration Guide*. The original feature was limited to PVCs only. This feature is an extension because it applies to SVCs.

The PVC Bundle feature requires that the user configure PVCs for different IP ToS. The PVCs have to be set up throughout the ATM network between end points. The IP to ATM Class of Service Mapping for SVC Bundles feature needs configuration only at the end points. The user uses UNI to set up SVCs in a bundle between end points. The SVCs need not be set up. When the router receives the first IP packet for the destination configured in the SVC bundle, that event triggers the SVC creation.

A default SVC is used for non-IP traffic, IP traffic with no precedence, and IP traffic with the precedence bit set but for which no SVC exists. SVC setup for the specific IP precedence traffic is triggered when the first IP packet with that precedence bit set is received.

#### Benefits

##### Reduced Configuration

SVC bundle configuration requires less configuration than a PVC configuration. The PVC bundle feature needs the configuration of PVCs in bundles throughout the ATM network. However, an SVC bundle would need configuration only at the end points and would use UNI to set up SVCs in the bundle between end points.

#### Platforms/Considerations

---

Routers

72xx, 75xx

---

#### Two-Rate Policer

##### Description

Networks police traffic by limiting the input or output transmission rate of a class of traffic based on user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or class of service (CoS).

The Two-Rate Policer performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria
- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, and Quality of Service (QoS) group.

With the Two-Rate Policer, you can enforce traffic policing according to two separate rates—committed information rate (CIR) and peak information rate (PIR). You can specify the use of these two rates, along with their corresponding values, by using two keywords, `cir` and `pir`, of the `police` command. For more information about the `police` command, see the “Command Reference” section of this document.

The Two-Rate Policer manages the maximum rate of traffic through a token bucket algorithm. The token bucket algorithm can use the user-configured values to determine the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm is affected by all traffic entering or leaving (depending on where the traffic policy with Two-Rate Policer is configured) and is useful in managing network bandwidth in cases where several large packets are sent in the same traffic stream.

The token bucket algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. Traffic entering the interface with Two-Rate Policer configured is placed in to one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be sent, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

The Two-Rate Policer is often configured on interfaces at the edge of a network to limit the rate of traffic entering or leaving the network. In the most common configurations, traffic that conforms is sent and traffic that exceeds is sent with a decreased priority or is dropped. Users can change these configuration options to suit their network needs.

## Benefits

### Bandwidth Management Through Rate Limiting

This feature provides improved bandwidth management through rate limiting. Before this feature was available, you could police traffic with the single-rate Traffic Policing feature. The Traffic Policing feature provided a certain amount of bandwidth management by allowing you to set the peak burst size (be). The Two-Rate Policer supports a higher level of bandwidth management and supports a sustained excess rate. With the Two-Rate Policer, you can enforce traffic policing according to two separate rates—CIR and PIR—specified in bits per second (bps).

### Packet Marking Through IP Precedence, QoS Group, and DSCP Value Setting

In addition to rate-limiting, the Two-Rate Policer allows you to independently mark the packet according to whether the packet conforms, exceeds, or violates a specified rate. Packet marking also allows you to partition your network into multiple priority levels or classes of service (CoS).

- Use the Two-Rate Policer to set the IP precedence or DSCP values for packets entering the network. Networking devices within your network can then use the adjusted IP precedence values to determine how the traffic should be treated. For example, the Weighted Random Early Detection (WRED) feature uses the IP precedence values to determine the probability that a packet will be dropped.
- Use the Two-Rate Policer to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

Traffic can be marked without using the Two-Rate Policer. If you want to mark traffic but do not want to use the Two-Rate Policer, see the Class-Based Marking feature module available with Cisco IOS Release 12.2(2)T. More information about the *Class-Based Marking* feature is available from the Cisco documentation website (Cisco.com) or the Cisco documentation CD.

### Packet Prioritization for Frame Relay Frames

The Two-Rate Policer allows users to mark the Frame Relay DE bit of the Frame Relay frame. The Frame Relay DE bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0.

### Packet Prioritization for ATM Cells

The Two-Rate Policer allows users to mark the ATM CLP bit in ATM cells. The ATM CLP bit is used to prioritize packets in ATM networks. The ATM CLP bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, cells with the ATM CLP bit set to 1 are discarded before cells with the ATM CLP bit set to 0.

## Platforms/Considerations

---

Routers	26xx, 36xx, 45xx, 46xx, 72xx, 75xx VIP
---------	--

---

### Marketing Contact

Vijay Krishnamoorthy  
vijakris@cisco.com

## Security

### DF Bit Override Functionality with IPsec Tunnels

#### Description

Currently, when the Don't Fragment (DF) bit is set on IP packets, there can be an issue with transmitting IP packets that are greater than 1500 bytes long. This problem occurred when an IPsec router processed the DF bit in an IPsec external header. The DF Bit Override feature, introduced in Release 12.2(2)T, addresses this issue by clearing the DF bit and fragmenting the packet on the encrypted link.

This should not be a problem, because if a packet can not enter the next link an ICMP message is sent to the source. The ICMP message tells the source to reduce the packet size, so that the packets would be able to enter the next link (encrypted link). However, firewalls may choose to filter these ICMP messages. On other hand, the Microsoft Web server does not listen to these messages even if they will get through the firewall. This is why there is a large demand for DF Bit Override Functionality with IPsec tunnels.

#### Benefits

- RFC 2401: IPsec MUST support the option of setting/clearing the DF bit when encapsulating a packet
- This solution solves an issue many have experienced

#### Platforms/Considerations

---

Routers	C800, C1600, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500
---------	--

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Mika Loukola

mika.loukola@cisco.com

#### Firewall Feature Set

#### Description

In this release the firewall feature set is delivered to the Cisco 820 series of platforms: the Cisco 826, Cisco 827 and Cisco 827-4V. The firewall feature set is an important component to provide business class security to the customers, protecting their internal networks for unauthorized access from sites on the Internet and other outside networks.

The platform uses the classic Cisco IOS Firewall Feature set, which protects from Denial of Service attacks, protects against session hi-jacking and provides a stateful inspection engine CBAC (Context Based Access Control) to inspect and protect the traffic passing through the CPE. The Firewall Feature Set also provides real time alerts as well as logging, and provides a high level of security for the small business or telecommuter using the high-speed “always on” connection provided by the CPE. The Cisco 820 series does not provide Intrusion Detection, as this higher end feature typically is used in situations where access to inside servers allowing telnet access need to be opened to allow for access from the Internet and the intrusion threat is significant.

For configuration details please refer to the Cisco IOS Software 12.2 security documentation.

#### Benefits

- CBAC Stateful Firewall protection provides protection against multi packet as well as atomic (single packet) attacks
- Java blocking—allows centralized protection from Java applets
- SMTP inspection—checks SMTP (simple mail transfer protocol) and filters out ESMTP commands that can be utilized in a mail server attacks

- Denial of Service attack protection—protects gains a number of denial of service attacks, like TCP syn flooding, SMURF attacks and many more
- Audit trail and realtime alerts—provide alerting and a track of events that has passed to enable threat analysis

**Platforms/Considerations**

---

Routers	C800, C805, C820, C1400, C1600, C1700, C2600, C3620, C3640, C3660, C7100, C7200, C7500, uBR905, C4GWY
---------	---

---

First appearance in a Cisco IOS Software release: 12.1(3)XG (special release) and 12.2(2)T.

**Marketing Contact**

Geir Leirvik  
geir@cisco.com

IPsec Triple DES

**Description**

IPsec Triple DES is an enhancement of the existing DES 56-bit encryption scheme. This allows for stronger encryption and increases the time it takes to decrypt captured messages, and in most cases, this feature provides confidentiality of the data that is in transit.

**Benefits**

- Provides high level of confidentiality of data in transit provided by strong encryption. IPsec Triple DES also often referred to as 3DES.

**Platforms/Considerations**

---

Routers	C800, C805, C820, C1700, C2600, C3620, C3640, C3660, C4500, C7100, C7200, C7500, uBR905
---------	---

---

First appearance in a Cisco IOS Software release: 12.1(3)XG (special release) and 12.2(2)T.

**Marketing Contact**

Geir Leirvik  
geir@cisco.com

Secure Copy

**Description**

Cisco IOS Software has had the ability to copy files (for example startup-config and router images) to and from routers using various ways, including rcp (from the Berkeley r-tools suite). Recently, Cisco IOS Software has started to support SSH (Secure Shell), which is a secure replacement for the Berkeley r-tool suite, however SCP (secure copy) functionality was not included. Users are increasingly aware of security and may have routers that need secure management spread out all over the Internet. While SSH and SCP are not the most comprehensive way to manage a router securely, SCP support allows the secure (and authenticated) copying of router configs as well as router images.

**Benefits**

- Enables users to copy config files securely across the network

**Platforms/Considerations**

---

Routers	C1700, C2600, C3620, C3640, C3660, C4500, C7200
---------	---

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Mika Loukola

mika.loukola@cisco.com

#### Secure Terminal-Line Access

##### Description

Cisco IOS Software has had a long-standing feature, called reverse-telnet, where telnetting to a certain port-range connected users to tty lines in various ways (directly, directly 8-bit, rotary, xremote, and so on). Administrators use this to connect a Cisco IOS router with multiple terminal lines to the consoles of other Cisco IOS routers (and other gear). This makes it easy to reach the router console from anywhere, simply by telnetting to the terminal server on a specific line. This helps to configure routers even when all network connectivity to that router is disconnected. Reverse-telnet also allows for modems attached to Cisco IOS routers to be used for dial-out. Generally, a rotary is used in this case.

In either case, people want to be able to access those tty lines securely, especially when configuring a router. Setting up the enable password over the Internet is not a viable solution. A new feature introduced in Cisco IOS Software Release 12.2(2)T, Secure Terminal-line Access, provides this secure functionality.

##### Benefits

- Allows users to access tty lines securely

##### Platforms/Considerations

---

Routers

C1700, C2600, C3620, C3640, C3660, C4500

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Mika Loukola

mika.loukola@cisco.com

#### Ability to Disable Xauth for Static IPSec Peers

##### Description

The Ability to Disable Xauth for Static IPSec Peers feature allows users to disable extended authentication (Xauth), which prevents the routers from being prompted for Xauth information—username and password.

Without the ability to disable Xauth, a user cannot select which peer on the same crypto map should use Xauth. That is, if a user has router-to-router IP security (IPSec) on the same crypto map as a virtual private network (VPN)-client-to-Cisco-IOS IPSec, both peers will be prompted for a username and password. Removing Xauth while configuring the preshared key for router-to-router IPSec, prevents duplicate Xauth information from being exchanged, thereby, reducing traffic on your network.

##### Benefits

If VPN-client-to-Cisco-IOS IPSec and router-to-router IPSec exist on a single interface, the Ability to Disable Xauth for Static IPSec Peers feature allows a user to remove Xauth while configuring the preshared key for router-to-router IPSec. Thus, the router will not prompt the peer for a username and password, which are transmitted when Xauth occurs for VPN-client-to-Cisco-IOS IPSec.

### Platforms/Considerations

Routers	8xx, 16xx, 1600R, 17xx, 25xx, 26xx, 3620, 3640, 3660, 4xxx, 71xx, 72xx, 75xx
Universal Broadband Routers (UBR)	UBR7200, uBR905, uBR925
Access Servers	AS5200

### Marketing Contact

Mika Loukola  
mloukola@cisco.com

### Distinguished Name Based Crypto Maps

#### Description

The Distinguished Name Based Crypto Maps feature allows you to configure the router to restrict access to selected encrypted interfaces for peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Initially, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself, thereby, enabling you to control which encrypted interfaces a peer with a specified DN can access.

#### Benefits

The Distinguished Name Based Crypto Maps feature allows you to set restrictions in the router configuration that prevent peers with specific certificates—especially certificates with particular DNs— access to selected encrypted interfaces.

### Platforms/Considerations

Routers	17xx, 26xx, 3620, 3640, 3660, 71xx, 72xx
Universal Broadband Routers (UBR)	uBR905, uBR925
Access Servers	AS5200

### Marketing Contact

Mika Loukola  
mloukola@cisco.com

### Enhanced Test Command

#### Description

The Enhanced Test Command feature introduces two new commands—aaa user profile and aaa attribute—that allow you to create a named user profile with calling line identification (CLID) or dialed number identification service (DNIS) attribute values, which can be associated with a test aaa group command.

Use the aaa attribute command to add CLID or DNIS attribute values to a user profile, which is created by using the aaa user profile command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the test aaa group command), thereby providing the RADIUS server with access to CLID or DNIS attribute information for all incoming calls.

### Benefits

The Enhanced Test Command feature allows you to add a named user profile with CLID or DNIS attribute values and associate the user profile with the test aaa group command. Thus, the attribute values that are added to the user profile go to the RADIUS server, and the RADIUS server can access CLID or DNIS information when it receives a RADIUS record.

### Platforms/Considerations

---

Routers	64xx, 71xx, 72xx, 75xx, 77xx
Access Servers	AS5300, AS5400, AS5800, AS5850

---

## Inter-Domain Gatekeeper Security Enhancement

### Description

The Inter-Domain Gatekeeper Security Enhancement provides a means of authenticating and authorizing H.323 calls between the administrative domains of Internet Telephone Service Providers (ITSPs).

An interzone ClearToken (IZCT) is generated in the originating gatekeeper when a location request (LRQ) is initiated or an admission confirmation (ACF) is about to be sent for an intrazone call within an ITSP's administrative domain. As the IZCT traverses through the routing path, each gatekeeper stamps the IZCT's destination gatekeeper ID with its own ID. This identifies when the IZCT is being passed over to another ITSP's domain. The IZCT is then sent back to the originating gateway in the location confirmation (LCF) message. The originating gateway passes the IZCT to the terminating gateway in the SETUP message. The terminating gatekeeper forwards the IZCT in the admission request (ARQ) answerCall field to the terminating gatekeeper, which then validates it.

Within the IZCT format, the following information is required:

- srcCarrierID—Source carrier identification
- dstCarrierID—Destination carrier identification
- intCarrierID—Intermediate carrier identification
- srcZone—Source zone
- dstZone—Destination zone
- interzone type
  - INTRA\_DOMAIN\_CISCO
  - INTER\_DOMAIN\_CISCO
  - INTRA\_DOMAIN\_TERM\_NOT\_CISCO
  - INTER\_DOMAIN\_ORIG\_NOT\_CISCO

### Benefits

- Provides security for wholesale providers by supporting authentication and authorization capability for internet telephony calls between foreign other ITSP domains.
- Provides the security functionality necessary for billing and settlement.

### Platforms/Considerations

---

Routers	25xx, 26xx, 36xx, 72xx
Access Servers	AS5300, AS5850

---

## L2TP Security

### Description

The L2TP Security feature provides enhanced security for tunneled PPP frames between the Layer Two Transport Protocol (L2TP) Access Concentrator (LAC) and the L2TP Network Server (LNS). Previous releases of the Cisco IOS provided only a one time, optional mutual authentication during tunnel setup with no authentication of subsequent data packets or control messages. In situations where the L2TP is used to tunnel PPP sessions over an untrusted infrastructure such as the internet, the security attributes of L2TP and PPP are inadequate. PPP provides no protection of the L2TP tunnel, and current PPP encryption protocols provide inadequate key management and no authentication or integrity mechanisms. The L2TP Security feature allows the robust security features of IPSec to protect the L2TP tunnel and the PPP sessions within the tunnel. In addition, the L2TP Security feature provides built in keepalives and standardized interfaces for user authentication and accounting to AAA servers.

The deployment of Microsoft Windows 2000 demands the integration of IPSec with L2TP as this is the default Virtual Private Dialup Network (VPDN) networking scenario. This integration of protocols is also used for local-area network (LAN)-to-LAN VPDN connections in Microsoft Windows 2000. The L2TP Security feature provides integration of IPSec with L2TP in a solution that is scalable to large networks with minimal configuration.

### Benefits

The enhanced security provided by the L2TP Security feature increases the integrity and confidentiality of tunneled PPP sessions within a standardized, well deployed layer 2 tunneling solution. The robust security features of IPSec and Internet Key Exchange (IKE) include confidentiality, integrity checking, replay protection, authentication and key management. Traditional routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP) will run transparently since there is a real PPP interface associated with the secure tunnel. Additional benefits include built in keepalives and standardized interfaces for user authentication and accounting to AAA servers, interface statistics, standardized MIBs, and multi-protocol support.

### Platforms/Considerations

---

Routers

1xxx, 16xx, 17xx, 3620, 3640, 3660, 45xx, 64xx, 71xx, 72xx, 75xx

---

## Marketing Contact

Neil Abogado

nabog@cisco.com

## Offload Server Accounting Enhancement

### Description

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

An offload server interacts with an access server via Virtual Private Network (VPN) to perform required Point-to-Point Protocol (PPP) negotiation for calls. The NAS performs call preauthentication, while the offload server performs user authentication. Thus, this feature allows the authentication and accounting data of the NAS to synchronize with the offload server as follows:

- During preauthentication, the NAS generates a unique session-id, which adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and retrieves a Class attribute. The new session-id is sent in preauthentication requests and resource accounting requests; the Class attribute is sent in resource accounting requests.

- The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted to the offload server via Layer 2 Forwarding (L2F) options.
- The offload server will include the new, unique session-id in user access requests and user session accounting requests. The Class attribute that was passed from the NAS will be included in the user access request, but a new Class attribute will be received in the user access reply; this new Class attribute should be included in user session accounting requests.

#### Benefits

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their NAS and offload server.

Although NASs can already synchronize information with an offload server, this feature extends the functionality to include a unique session-id, which adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and Class (attribute 25) information collected by the NASs.

#### Platforms/Considerations

---

Routers	71xx, 72xx, 75xx, 77xx
---------	------------------------

---

### RADIUS Attribute Screening

#### Description

The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers’ authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

#### Benefits

The RADIUS Attribute Screening feature provides the following benefits:

- Users can configure an accept or reject list consisting of a selection of attributes on the NAS for a specific purpose so unwanted attributes are not accepted and processed.
- Users may wish to configure an accept list that includes only relevant accounting attributes, thereby reducing unnecessary traffic and allowing users to customize their accounting data.

#### Platforms/Considerations

---

Routers	72xx
Access Servers	AS5300, AS5400, AS5800

---

## RADIUS Tunnel Preference for Load Balancing and Fail-Over

### Description

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides load balancing and fail-over home gateway groups in a standardized fashion. This feature introduces new software functionality; no command line configuration is associated with this feature.

Previously, load balancing and fail-over functionality for a Layer 2 Tunnel Protocol network server (LNS) was provided by the Cisco proprietary Vendor Specific Attribute (VSA). In a multivendor network environment, using VSA on a RADIUS server can cause interoperability issues among network access servers (NAS) manufactured by different vendors. Even though some RADIUS server implementations are capable of sending VSAs that the requesting NAS can understand, the user still must maintain different VSAs for the same purpose in a single-service profile.

A consensus regarding the tunnel attributes that are to be used in a multivendor network environment is defined in RFC 2868. In RFC 2868, Tunnel-Server-Endpoint, in conjunction with the Tunnel-Medium-Type, specifies the address to which the NAS should initiate a new session. If multiple Tunnel-Server-Endpoint attributes are defined in one tagged attribute group, they are interpreted as equal-cost load-balancing home gateways (HGWs).

The Tunnel-Preference attribute defined in RFC 2868 can be used as a measure to form load balancing and fail-over HGW groups. When the Tunnel-Preference values of different tagged attribute groups are the same, the Tunnel-Server-Endpoint of those attribute groups are considered to have the same priority unless otherwise specified. When the Tunnel-Preference values of some attribute groups are higher (they have a lower preference) than other attribute groups, their Tunnel-Server-Endpoints will have higher priority values. When an attribute group has a higher priority value, that attribute group will be used for fail-over in case the attribute groups with lower priority values are unavailable for the connections.

Before Cisco IOS Release 12.2(4)T, a specially formatted string would be transported within a Cisco VSA “vpdn:ip-addresses” string to a NAS for the purpose of HGW load balancing and fail-over. For example, 10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 would be interpreted as IP addresses 10.0.0.1, 10.0.0.2, and 10.0.0.3 for the first group for load balancing. New sessions are projected to these three addresses based on the least-load-first algorithm. This algorithm uses its local knowledge to select an HGW that has the least load to initiate the new session. In this example, the addresses 2.0.0.1 and 2.0.0.2 in the second group have a higher value (and therefore a lower priority), and are applicable only when all HGWs specified in the first group fail to respond to the new connection request, thereby making 2.0.0.1 and 2.0.0.2 the fail-over addresses.

The virtual private dialup network (VPDN) authorization library creates authentication, authorization, and accounting (AAA) requests and parses AAA responses. When multiple tunnel attribute sets grouped by different tag values are returned in AAA responses, multiple tunnel information blocks need to be allocated and indexed by the tag value. The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature allows for more than one of these blocks to be returned to the library client. Before Cisco IOS Release 12.2(4)T, only one block would be returned. To preserve the application programming interface (API) and minimize the impact to clients that are using the API, these blocks are organized in a double link list that is invisible to clients. The linkage information is hidden inside the information base at the beginning of the blocks. Clients pass tunnel information blocks around as if there were only one.

Each tunnel information block has a tunnel preference, and the addresses within a given block can also have priorities. A set of rules decides which address takes precedence over another for load balancing and fail-over.

The addresses are sorted using these rules and passed to the VPDN Load Sharing Group (LSG) library. LSG chooses one feasible and least-loaded address based on its local knowledge and returns the address to the VPDN call manager. The VPDN call manager then tries connecting using this address. If the connection succeeds, the VPDN call manager informs LSG to increase the load by one with that address; otherwise, it informs LSG about the failure and LSG marks the address as unavailable for a certain period of time.

#### Benefits

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides industry-standard load-balancing and fail-over functionality for a LNS that previously was provided by the Cisco proprietary Vendor Specific Attribute (VSA). The feature conforms to the tunnel attributes that are to be used in a multivendor network environment as defined in RFC 2868, thereby eliminating interoperability issues among network access servers manufactured by different vendors.

#### Platforms/Considerations

---

Routers	8xx, 16xx, 17xx, 26xx, 3620, 3540, 3660, 6400, 71xx, 72xx, 75xx
---------	---

---

## Voice

### 56K CSU Support for Cisco Signaling Link Terminal (SLT)

#### Description

The Cisco Signaling Link Terminal (SLT) enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 Signaling Link Terminal feature set, providing reliable interoperability with the Cisco Signaling Controller (SC) or the Cisco Virtual Switch Controller (VSC). The SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using the Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports upper-layer SS7 protocols across an IP network to the Cisco SC or Cisco VSC.

The 56K CSU Support for Cisco Signaling Link Terminal (SLT) option adds a new interface to the already rich portfolio of physical SS7 termination choices available to service providers. Specifically, this option provides Cisco SLT support for the WIC-1DSU-56K4 interface card. While the Cisco SLT already provides a V.35 interface using the one or two port high-speed serial interface cards (WIC-1T and WIC-2T), these cards require an external CSU/DSU to interface with digital signaling facilities. The 56K CSU Support for Cisco Signaling Link Terminal option, utilizing the WIC-1DSU-56K4, eliminates the need for external equipment, allowing direct termination if the digital facility on the Cisco SLT.

As with all SS7 interface options on the Cisco SLT, the 56K CSU support option permits fast servicing as Field Replaceable Units (FRUs).

#### Benefits

- Reduces Overall Cost of Cisco SS7-Enabled Solutions—The new 56K CSU Support for Cisco Signaling Link Terminal (SLT) option eliminates the need for external digital facility interface equipment. This saves customers money, lowering the overall solution costs of deploying Cisco SS7 enabled solutions.
- Lowers Central Office (CO) Real Estate Cost to Service Providers—The 56K CSU Support for Cisco Signaling Link Terminal (SLT) option reduces the amount of equipment necessary to deploy Cisco SS7-enabled solutions by eliminating the need for an external CSU/DSU for each SS7 signaling link. This is especially important in installations requiring an optimized footprint where CO rack space is at a premium.
- Simplify Central Office Cable Plant—With the 56K CSU Support for Cisco Signaling Link Terminal (SLT) option, SS7 facilities can terminate directly into the Cisco SLT without the use of an external CSU/DSU. This reduces the cost and complexity of CO wiring plans.

## Platforms/Considerations

---

Routers	C2600
---------	-------

---

### Caveats

- It is important to note that the Cisco SLT supports only the SS7 MTP 2 serial protocol. Therefore, the serial interfaces cannot be configured for other protocols. It is also important to note that the Cisco SLT is not an SS7 over IP router. It can only be used as a part of the Cisco SC or VSC node to backhaul higher layer SS7 protocols over the node's IP signaling control network.

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

George Mather  
gmather@cisco.com

### FXO Answer and Disconnect Supervision

#### Description

The FXO Answer and Disconnect Supervision feature enables analog FXO ports to monitor call progress tones and voice and fax transmissions returned from a PBX or from the PSTN.

Users can configure voice ports to detect either the standard call progress tones that are preconfigured for certain countries, or they can configure custom call progress tone detection. Tone detection is performed by the digital signal processor (DSP) and causes a DSP event to be reported to the host software.

Answer supervision is triggered when the DSP detects voice, modem, or fax transmissions. Answer supervision also allows calls to be timed out after a configurable number of rings. Configuring answer supervision automatically enables disconnect supervision; however, you can configure disconnect supervision separately if answer supervision is not required.

Disconnect supervision can be configured to detect call-progress tones sent by the PBX or PSTN (for example, busy, reorder, out-of-service, number-unavailable), or to detect any tone received (for example, busy tone or dial tone). When an incoming call ends, the DSP detects the associated tone, and the analog FXO voice port goes on-hook. This prevents the voice port from remaining off-hook when no call is in progress.

Users can configure disconnect tones to be detected either continuously during calls or only during call setup (before calls are answered). Detection of any tone operates only during call set-up. If detection of any tone is configured, echo cancellation must be enabled to prevent disconnection due to detection of the router's own ringback tone.

#### Benefits

- Answer supervision allows interoperability with analog PSTN and PBX systems that are incompatible with the answer-supervision and disconnect-supervision features provided by digital trunk interfaces.
- Answer supervision improves the accuracy of billing records by eliminating the reporting of failed calls as having been connected.
- Disconnect supervision allows interoperability with PSTN and PBX systems regardless of their ability to transmit supervisory tones. These functions prevent billing errors that could otherwise result from failure to detect noncompletion or termination of long-distance calls.

## Platforms/Considerations

---

Routers	C1700, C2600, C3620, C3640, C3660
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Mark Maslach  
mmaslach@cisco.com

H.323 Version 2 Phase 2

#### Description

H.323 v2 enhances the H.323 VoIP solution with several new features for improved interoperability with the TDM network. H.323 v2 adds the following new features to H.323 v1:

1. Supplementary Services: H.450.3—Call Deflection, H.450.2 Call Transfer
2. Fast Connect Capability and H.245 Tunneling
3. H.235 Security Enhancements
4. Gatekeeper Transaction Message Protocol

This feature adds H.323v2 enhancements to the Cisco 7200 and Cisco 7500 Series Routers. With these new features, these multiservice routers can function as H.323 voice gateways in several Cisco Solutions such as AVVID and MNET.

#### Benefits

- Adds Fast Connect capability on the Cisco 7200 and the Cisco 7500 Series Routers. With this capability, the time to set-up a call improves significantly, leading to better end-user experience and better network utilization.
- Adds signaling for Supplementary Services such as Call Transfer, Call Deflection, Call Forwarding. This will provide enterprise customers the same features they get from their traditional PBXs.

#### Platforms/Considerations

---

Routers	C2600, C3620, C3640, C3660, C7200, C4GWY
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Harbans Kaur  
harbkaur@cisco.com

MGCP CAS PBX and AAL2 PVC

#### Description

This feature provides termination of CAS signaling from a traditional PBX and transports the signaling in a ATM network using MGCP protocol. The MGC model provides a scalable solution for Service Providers by separating the media gateway and media control into two separate network elements, and provides a standards-based communication between the two.

Voice over AAL2 offers a bandwidth-efficient solution for transporting voice in a packet network. The current solution offers an AAL2 PVC-based solution.

#### Benefits

- Provides a scaleable, standards-based Voice over AAL2 solution to Service Providers
- Provides interworking with the traditional CAS PBXs

## Platforms/Considerations

---

Routers	C1700, C2600, C3620, C3640, C3660
Multiservice Access Concentrator (MC)	MC3810

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Harbans Kaur

harbkaur@cisco.com

SIP Gateway Support for Third Party Call Control

### Description

The SIP Gateway Support for Third Party Call Control allows for the gateway to participate in a SIP session in which a party other than the parties established the session. The implementation of this capability is based upon the current IETF draft 'draft-rosenberg-sip-3pcc-01.txt'.

Third party call control is the ability of one entity to create a call in which the communication exists between parties other than itself. The party that initiates the Third Party Call Control has to know the other parties that it wishes to include in the call and be a conduit of the information flow between the two parties. While the controller of the connection is involved in the signaling that passes between the other parties, the media is passed directly between the parties in the call.

Support of Third Party Call Control on the gateway means that the gateway can support the necessary signaling from a controller that is attempting to establish a call in which the gateway is one of the other parties. The appropriate signaling and media support in the gateway will allow the gateway to participate within the connection.

### Benefits

- Enables enhanced services in a SIP network—Third Party Call Control allows for applications in the SIP network to establish connections as value added services. An example of this is a click-to-dial service.
- Enhanced interoperability with other SIP end points—the Cisco SIP gateway can reside in more feature rich networks making the Cisco SIP gateway more deployable with customers.

## Platforms/Considerations

---

Routers	C2600, C3620, C3640, C3660
---------	----------------------------

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

### Marketing Contact

Steve Levy

stlevy@cisco.com

SLT Dual Ethernet

### Description

The Cisco Signaling Link Terminal (SLT) enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 Signaling Link Terminal feature set, providing reliable interoperability with the Cisco Signaling Controller (SC) or the Cisco Virtual Switch Controller (VSC). The SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using Cisco's Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports upper-layer SS7 protocols across an IP network to the Cisco SC or Cisco VSC.

The SLT Dual Ethernet option allows service providers to now deploy redundant backhaul signaling networks between the Cisco SLT and the Cisco SC2200 or Cisco VSC3000. Redundancy can be on an interface or network level, giving customers multiple options when deploying Cisco SS7 enabled solutions.

#### Benefits

- Reduces Single Points of Failure in Cisco SS7 Enabled Solutions—The new SLT Dual Ethernet feature gives Service Providers the option to build redundancy into their IP backhaul network carrying SS7 signaling between the Cisco SLT and the Cisco SC2200 or Cisco VSC3000. Redundancy can be on an interface or network level, giving customers additional options for reliability when deploying Cisco SS7 enabled solutions.
- Gives Service Providers More Networking Options—While Cisco recommends using the new SLT Dual Ethernet feature, customers can deploy the SLT in single Ethernet configurations where signaling network redundancy is either not needed or economically not feasible.
- Backwards Compatible—Existing customers can upgrade to the latest Cisco IOS Software image for the Cisco SLT without having to immediately deploy the dual Ethernet feature. Service providers can deploy this feature as their schedule permits without having to “flash cut” to a new signaling backhaul network configuration.

#### Platforms/Considerations

---

Routers

C2600

---

#### Caveats

- It is important to note that the Cisco SLT supports only the SS7 MTP 2 serial protocol. Therefore, the serial interfaces cannot be configured for other protocols. It is also important to note that the Cisco SLT is not an SS7 over IP router. It can only be used as a part of the Cisco SC or VSC node to backhaul higher layer SS7 protocols over the node’s IP signaling control network.
- Also note—While the Dual Ethernet option is available on the Cisco SLT in Cisco IOS release 12.2(2)T, it is currently not supported on the Cisco SC2200 or Cisco VSC3000. For availability, please contact the respective product managers for each product.

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

George Mather  
gmather@cisco.com

SLT G.732 Support

#### Description

The Cisco Signaling Link Terminal (SLT) enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 Signaling Link Terminal feature set, providing reliable interoperability with the Cisco Signaling Controller 2200 (SC2200) or the Cisco VSC3000 Virtual Switch Controller (VSC3000). The SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports upper-layer SS7 protocols across an IP network to the Cisco SC2200 or VSC3000.

The SLT G.732 feature adds support for ITU-T G.732 SNMP reporting of excessive bit error ratios detected by the monitoring the frame alignment signal (loss of frame alignment fault conditions), and subsequent alarming actions. ITU-T G.732 is an extract from the ITU-T Blue Book describing characteristics of primary PCM multiplex equipment operating at 2048 kbit/s (E-1).

The SLT G.732 Support feature is available on the following SLT-supported interfaces:

- 1-port E1 multiflex trunk interface (VWIC-1MFT-E1)
- 2-port E1 multiflex trunk interface (VWIC-2MFT-E1)
- 2-port E1 multiflex trunk interface with Drop and Insert (VWIC-2MFT-E1-DI)

#### Benefits

- Improved Alarming Capabilities for Cisco SLT—The SLT G.732 support option adds reporting of excessive bit errors by the monitoring the frame alignment signal on E-1 SS7 interfaces.
- Standards-based Implementation—SLT G.732 alarming can be reported on most SNMP-based management systems.
- Backwards Compatible—Customers can upgrade to the latest version of Cisco IOS Software for the Cisco SLT even if they decide not to use the G.732 alarming feature.

#### Platforms/Considerations

---

Routers	C2600
---------	-------

---

#### Caveats

- It is important to note that the Cisco SLT supports only the SS7 MTP 2 serial protocol. Therefore, the serial interfaces cannot be configured for other protocols. It is also important to note that the Cisco SLT is not an SS7 over IP router. It can only be used as a part of the Cisco SC or VSC node to backhaul higher layer SS7 protocols over the node's IP signaling control network.

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

George Mather  
gmather@cisco.com

Voice over ATM with AAL2 Trunking

#### Description

With the support of this feature, the Cisco 7200 series routers can now support three different mechanisms for transporting Voice in an ATM network, AAL2, AAL1, and AAL5. Voice over AAL2 provides customers with a standards based mechanism for transporting voice traffic over ATM networks. ATM allows packetized data to be integrated with packetized voice in a low latency, high QoS-capable manner. AAL2 is a bandwidth efficient ATM mechanism for transporting multiple compressed voice calls in one ATM VC, thus reducing the cell tax. This feature supports compressed and uncompressed modes as well as numerous voice features such as Call Admission Control, Voice Activity Detection, Silence Suppression, Fax detection, and modem detection. This feature is for Permanent Virtual Circuits (PVC), and does not provide switching based on a call agent. (Call switching using SVCs and external call agent is supported in the phase 2 of this project.)

#### Benefits

- Provides bandwidth efficient trunking between PBXs for Enterprise Customers, or between End Office switches for service providers
- Enables support of the Cisco Velocity Solution for Integrated Access for voice and data
- Supports voice compression using a variety of codecs—G.729, G.711, G.726
- Supports modem and fax passthru

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact

Harbans Kaur

harbkaur@cisco.com

Cisco H.323 Scalability and Interoperability Enhancements

Description

The Cisco H.323 Scalability and Interoperability Enhancements feature upgrades the Cisco H.323 Gatekeeper (GK) and Cisco H.323 Gateway to comply with H.323 Version 3. The enhancements in this release include:

- Support for mandatory H.323 Version 3 elements in the gateway and GK, including:
  - multipleCalls—This field is set to TRUE in all H.225 messages for TCP calls.
  - maintainConnection— If the call-idle timer is set to a nonzero value, this field is set to TRUE in all H.225 messages for TCP calls. Otherwise, it is set to FALSE.
  - alternateTransportAddresses—This structure contains the keyword annexE and the transport address of an alternate Annex E.
  - useSpecifiedTransport—This field is marked as annexE. It is accompanied by the alternateTransportAddresses structure which specifies the Annex E transport address.
- Support for H.225 call signalling over UDP. H.225 messages can be transported over TCP or UDP (as described in Annex E). At registration time, a Cisco H.323 Gateway indicates to the GK whether it is capable of transmitting over both TCP and UDP. If it is, the Cisco H.323 Gateway registers both its TCP and UDP addresses.
- Address resolution using border elements (BE). The BE (as described in Annex G) is colocated with the Cisco H.323 Gatekeeper and provides additional address resolution capabilities. The BE can cache address information from neighboring BEs. When the GK receives a call that it cannot resolve, it can contact its local BE. If the address is in the BE’s cache, the BE on the GK sends an AccessRequest to the BE in the terminating domain. If the address is not in the BE’s cache, then the BE attempts to resolve the address by sending an AccessRequest to each of its neighboring BEs.

Table 1 Address Resolution Using Border Elements

Elements	Action
Gateway A to gatekeeper D/Border Element D	Gateway A sends an ARQ to gatekeeper D/border element D.
Gatekeeper D/border element D to border element B	Gatekeeper D/border element D is a noncaching BE and it cannot resolve the address internally. Therefore, border element D sends an AccessRequest to border element B.
Border element B to border element F/ gatekeeper F	Border element B searches its cache to for the closest match and locates a descriptor that indicates that the access request should be sent to border element F/gatekeeper F.
Border element F/gatekeeper F to border element D	Border element F/gatekeeper F returns an access confirmation to border element D. The access confirmation contains a template with a single address indicating where the SETUP message should be sent.
Gatekeeper D/border element D to gateway A	Gatekeeper D/border element D sends an ACF to gateway A.
Gateway A to gateway F	Gateway A sends a SETUP message to gateway F.

- Support for bandwidth request (BRQ) messages. The Cisco H.323 Gateway requests the maximum bandwidth required to establish a call when it requests call admission using the admission request (ARQ) message. If the Codec type used for the established call requires less bandwidth than that allocated, the Cisco H.323 Gateway reports the lesser amount using the BRQ message. This BRQ message reports the actual bandwidth being utilized by the call. The bandwidth reported in the BRQ overrides the value previously reported in the ARQ message.
- Support for concurrent calls over a single H.225 call signalling channel. The call signalling channel is capable of carrying signalling for many concurrent calls. It uses the call reference value to associate a message with the call. H.323 endpoints indicate whether they are capable of handling multiple calls by setting a flag in the H.225 messages. If endpoint is unable to process any new calls on a given TCP connection, it can request a new connection by rejecting the SETUP message with a ReleaseComplete message with the cause code set to NewConnectionNeeded. The originating endpoint then establishes a new TCP connection and continues with the call setup. Cisco gateways have been enhanced to establish a new connection if a third-party endpoint requests one.

The commands in this feature module are documented in the “Command Reference” section. Table 2 lists the new and changed commands and the function to which they apply.

Table 2 Functions and Commands

Function	Commands
Annex G BE configuration	<ul style="list-style-type: none"> <li>• h323-annexg</li> <li>• call-router</li> <li>• local</li> <li>• neighbor</li> <li>• port</li> <li>• id</li> <li>•query-interval</li> <li>• cache</li> <li>• advertise</li> <li>• ttl</li> <li>• hopcount</li> <li>• timer</li> <li>• prefix</li> </ul>
BE management	<ul style="list-style-type: none"> <li>• clear call-router routes</li> <li>• shutdown</li> </ul>
H.225 timeout	<ul style="list-style-type: none"> <li>• h225 timeout tcp call-idle</li> <li>• h225 timeout setup</li> </ul>
H.323	<ul style="list-style-type: none"> <li>• h323</li> <li>• session transport</li> </ul>
Bandwidth management	<ul style="list-style-type: none"> <li>• emulate</li> </ul>
Verifying configuration	<ul style="list-style-type: none"> <li>• show call active</li> <li>• show call history</li> <li>• show call-router routes</li> <li>• show call-router status</li> </ul>
Call start procedures	<ul style="list-style-type: none"> <li>• call start</li> </ul>

### Benefits

- Implementation of the mandatory elements ensures that Cisco H.323 Gateways and GKs are compatible with other H.323 Version 3 components.
- Transmission of H.225 messages is independent of the transport layer (TCP or UDP).
- More efficient use of bandwidth using the BRQ message.
- Reduced call setup and call clearing times and increased call capacity through the use of concurrent calls over the call signalling channel.
- Call routing by GK using Annex G Interdomain Address Resolution Protocol.

### Platforms/Considerations

#### GK functions:

Routers	25xx, 26xx, 36xx, 72xx
Multiservice Access Concentrator	MC3810

#### Gateway functions:

Routers	17xx, 26xx, 36xx, 72xx
Universal Broadband Routers (UBR)	uBR9xx, uBR924

### Location Confirmation (LCF) Enhancements for Alternate Endpoints

#### Description

The LCF Enhancements for Alternate Endpoints feature allows a Cisco IOS Gatekeeper (GK) to collect additional routes to endpoints that are indicated by multiple LCF responses from remote GKs, and convey a collection of those routes to the requesting (calling) endpoint. Currently, the originating GK sends Location Request (LRQ) messages to multiple remote zones. Remote GKs in the zones return LCF responses to the originating GK. The LCF responses indicate alternate routes to the remote GK's endpoints. The consolidation of LCF responses to multiple LRQs can provide many alternate routes to reach a given destination. An endpoint can have up to 20 alternate endpoints.

The remote GK zones have been configured in the originating GK using the zone remote command, specifying the cost and priority to each remote zone. After receiving the LCF responses, the originating GK determines the best route to an endpoint based on the cost and priority of remote zones returning the responses. The originating GK then forwards route information to the requesting endpoint in the admission confirmation (ACF) message, which contains an ordered list of alternate endpoints.

The LCF Enhancements for Alternate Endpoints feature allows the originating GK to discover and relay more possible terminating endpoints to the requesting endpoint, therefore providing alternate routes to endpoints that can be used if the best route is busy or does not provide any alternate routes. The endpoint receiving the list of alternate endpoints tries to reach them in the order in which the alternate endpoints were received. The LCF Enhancements for Alternate Endpoints feature can be used on GKs that originate LRQs and directory GKs that forward LRQ messages.

The LCF Enhancements for Alternate Endpoints feature allows you to choose the number of alternate routes you want the GK to collect during the existing LRQ timer window. When the timer expires or the best response is received and sufficient alternates are received, the resolved address and alternate endpoints from all the LCFs received by the GK are consolidated in a single list. The address and endpoints are sent as alternate endpoints in the Admission Confirmation (ACF) or LCF messages from the GK. If this feature is not enabled, the GK stops collecting routes after the LRQ timer expires, then chooses the best LCF and sends it in the ACF message. After you enable the feature, the GK stops collecting routes after the LRQ timer expires, then consolidates the endpoints from all LCF messages received.

**Benefits**

- Provides additional alternate routes to endpoints obtained from LCFs
- Allows the Cisco IOS Gateways (GWs) to attempt to connect a call using all available routes in situations where the more preferred route is temporarily unavailable

**Platforms/Considerations**

Routers	25xx, 26xx, 36xx, 72xx
Multiservice Access Concentrator	MC3810

MGCP 1.0 with NCS 1.0 and TGCP 1.0 Profiles

**Description**

This feature implements the following MGCP protocols on the supported Cisco media gateways:

- MGCP 1.0 (RFC2705)
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs)

Specific feature support within these protocols is summarized in Table 3. Terms in the table are defined as follows:

- VoIP—includes signaling methods under Voice over IP.
- AAL2 PVC—includes signaling methods under Asynchronous Transfer Mode (ATM) Adaptation Layer 2 (AAL2) Permanent Virtual Circuit (PVC).
- Basic/Extended RGW—a collection of residential gateway features supporting channel-associated signaling (CAS). Digital CAS (E&M) interfaces and analog (FXO, FXS, and E&M) interfaces are supported on platforms with the appropriate voice hardware.
- ISUP—supports ISDN user part signaling for SS7 trunks.
- FGD-OS—supports Feature Group D Operator Services signaling over T1 or E1 trunks.
- Incoming CAS—for digital incoming MF CAS wink-start trunks in which an operator at an Operator Services Console can initiate the Operator Interrupt and Busy Line Verify (OI/BLV) functions. These features are supported on digital CAS interfaces.
- CAS PBX—includes CAS PBX trunks, digit maps, CAS events, and quarantine buffer software. These features are supported on digital CAS interfaces.

Table 3 Feature Support by Platform

		VoIP		AAL2 PVC
		MGCP 1.0	TGCP1.0	MGCP 1.0
Cisco CVA122 and Cisco CVA122E	Basic/Extended RGW			Basic/Extended RGW
Cisco uBR925	Basic/Extended RGW			Basic/Extended RGW
Cisco 2600 series and Cisco 2650	Basic/Extended RGW			
Cisco 3660	ISUP, FGD-OS, Incoming CAS	ISUP, FGD-OS, Incoming CAS		
Cisco MC3810	Basic/Extended RGW, CAS-PBX			Basic/Extended RGW, CAS-PBX

### Feature Definition

Media Gateway Control Protocol (MGCP) 1.0 is a protocol for the control of Voice over IP (VoIP) calls by external call-control elements known as media gateway controllers (MGCs) or call agents (CAs). It is described in the informational RFC2705, published by the Internet Society.

PacketCable is an industry-wide initiative to develop interoperability standards for multimedia services over cable facilities using packet technology. PacketCable developed the NCS and TGCP protocols, which contain extensions and modifications to MGCP while preserving basic MGCP architecture and constructs. NCS is designed for use with analog, single-line user equipment on residential gateways, while TGCP is intended for use in VoIP-to-PSTN trunking gateways in a cable environment. To meet European cable requirements and equipment characteristics, the EuroPacketCable working group has adapted PacketCable standards under the name *IP Cablecom*.

### MGCP Model

MGCP bases its call control and intelligence in centralized *call agents*, also called media gateway controllers. The call agents issue commands to simple, low-cost endpoints, which are housed in media gateways (MGs), and they also receive event reports from the gateways. MGCP messages between call agents and media gateways are sent over IP/UDP.

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature provides protocols for residential gateways (RGWs) and trunking gateways (TGWs), which sit at the border of the packet network to provide an interface between traditional, circuit-based voice services and the packet network. Residential gateways offer a small number of analog line interfaces, while trunking gateways generally manage a large number of digital trunk circuits.

Two basic MGCP constructs are *endpoints* and *connections*. An endpoint is a source or sink for call data (RTP/IP) that is flowing through the gateway. A common type of endpoint is found at the physical interface between the POTS or PSTN service and the gateway; this type of endpoint might be an analog voice port or a digital DS0 group. There are other types of endpoints as well, and some are logical rather than physical. An endpoint is identified by a two-part endpoint name that contains the name of the entity on which it exists (for example, an access server or router) and the local name by which it is known (for example, a port identifier).

A connection is a temporary allocation of resources that enables a call to be completed. One or more connections is necessary to complete a call. Connections have names that identify them with the call to which they belong. Connections can be one-to-one or multipoint. Calls and connections are initiated, modified, and deleted on instructions from call agents.

Call agents manage call flow through standard MGCP *commands* that are sent to the endpoints under their control. The commands are delivered in standard ASCII text, and may contain session descriptions transmitted in Session Description Protocol (SDP), a text-based protocol. These messages are sent over IP/UDP.

Call agents keep track of endpoint and connection status through the gateway's reporting of standard events that are detected from endpoints and connections. Call agents also direct gateways to apply certain standard signals when a POTS/PSTN connection expects them. For example, when someone picks up a telephone handset, an off-hook event is detected on an endpoint on the residential gateway to which the telephone is connected. The gateway reports the event to a call agent, which orders the gateway to apply the dial-tone signal to the endpoint reporting the off-hook event. The person picking up the handset hears dial tone.

Related events and signals are grouped into standard packages that apply to particular types of endpoints. For instance, the off-hook event is found in the line package, which is associated with analog-line endpoints, which in turn are associated with residential gateways. Standard events, signals, and packages are defined in the NCS, TGCP, and MGCP standards and RFCs listed in the "Supported Standards, MIBs, and RFCs" section.

#### Benefits

- MGCP 1.0 provides flexible interoperability with a wide variety of call agents, thus enabling a wide range of solutions.
- MGCP 1.0 contains many improvements over its previous release (MGCP 0.1).
- NCS 1.0 and TGCP 1.0 allow participation in packet cable solutions.
- The ability to interoperate with H.323 and SIP control agents allows leverage of the feature sets available in the different protocols, and provides the ability to migrate smoothly from one protocol to another.

#### Platforms/Considerations

Routers	26xx, 3660
Universal Broadband Routers (UBR)	UBR925
Multiservice Access Concentrator	MC3810
CVA	CVA122, CVA122E

### PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

#### Description

The *PRI Backhaul Using the Simple Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer* feature fulfills the need for a standards based PRI Signaling backhaul that works with third party Call Agents to enable solutions like Integrated Access, IP PBX, and Telecommuter.

This feature provides the following:

- PRI Backhaul—Specific implementation for backhauling PRI.
- SCTP—New general transport protocol that can be used for backhauling signaling messages.
- IUA—Mechanism for backhauling any Layer 3 protocol that normally uses Q.921.

These features do the following:

- Provide a configuration interface for Cisco IOS software implementation.
- Implement the protocol message flows for SCTP and IUA.

#### Benefits

#### Third-Party Interoperability

This feature supports interoperability with third-party Call Agents.

### Solutions Enabling

This feature supports the following solutions, which require signaling backhaul functionality:

- IP PBX
- IP Centrex
- Enterprise Toll Bypass
- IXC/Tandem Bypass

### Platforms/Considerations

---

Routers

3660

---

### PSTN Fallback

#### Description

The PSTN Fallback feature monitors congestion in the IP network and redirects calls to the PSTN or rejects calls on the basis of network congestion. The fallback subsystem has a network traffic cache that maintains the Calculated Planning Impairment Factor (ICPIF) or delay/loss values for various destinations. Performance is improved because each new call to a well-known destination does not have to wait on a probe to be admitted and the value is usually cached from a previous call.

The ICPIF calculates an impairment factor for every piece of equipment along the voice path, and then adds them up to get the total impairment value. Refer to International Telecommunication Union (ITU) standard G.113 for more information. The ITU assigns a value to the types of impairments, such as noise, delay, and echo.

The ICPIF method of determining the impairment value was introduced for compatibility with Cisco H.323 applications. Part of ICPIF includes a concept of Total Impairment Value that is a function of loss of packets, delay of packets, and codecs used based on the round-trip reports from Service Assurance Agent (SAA).

SAA is a network congestion analysis mechanism that provides delay, jitter, and packet loss information for the configured IP addresses. SAA is based on a client-server protocol defined on the User Datagram Protocol (UDP). The UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. The SAA probe packets go out on randomly selected ports from the top end of the audio UDP port range.

The information that the SAA probes gather is used to calculate the ICPIF or delay/loss values that are stored in a fallback cache where they remain until the cache ages out or overflows. Until an entry ages out, probes are sent periodically for that particular destination. This time interval is user configurable.

With this release, you can also configure codes that indicate the cause of the network rejection; for example, packets that are lost or that take too long to be transmitted. A default cause code of 49 displays the message “Quality of Service Unavailable.”

#### Benefits

With this release, the PSTN Fallback feature and enhancements provide the following benefits:

- Automatically routes a call to an alternate destination when the data network is congested at the time of the call setup.
- Enables the service provider to give a reasonable guarantee about the quality of the conversation to their Voice over IP (VoIP) users at the time of call admission.
- Provides delay, jitter, and packet loss information for the configured IP addresses.
- Caches call values from previous calls. New calls do not have to wait for probe results before they are admitted.

- Enables a user-configurable cause code display indicating the type of call rejection.

#### Platforms/Considerations

Routers	26xx, 36xx, 72xx, 75xx
Multiservice Access Concentrator	MC3810

### Sequential LRQ Enhancement

#### Description

The Sequential LRQ Enhancement feature enhances the existing sequential LRQ feature in the Cisco IOS Gatekeeper (GK) to provide a potentially faster LRQ response to the originator of the request when a location reject (LRJ) response is received while the GK is sending sequential LRQs. In the current sequential LRQ implementation on the GK, the GK sends an LRQ to the next zone only after the sequential delay timer expires. The Sequential LRQ Enhancement feature introduces a fixed delay for the GK to send sequential LRQs to successive zones even when a negative response or an LRJ is received from the current zone. You configure this fixed delay using the `lrq lrj immediate-advance` command. If an LRJ is received from the current zone, the GK assumes that the current zone cannot satisfy the request and immediately sends an LRQ to the next zone. This feature works for both typical and directory GKs. For more information on directory GKs, see the `lrq forward-queries` command section in the *Cisco IOS Voice, Video, and Fax Command Reference*, Cisco IOS Release 12.2.

#### Benefits

This feature provides faster LRQ responses to originators by allowing the GK to send LRQs to sequential zones before the sequential delay timer expires, if an LRJ or negative response is received

#### Platforms/Considerations

Routers	25xx, 26xx, 36xx, 72xx
Multiservice Access Concentrator	MC3810

## WAN Services

### ADSL Over ISDN

#### Description

ADSL uses the local loop to provide high speed access by using parts of the frequency spectrum available on a typical local loop to provide high speed “last mile” access, while still allowing for base band services such as analog telephone to run on the same loop simultaneously.

For this purpose ADSL splits up the 1.1 MHz frequency range into 256 bins that occupy 4 KHz of bandwidth each. For traditional ADSL, as defined in ITU G.992.1 Annex A or ANSI T1.413, this means that the first bin is used for voice, and ADSL uses the bins from approximately 40 KHz and up.

This feature utilizes hardware and software feature to allow ISDN to exist as the base band service, provide more bandwidth for ISDN services, and enable ADSL to use the bins from about 140 KHz and higher. This feature is delivered according to the ETSI 101-388 standard with the intention to extend this functionality to supporting ITU G.992.1 Annex B via a software upgrade.

There is a special model Cisco 826 router that supports this feature.

#### Benefits

- ADSL support for countries with high density of ISDN deployed: Nordic countries, Germany and Belgium.

- Interoperability with Alcatel ASAM ADSL over ISDN DSLAMs
- Business class ADSL solution for ADSL over ISDN

Platforms/Considerations

---

Routers

C820

---

First appearance in a Cisco IOS Software release: 12.1(3)XG (special release) and 12.2(2)T.

Marketing Contact

Geir Leirvik  
geir@cisco.com

DHCP Option 82 Support for Routed Bridged Encapsulation

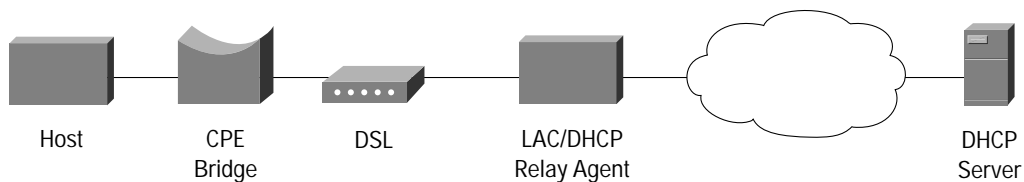
Description

Sub-option fields of “DHCP Relay Agent Information Option” (option 82) can be used to pass information about the Physical port, on DHCP relay agent, through which the DHCP requests are coming in.

As a trusted box inserts this information, that information could be used as the key by policy management scripts running on the DHCP server to control IP address assignment and to implement any other policies. Such policies can include not allowing more than X number of IP addresses to a given physical port on LAC.

So, this feature is about RBE providing that Physical port information to DHCP relay agent, which in turn would insert that into “DHCP Relay Agent Information Option”, while forwarding the DHCP request to server.

Figure 4 Topology of RBE deployment, with DHCP to assign IP addresses.



Benefits

- Enforces policy-based IP addresses assignment
- Provides security against DHCP IP exhaustion attacks from remote hosts

Platforms/Considerations

---

Routers

C3640, C7200, C7500

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

Marketing Contact

Murali K. Kolli  
mkolli@cisco.com

X.25 Annex G Session Status Change Reporting

Description

In current Cisco IOS Software there is no convenient way to detect and notify of any failed Annex G sessions.

This feature provides a solution to detect such failures and two different ways of notification in case of failures.

Detecting a failed Annex G. link using LAPB T4 timer (idle timer) associated with each DLCI solves this problem. During the PVC establishment, each PVC registers to LAPB with information including interface name and the corresponding DLCI number. When this timer expires, LAPB considers the link down and starts to send out SABMs. The Cisco 2600 will then send out a message containing: interface name, DLCI number, time/date information and up/down state. This message will be sent to the console as well as syslog.

#### Benefits

- Customers are notified of failed Annex G sessions immediately
- Users receive diagnostic information that allows them to investigate the cause of the Annex G session failure

#### Platforms/Considerations

---

Routers

C2600, C3640, C3660, C4500, C7200

---

First appearance in a Cisco IOS Software release: 12.2(2)T.

#### Marketing Contact

Murali Kolli

mkolli@cisco.com

Adaptive Frame Relay Traffic Shaping for Interface Congestion

#### Description

The Adaptive Frame Relay Traffic Shaping for Interface Congestion feature enhances Frame Relay traffic shaping functionality by adjusting permanent virtual circuit (PVC) sending rates based on interface congestion. When this new feature is enabled, the traffic-shaping mechanism monitors interface congestion. When the congestion level exceeds a configured value called queue depth, the sending rate of all PVCs is reduced to the minimum committed information rate (minCIR). As soon as interface congestion drops below the queue depth, the traffic-shaping mechanism changes the sending rate of the PVCs back to the committed information rate (CIR). This process guarantees the minCIR for PVCs when there is interface congestion.

This new feature works in conjunction with backward explicit congestion notification (BECN) and Foresight functionality. If interface congestion exceeds the queue depth when adaptive shaping for interface congestion is enabled along with BECN or ForeSight, then the PVC sending rate is reduced to the minCIR. When interface congestion drops below the queue depth, then the sending rate is adjusted in response to BECN or ForeSight.

Before the introduction of this feature, interface congestion caused packets to be delayed or dropped at the interface. The Adaptive Frame Relay Traffic Shaping for Interface Congestion feature helps ensure that packet drop occurs at the virtual circuit (VC) queues. When used with FRF.12 fragmentation, this feature also ensures that packets are dropped before fragmentation occurs.

#### Benefits

The Adaptive Frame Relay Traffic Shaping for Interface Congestion feature:

- Guarantees minCIR for PVCs when there is interface congestion, as long as the sum of the minCIR values for the PVCs is less than the usable interface bandwidth.
- Increases the useful data rate by ensuring that packets are dropped before FRF.12 fragmentation.
- Enables intelligent packet drop by ensuring that packets are dropped at the VC queue rather than the interface.

## Platforms/Considerations

---

Routers	25xx, 26xx, 36xx, 4xxx, 45xx, 72xx, 75xx
---------	--

---

### Cisco Modem User Interface Option

#### Description

The Cisco Modem User Interface feature enables Cisco routers to behave like a modem and be configured using standard Hayes modem commands.

With the Cisco Modem User Interface feature, a point of sale (POS) terminal, such as those used by gasoline service stations to charge customers for merchandise and services, can use high-speed Internet connections rather than slow-speed telephone connections to transfer data.

The user interface to the higher speed connection will not change when the Cisco Modem User Interface feature is used; the user interface will still appear as if the connection on the POS terminal is through a modem and a telephone line.

Although there are a wide variety of proprietary extensions to the Hayes modem commands, the Cisco Modem User Interface feature supports only a subset of the commands. This basic functionality is enhanced with Cisco-specific modem register settings, Telnet connection capability, and dial-related Cisco IOS commands.

#### Benefits

The Cisco Modem User Interface feature allows Cisco routers to replace modems, and thereby update a slow telephone call-modem negotiation process with a high-speed Internet connection. Together, these features provide the following benefits:

- Reduced costs, because modems are no longer necessary.
- Increased connection speeds, because Internet connections are faster than modem connections.

## Platforms/Considerations

---

Routers	17xx, 26xx, 3xxx
---------	------------------

---

### Frame Relay 64-Bit Counters

#### Description

The Frame Relay 64-Bit Counters feature provides 64-bit counter support on Frame Relay interfaces and subinterfaces. This feature enables the gathering of statistics through Simple Network Management Protocol (SNMP) for faster interfaces operating at OC-3, OC-12, and OC-48 speeds.

The following counters are supported by this feature: Bytes In, Bytes Out, Packets In and Packets Out.

The show frame-relay pvc command has been modified to display the 64-bit counters.

#### Benefits

The values in 32-bit counters sometime wrap because the field is too small. Wrapping causes the values in these fields to become meaningless. 64-bit counters support the reliable gathering of statistics by SNMP by preventing the wrapping of counter values.

## Platforms/Considerations

---

Routers	72xx, 75xx
---------	------------

---

### Leased/Switched BRI Interfaces for ETSI NET3

#### Description

In most BRI configurations, both B channels of a leased-line service are used as point-to-point leased lines with the D channel disabled. Data transmission over the B channels is no different than data transmission over point-to-point leased lines.

A new feature available in Cisco IOS Release 12.2(4)T, Leased and Switched BRI Interfaces for ETSI NET3, allows one BRI B channel on a European Telecommunications Standards Institute (ETSI) NET3 switch to be configured as a leased line, and the second B channel to be configured as a standard ISDN or dial interface and used as a switched channel to the Public Switched Telephone Network (PSTN). When the Leased and Switched BRI Interfaces for ETSI NET3 feature is configured, one B channel functions as a point-to-point 64-kbps leased line and the other B channel functions as a circuit-switched channel using the D channel to provide the signaling features available for the ETSI NET3 signaling protocol.

#### Benefits

The Leased and Switched BRI Interfaces for ETSI NET3 feature allows Internet service providers to split one ISDN line into a leased-line interface and a dialer interface, thereby increasing connection capability without increasing cost.

## Platforms/Considerations

---

Routers	8xx
---------	-----

---

### VPDN Group Session Limiting

#### Description

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of Virtual Private Dial Network (VPDN) sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group Session Limiting feature, you can limit the number of Layer Two Forwarding Protocol (L2F) or Layer Two Transport Protocol (L2TP) VPDN sessions allowed for each VPDN group. This feature is implemented with the introduction of the session-limit *number* command in VPDN group configuration mode. Session limiting for VPDN groups is applied after global VPDN session limiting (which is configured with the vpdn session-limit *session* command in global configuration mode) is enforced.

#### Benefits

The VPDN Group Session Limiting feature gives more control to network administrators by enabling them to limit how many sessions a VPDN group can terminate. This feature enables service providers to cater to all types of organizations, large or small, by enabling finer configuration granularity.

## Platforms/Considerations

---

Routers	1xxx, 14xx, 16xx, 17xx, 25xx, 26xx, 29xx, 35xx, 3620, 3640, 3660, 38xx, 4xxx, 45xx, 62xx, 64xx, 71xx, 72xx, 75xx, 1xxxx
---------	---

---



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
www-europe.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney  
NSW 2060 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia  
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru  
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa  
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R) 201734/ETMG 10/01