Cisco IOS Software Release 12.2 Features & Hardware

Last Updated: February 2004

Cisco IOS Software Release 12.2 Introduction

Cisco IOS® Software is the world's leading networking software, delivering a seamless integration of technology innovation, business-critical services and hardware support. This product bulletin announces the General Deployment certification of Cisco IOS Software Major Release 12.2.

Cisco IOS® Software Major Release 12.2 achieved General Deployment certification in February 2004. With this certification, Major Release 12.2 recognizes a new level of maturity to the already robust portfolio of Cisco IOS Software releases. The releases in this portfolio, including Release 12.2, Release 12.3, and Release 12.3T, each address specific customer needs.

- Major Release 12.2 (First Commercial Shipment [FCS]: April 2001) consolidates the features, functionality, and hardware support introduced in Release 12.1T. Now General Deployment-certified, this release reflects the maturity of extensive deployment in diverse customer networks.
- Major Release 12.3 (FCS: May 2003) is the latest example of how Cisco software delivers benefits through innovation and integration. It is a consolidated release designed for Enterprise, Access, and Cisco channel partners. It delivers innovative, optimized features that enable easy access to Voice, Security, and Quality of Service (QoS), and the leading-edge functionality and platform support introduced in Cisco IOS Software Release 12.2T.
- Cisco is issuing the Release 12.3T family as a series of individual releases, each of which create significant revenue opportunities and include hundreds of new business-critical features, powerful new hardware support, and ongoing quality improvements.

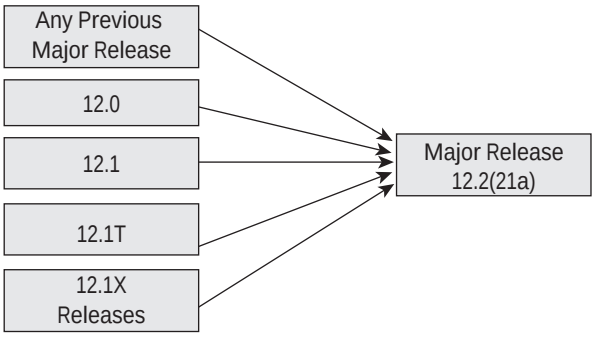
Highlights of Major Release 12.2 include Quality of Service, Multiprotocol Label Switching, Traffic Classification, and Multimedia advancements, in addition to the introduction of the Cisco 2600XM Series Router. This release will integrate the functionality and platform support previously introduced in Cisco IOS Software Releases 12.1 and 12.1T.

Cisco IOS Software Release 12.2(21a) is the FCS of Release 12.2 General Deployment and includes support for the Cisco 2600, 3600, 7200, and 7500 Series Routers.

Migration Guide

The following Cisco IOS Software releases identify the current recommended migration into General Deployment-certified releases in the Release 12.2 family:

Figure 1



Feature Matrix

Connectivity and Scalability	Hardware	IBM Support	IP and Routing
Asynchronous Rotary Line Queuing *12.1(1)T*	Cisco 3660 Router *12.1(1)T*	TN3270 Server Connectivity Enhancements *12.1(5)T*	DHCP Relay Support for Unnumbered Interfaces *12.1(2)T*
ISDN Network Side for ETSI Net5 PRI *12.1(1)T*	MC3810-V3 and MC3810-HCM6/ MC3810-HCM2 *12.1(2)T*		DHCP Server Import Capability *12.1(2)T*
Cable Interface Bundling *12.1(1)T*	Virtual Private Network (VPN) Module for the Cisco 1700 Series Routers *12.1(2)T*		DHCP Client *12.1(2)T*
Point-to-Point Wireless Support for the Cisco uBR7200 Series *12.1(1)T*	OC-3/STM-1 ATM Circuit Emulation Services (CES) Network Modules for the Cisco 3600 Multiservice Access Routers *12.1(2)T*		NAT—Support for PPTP in an Overload (Port Address Translation) Configuration *12.1(2)T*
FR/ATM Service Interworking (FRF.8) *12.1(2)T*	DS3 and E3 ATM Network Modules for the Cisco 2600 and 3600 Multiservice Access Routers *12.1(2)T*		DHCP Server—Easy IP Phase 2 *12.1(3)T*
FR/ATM Network Interworking (FRF.5) *12.1(2)T*	Virtual Private Network (VPN) Modules for the Cisco 2600 and 3600 Series Routers *12.1(3) XI(1)*		HSRP Support for MPLS VPNs *12.1(3)T*
AAA Server Group Deadtimer *12.1(2)T*	1 Port Enhanced ESCON Channel Port Adapter *12.1(5)T*		MPLS Traffic Engineering Enhancements *12.1(3)T*
Network Side PRI Signaling, Trunking, and Switching *12.1(3)T*	AS58-324UPC-CC *12.1(3)T*		AutoInstall Using DHCP for LAN Interfaces *12.1(5)T*
NTT PRI NFAS *12.1(3)T*	TDM Potent: MIX-enabled 2/4/8 Port Multichannel T1/E1 Port Adapter with CSU/DSU *12.1(5)T*		NAT—Support of IP Phone to Cisco CallManager *12.1(5)T*
PPP over ATM SVC's *12.1(3)T*	Catalyst 4000 Access Gateway Module *12.1(5)T*		NAT—Support of H.323 v2 Call Signaling (FastConnect) *12.1(5)T*

Connectivity and Scalability	Hardware	IBM Support	IP and Routing
TCP Clear Performance Optimization *12.1(3)T*	Cisco 2600/3600 10/100 Ethernet/ Token Ring Mixed Media NMs *12.1(1)T*		NAT—Support for NetMeeting Directory (Internet Locator Service-ILS) *12.1(5)T*
General Packet Radio Service (GPRS) *12.1(3) T*	ICS 7750 Multiservice Route Processor 200 *12.1(3)XI*		Trace Route Enhancement for MPLS *12.1(5)T*
Distributed FRF.11/.12 *12.1(5)T*			MPLS Scalability Enhancement for LSC and ATM LSR *12.1(5)T*

LAN Support and WAN Services	Management	Multimedia	Quality of Service
Frame Relay Switching Enhancements: Shaping and Policing *12.1(2)T*	Service Assurance Agent Enhancements *12.1(1)T*	Bidirectional PIM *12.1(2)T*	Express Resource Transport Protocol and TCP Header Compression (CRTP) *12.1(1)T*
	Virtual Switch Interface Master MIB *12.1(3)T*	Source Specific Multicast (SSM) *12.1(3)T*	COPS for RSVP *12.1(1)T*
	MSDP MIB *12.1(5)T*	IGMP Version 3 *12.1(5)T*	DOCSIS 1.0+ Quality-of-Service Enhancements *12.1(1)T*
	Trace Route Support in a MPLS Network *12.1(5)T*	PIM Dense Mode State Refresh *12.1(5)T*	DOCSIS 1.0+ (UBR924) *12.1(1)T*
	NTP MIB *12.1(5)T*	Router-Port Group Management Protocol (RGMP) *12.1(5)T*	Class-Based Shaping *12.1(3)T*
	Interface Index Persistence *12.1(5)T*	Multimedia Conference Manager with Voice Gateway image with RSVP to ATM SVC *12.1(5)T*	Class-Based Marking *12.1(3)T*
	Monitoring Resource Availability on Cisco AS5x00 Universal Access Servers *12.1(5)T*		Distributed Low Latency Queuing *12.1(5)T*
			Distributed Traffic Shaping *12.0(4)XE*
			Network-Based Application Recognition (NBAR) *12.1(5)T*
			RSVP Support for Frame Relay *12.1(5)T*
			Class Based Policer for the DiffServ AF PHB *12.1(5)T*
			Class Based QoS MIB *12.1(5)T*
			DiffServ Compliant WRED *12.1(5)T*

LAN Support and WAN Services	Management	Multimedia	Quality of Service
			Distributed cRTP *12.1(5)T*
			QoS Device Manager *12.1(1)E*

Reliability	Security	Switching	Voice
PGM Host *12.1(1)T*	SSH Version 1 Server Support *12.1(1)T*	Media Gateway Control Protocol for the Cisco AS 5300 Voice/Gateway *12.1(1)T*	Cisco Signaling Link Terminal (SLT) *12.1(1)T*
Cisco 7500 Single Line Card Reload *12.1(5)T*	Preauthentication *12.1(2)T*		Settlements for Packet Voice, Phase 2 *12.1(1)T*
	Preauthentication with ISDN PRI and Channel Associated Signaling *12.1(3)T*		H.323 Version 2 Support Phase 2 *12.1(1)T*
	Secure Shell Version 1 Integrated Client *12.1(3)T*		Voice over ATM on Cisco 3600 Routers *12.1(2)T*
			Voice over Frame Relay Using FRF.11 and FRF.12 *12.1(2)T*
			QSIG Protocol Support on Cisco MC3810, 7200, 2600, and 3600 Series Routers *12.1(2)T*
			Voice over IP on Cisco MC3810 *12.1(2)T*
			Voice over ATM with AAL2 Trunking *12.1(2)T*
			Caller ID on 2600, 3600 and MC3810 *12.1(3)T*
			Media Gateway Control Protocol Residential Gateway Support *12.1(3)T*
			Modem PassThrough over Voice over IP *12.1(3)T*
			Interworking Signaling Enhancements for H.323 and SIP VoIP *12.1(3)T*
			Hoot'n Holler over IP *12.1(3)T*
			Dial Peer Enhancements for Cisco AS5800 Access Server H.323 VoIP Gateways *12.1(3)T*
			Support for Cisco CallManager *12.1(3)T*

Reliability	Security	Switching	Voice
			PSTN Fallback *12.1(3)T*
			Advanced Voice Busyout Monitor (AVBO) *12.1(3)T*
			Trunk Conditioning for FRF.11 and Cisco Trunks *12.1(3)T*
			Fax Relay Packet Loss Concealment *12.1(3)T*
			Interactive Voice Response Version 2.0 on Cisco VoIP Gateways *12.1(3)T*
			Link Fragmentation and Interleaving (LFI) for Frame Relay and ATM Virtual Circuits *12.1(5)T*
			T.37/T.38 Fax Gateway *12.1(5)T*
			Enhanced Voice Services for Japan for Cisco 800 Series Routers, Cisco 813 *12.1(5)T*
			ISDN Progress Indicator Support for SIP Using 183 Session Progress *12.1(3)XI*

VPN	WAN Optimization	WAN Services	Wireless
Inter-Autonomous System for MPLS VPNs *12.1(5)T*	Frame Relay Fragmentation with Hardware Compression *12.1(5)T*	CUG Selection Facility Suppress Option *12.1(5)T*	MICA PIAFS *12.1(3)T*
	PPP Over Fast Ethernet 802.1Q *12.1(5)T*	Frame Relay Switching Diagnostics and Troubleshooting *12.1(5)T*	GSM Enhanced Full Rate Codec (EFR) *12.1(5)T*
	CEF Switching for Routed Bridge Encapsulation *12.1(5)T*	PPPoE RADIUS Port Identification *12.1(5)T*	

Connectivity and Scalability

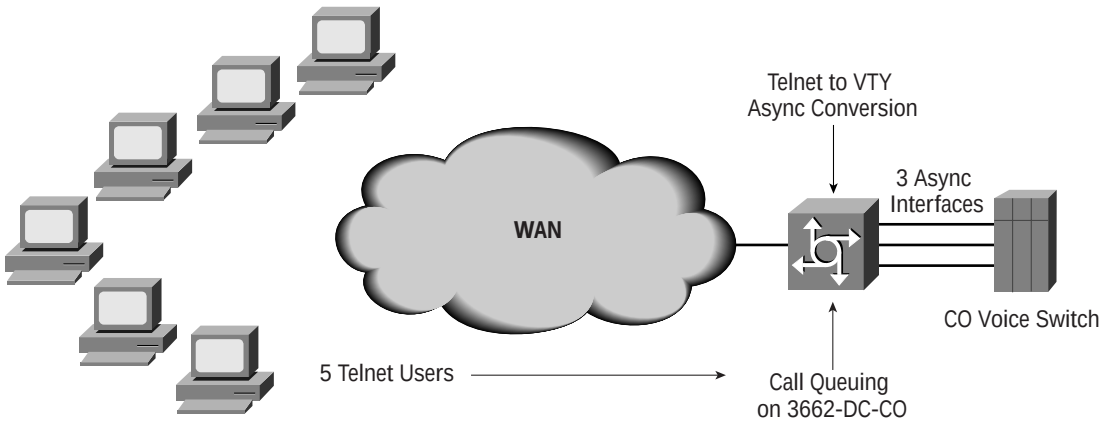
Asynchronous Rotary Line Queuing

Description

Asynchronous Rotary Line Queuing solves problems that most telcos face when users vie for the same voice switch craft port resources within the telcos management network TMN's Data Communication Network (DCN). Voice switches such as the DMS have asynchronous management interface ports that need to be accessed by multiple engineers from various data centers in the network. Typically, there are three to four async ports but seven to eight users may contend for them at the same time.

Until now, telcos typically used a device from Infotron, a small niche player in the United Kingdom. This device allows rotary access to these ports. Users who tried to access these ports after initial ports were busy were put into a queue to wait for a free port. In other words, they couldn't get cleared because of busy ports; they were suspended and had to wait in queue. Asynchronous Rotary Line Queuing solves this issue for central offices.

Figure 2
Asynchronous Rotary Line Queuing



Benefits

- Telcos don't have to implement small black box solutions that lower overall operating costs
- Telcos can implement one platform, such as the 3662-DC-CO or 2600 class platforms for DCN connectivity

Platforms/Considerations

Routers	All Cisco IOS routers

First appearance in a Cisco IOS Software "T" release: 12.1(1)T

ISDN Network Side for ETSI Net5 PRI

Description

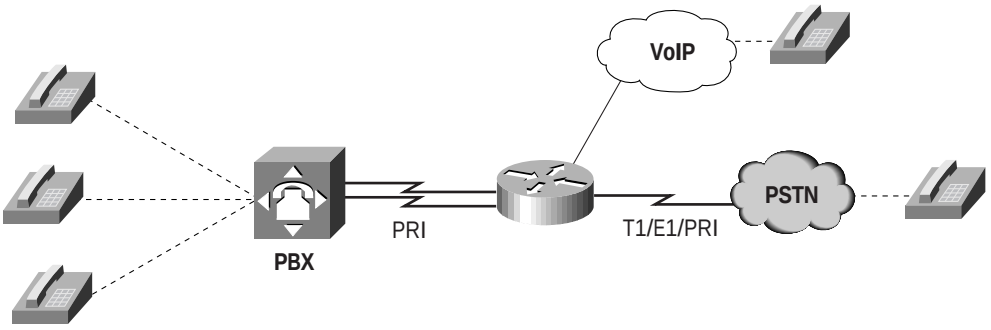
The ISDN Network-Side PRI for ETSI NET5 feature enables Cisco IOS Software to replicate the public switched network interface to a PBX that is compatible with ETSI NET5.

Routers and PBXs are both traditionally CPE with respect to the public switched network interfaces. For voice over IP (VoIP) applications, it is desirable to interface routers to PBX's with the router representing the public switched network.

Enterprise organizations use the VoIP feature with Cisco products as a method to reduce long-distance costs for phone calls within and outside of their organizations. However, sometimes a call cannot be placed over VoIP, and the call needs to be placed using the PSTN. The customer then needs two devices connected to a PBX to allow some calls to be placed using VoIP and some calls to be placed over the PSTN.

The ISDN Network-Side PRI will allow Cisco ISDN-enabled routers to switch calls across interfaces as legacy phone switches do today and mimic the behavior of the legacy phone switches. As shown in Figure 3, when a call arrives at the router, it is either passed to VoIP or terminated on the router.

Figure 3
ISDN Network Side PRI



Benefits

- For Voice-over-IP applications, a customer PBX may be directly connected to a Cisco router rather than to the PSTN so that PBX station calls may be automatically routed to the IP network
- Bypassing the PSTN tariffed services, such as trunks and administration, increases cost savings when using Voice-over-IP in the network

Platforms/Considerations

Routers	2600, 3620, 3640, 3660, 4500, 7200, 7500
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software “T” release: 12.1(1)T

Cable Interface Bundling

Description

Interface bundling aids in the distribution of IP addressing across RF line cards in a single UBR7200 chassis without adding the disadvantages of a bridged CMTS. Current software consumes an IP subnet for each RF line card, while lessening IP subnet consumption is considered critical for several customers. A solution to reduce the number of subnets consumed per UBR7200 is therefore required. Cable interface bundling allows a service provider to share one IP subnet across multiple cable interfaces that are grouped into a cable interface bundle. This eliminates the need to designate a separate IP subnet for each individual cable interface. This in turn avoids the performance, memory, and security problems that would result if a bridging solution were used to manage the subnets, especially for a large number of subscribers.

Interface bundling allows the conservation of IP subnets, while retaining its routing functionality between cable interfaces and to the egress port. Routed networks provide:

- *Security*—access to applications can be filtered and bandwidth limited based on Layer-3 attributes.
- *Stability*—broadcast and other network anomalies can be isolated to a single subnet.
- *Scalability*—IP addresses have a structure that is mapped onto the network topology. Layer 2 (bridged) networks have no such structure; therefore, each bridge must know every MAC address on the network; eventually network size will be limited by the size of the MAC address forwarding tables in the bridges.

Please access additional information on cable interface bundling at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xr/bundling.htm

Benefits

- Offers IP address conservation with the routing capabilities of the CMTS, thereby eliminating the bridged CMTS competitors' argument that a routed CMTS complicates IP addressing issues
- Simplifies IP addressing across multiple modem cards in the UBR7200 chassis

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	UBR7200

First appearance in a Cisco IOS Software "T" release: 12.1(1)T.

Point-to-Point Wireless Support for the Cisco uBR7200 Series

Description

Point-to-point wireless is defined as a fixed dedicated wireless link from one site to another.

Broadband wireless is a system that delivers tens of megabits of data, using microwave or millimeter-wave radio technology.

This product delivers 44-Mbps full-duplex point-to-point (PTP) fixed-site data in a 12-MHz RF channel in the MMDS band (2.500 to 2.690 GHz) and the U-NII band (5.725 to 5.825 GHz). Future phases will deliver lower data rates in other frequency bands.

The PTP wireless router is be an integrated solution, which will consist of a base router (Cisco universal broadband router 7246), a wireless modem line card, an RF head unit, a power-feed panel, cables, and antenna subsystems. This PTP wireless router will be deployed in a service provider's "network cloud" environment, as well as in enterprise campus locations. Thus, the target customers for the PTP wireless router will be both the service provider channel and the enterprise end user.

The PTP wireless router system will be positioned as another option in the broadband access portfolio of Cisco solutions. Currently, these solutions consist of Digital Subscriber Lines (DSL) and cable technologies.

The PTP link is a "last-mile-access" link to reach local customers. It is not targeted for a "long-haul" or "backbone" application. The distinction is in the performance requirements normally assigned to a "last-mile" link in a telecommunications network. Of course this does not prevent it from being used in a "backbone" or "backhaul" application when the performance meets specified needs.

Benefits

- The first broadband wireless solution to provide high speed wireless connections in obstructed environments
- Cisco IOS integrated router solution, seamless interconnect between the wireless path and other router connections; manage one network
- Fiber quality performance, 10^-11 bit-error-rate (BER) performance for data, 10^-8 for voice plus forward error correction (FEC) and automatic repeat request (ARQ) capability
- Software modem: configurable radio settings through remote interface
- Full simple network management protocol (SNMP) support with on-board diagnostics and path monitoring

Platforms/Considerations

Universal Broadband Router	Cisco 7246, 7223

First appearance in a Cisco IOS Software release: 12.1(1)T.

FR/ATM Service Interworking (FRF.8)

Description

Frame Relay (FR)/ATM service interworking (IW) is a technique to allow communication between a Frame Relay end user and an ATM end user. The technique is based upon the FRF.8 (Frame Relay Forum) Implementation Agreement (IA). FRF.8 specifies that a Frame Relay end station may communicate with an ATM end station provided that there is a router that is performing FRF.8 in software between the two end stations. FRF.8 essentially allows protocol translation of Frame Relay traffic to ATM traffic. It is for permanent virtual circuit (PVC)-based networks only and requires a one-to-one mapping of FR PVCs to ATM PVCs.

Benefits

- Allows communication between a FR end station and an ATM end station
- Based upon the FRF.8 standard.
- Requires a one-to-one mapping of FR PVCs to ATM PVCs

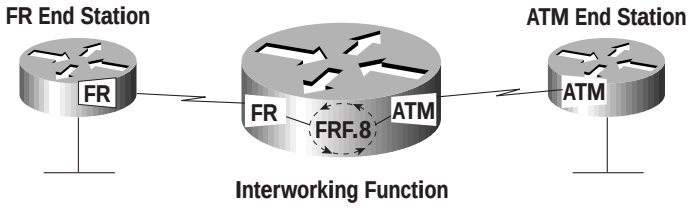
Platforms/Considerations

Routers	Cisco 26xx, Cisco 36xx
Multiservice Access Concentrator (MC)	Cisco MC3810

First appearance in a Cisco IOS Software release: 12.1(2)T.

Figure 4

FR/ATM Service Interworking (FRF.8)



- **Allows a FR end station to communicate with an ATM end stationn**
- **PVC only**
- **Requires one-to-one mapping between FR PVC and ATM PVC**

FR/ATM Network Interworking (FRF.5)

Description

FR/ATM IW is a technique to allow transport of Frame Relay traffic through an ATM network. The technique is based upon the FRF.5 implementation agreement specifies that two Frame Relay end stations may communicate with each other through an ATM network between the end stations. This works provided that there are routers at each side of the end stations that are performing FRF.5 in software between the FR and ATM ports. FRF.5 essentially allows tunneling of Frame Relay traffic through an ATM network. It is for based networks only and allows multiple FR PVCs to be multiplexed onto a single ATM PVC.

Benefits

- Allows communication between FR end stations through an ATM network
- Based upon the FRF.5 standard
- Allows multiple FR PVCs to be multiplexed onto a single ATM PVC

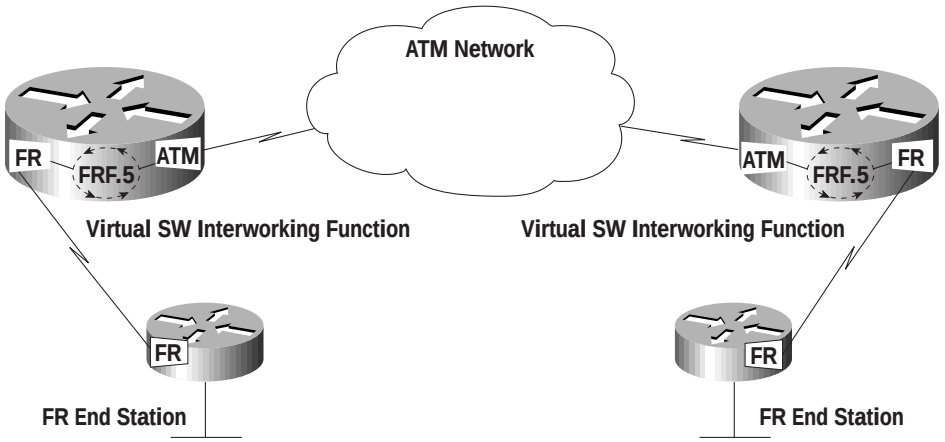
Platforms/Considerations

Routers	Cisco 26xx, Cisco 36xx
Multiservice Access Concentrator (MC)	Cisco MC3810

First appearance in a Cisco IOS Software release: 12.1(2)T.

Figure 5

FR/ATM Network Interworking (FRF.5)



- **Allows two FR end stations to communicate over an ATM network**
- **PVC only**
- **Multiple FR PVC's can be mapped to a single ATM PVC**

AAA Server Group Deadtimer

Description

In previous Cisco IOS Software releases, a limited configuration may be applied to a AAA server group that includes the list of AAA servers in the server group. The AAA Server Group feature allows users to select a subset of servers from a global host list and use the server group for a particular service. The currently supported server host types are RADIUS and TACACS+ server hosts.

A global configuration sets the deadtime in minutes when to stop waiting for a non-responding server.

With the AAA Server Group Deadtimer feature the deadtime configuration will be configured per server group. The deadtime attribute is supported only for RADIUS hosts. If the deadtime is defined globally, the local server group deadtime configuration will override the global configuration.

Benefits

- Before the introduction of the AAA Server Group Deadtimer feature, the server deadtime attribute could be configured only as a unique, global attribute in Cisco IOS AAA.
- This feature allows you to fully configure a server in the server group. And it allows you to configure each dead server timer per server group. Thus, you are no longer limited to a global configuration when configuring a server group.

Platforms/Considerations

Routers	Cisco 2600, 36xx, 38xx, 4x00, and 7x00
Access Servers (AS)	Cisco 5300, 5400, and 5800

First appearance in a Cisco IOS Software release: 12.1(2)T.

Network Side PRI Signaling, Trunking, and Switching

Description

The Network side PRI Signaling, Trunking, and Switching feature enables Cisco IOS Software to replicate the public switched network interface to a PBX. Network Side PRI enables the NAS to provide a standard ISDN PRI network-side interface to the PBXs and mimic the behavior of legacy phone switches. To a PBX, the NAS functions as a National ISDN PRI switch type or an ETSI PRI Net5 switch. No change in PBX capability or behavior is required.

Call switching using dial peers enables Cisco (voice-over-IP) VoIP gateways to switch voice and data calls between different interfaces based on the dial peer matching. An incoming call is matched against configured dial peers, and based on the configured called number, the outgoing interface is selected. Any call that arrives from an ISDN PRI network side on a supported platform is either terminated on the NAS, switched to an IP network, or switched to the PSTN, depending on the configuration. A dial peer is an addressable call endpoint identified, for example, by a phone number or a port number. In VoIP, there are two kinds of dial peers: POTS and VoIP. The Cisco AS5800 access server switches both voice and data calls. The Cisco AS5300 access server switches only voice calls.

The Trunk Group Resource Manager (TGRM) supports the logical grouping, configuration, and joint management of one or more PRI interfaces. The TGRM is used to store configuration information and to accept or select an interface from a trunk group when requested. A trunk group is provisioned as the target of a dial peer, and the TGRM transparently selects the specific PRI interface and channels to use for incoming or outgoing calls. A trunk group can include any number of PRI interfaces, but all the interfaces in a trunk group must use the same type of signaling.

The Class of Restrictions (COR) functionality provides the ability to deny certain call attempts based on the incoming and outgoing class of restrictions provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, to 900 numbers), and applies different restrictions to call attempts from different originators. COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call.

In Cisco IOS Software Release 12.1(2)XH, the trunking and COR parts of this feature are available only on the Cisco AS5800. The remainder of the feature is platform independent.

Benefits

- The Network Side PRI Signaling, Switching, and Trunking feature allows you to bypass PSTN tariffed services such as trunking and administration, extending the cost savings of VoIP.
- It allows your PBXs to be connected directly to a Cisco NAS, so PBX station calls can be routed automatically to the IP network without the need for special IP telephones.
- It provides flexibility in network design.
- It also enables you to block calls selectively based on the called number or the calling number.

Platforms/Considerations

Routers	C2600, C36xx, C4x00, C7x00,
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

NTT PRI NFAS

Description

NTT PRI NFAS adds the NTT switch type to the existing ISDN PRI NFAS with D Channel Backup feature.

ISDN Non-Facility Associated Signaling (NFAS) allows multiple ISDN Primary Rate Interfaces (PRIs) to be controlled by a single D channel. The NTT switch type for NFAS does not use an associated D channel for backup.

Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

Benefits

- Addition of the NTT switch type makes NFAS available in geographic areas where NTT switches are available.
- Use of a single D channel to control multiple PRI interfaces can free one B channel on each interface to carry other traffic.

Platforms/Considerations

Routers	C36xx, C4x00, C7x00
Access Servers (AS)	5300, 7200

First appearance in a Cisco IOS Software Release: 12.1(3)T.

PPP over ATM SVC's

Description

As DSL deployments scale to beyond the trial stage of <1000 customers to upwards of millions of customers, efficiencies must be brought about in the provisioning of the service. Currently, DSL service has been standardized on PPP over ATM. In provisioning a customer, PVC's are "nailed up" between the subscriber and the Network Access Provider (NAP) or, in some cases, all the way to the Network Service Provider (NSP). The cost of provisioning these subscribers with PVC's, even as GUI based provisioning alternatives are developed, are untenable from the service provider's (esp. NAP) viewpoint. Enabling service providers with PPP over ATM SVC's will reduce this cost as well as enhance the manageability of DSL services.

Support for PPP over ATM SVC's will also help NAP's provide services to end-users by providing a method of destination selection as well as QoS selection. Based upon the invoked address, a VC will be set up that sets up a PPP session for a particular level of bandwidth and service (VBR, UBR etc.) as well as to the particular network of interest (e.g. ISP1, ISP2, Corp1, Corp2). With telecommuting and home networking becoming more prolific, support for multiple destinations will become a standard requirement.

From an end-to-end perspective, the Cisco DSL product line is able to leverage PPP over ATM SVC's from either the NAP or the NSP perspective. While, the CPE and DSLAM will have very little to offer, the aggregation device in the NAP and the termination and service delivery device in the NSP (either the Cisco 6400 or 7200 series in both cases) will need to have SVC functionality. On the client side, Microsoft is building SVC capability into Windows 98 an extending it in Win2000 (includes ILMI support). With this feature, Cisco leads the market in enabling end-to-end SVC's. At the SVC termination point, layer 2 service selection of this type can then lead to layer 3 selection at the NSP (provided for by Vulcan/SSG functionality in the Cisco 6400).

Benefits

- PVC's no longer need to be "nailed up" between the subscriber and the Network Access Provider (NAP)
- Network Scaling-Ease of management with no PVC definitions SVC's allocate resources more dynamically
- Can reduce network operating costs.
- Help's the NAP's provide services to end-users by providing a method of destination selection as well as QoS selection.
- Window 98 and Win2000 compatible

Platforms/Considerations

Routers	Cisco 3600, 6400, 7200 and 7500

First appearance in a Cisco IOS Software release: 12.1(3)T.

TCP Clear Performance Optimization

Description

The feature provides inbound and outbound performance optimization for service providers who provide ports to America Online (AOL) using the Cisco AS5800. This feature enables an AS5800 to support 1344 (2 x T3) clear-channel Telnet sessions, otherwise known as "TCP-Clear". Each TCP-Clear session carries data for a single AOL user.

Outbound TCP-Clear traffic handling is now event-driven and processed at interrupt level. In addition, the flow control algorithm is enhanced to handle the higher volume of traffic and to eliminate some out-of-resource conditions that could result in abnormal termination of the session.

Inbound TCP-Clear traffic has the same optimizations as outbound, and scanning for special characters is also eliminated. This scanning is required on a normal Telnet session to process Telnet control sequences but is CPU intensive. In TCP-Clear, no Telnet control sequences are ever sent. In addition, a Nagle algorithm is used to form the inbound data stream into larger packets, minimizing packet-processing overhead.

Benefits

- Wholesale dial service providers with AS5800s can now run handle AOL user loads to 100 percent of system capacity
- Each TCP-Clear/AOL session requires far less CPU thereby leaving more processing capability for other traffic types running on the same system
- Any mixture of PPP/AOL traffic can be handled by the AS5800

Platforms/Considerations

Access Servers (AS)	AS5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

General Packet Radio Service (GPRS)

Description

General Packet Radio Service (GPRS) is defined and standardized by the European standards body ETSI. GPRS is a packet-based (IP/X.25) data service for GSM networks. The GPRS network essentially consists of two major elements, the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).

Cisco GGSN is the gateway to IP-based network and services, whether it is the public Internet or a corporate intranet. The GGSN provides authenticated access for a mobile subscriber for resources in the IP domain, whether it is to connect to a corporate network or an ISP, for data services such as e-mail, Web browsing, or other Internet-based applications. Cisco GGSN is a software solution on standard Cisco IOS router platform. Thus, the Cisco GGSN leverages all the benefits of Cisco IOS technology such as support for routing protocols and features such as DHCP, NAT, VPN, IPSec., and so on.

Benefits

- Fewer routers required to support the same number of areas-this feature makes it possible for one Cisco router to support multiple Level 1 areas, as opposed to the single Level 1 area previously supported by each router
- Network scaling-because a single Cisco router is capable of supporting up to 29 Level 1 areas plus one Level 2 area, expansion of networks using multi-area IS-IS routing is simpler
- Connectivity for local Level 1 areas on the same router-this feature also provides connectivity between Level 1 areas local to the router, previously, Level 1 areas could be connected only by using the Level 2 backbone

Platforms/Considerations

Platforms supported are 7200 VXR, 75xx, and 36XX platforms will be supported in subsequent releases.

First appearance in a Cisco IOS Software “T” release: 12.1(3)T

Distributed FRF.11/.12

Description

FRF.11 provides a standards-base voice transport, and FRF.12 provides a standards-based data fragmentation mechanism over Frame Relay. When voice and data frames are interleaved in a Frame Relay network using low-speed links or low CIR values, fragmentation of large data frames becomes necessary to avoid excessive delays experienced by real-time traffic such as voice.

Distributed FRF.11/12 provides the above functionality for the VIP on the Cisco 7500 series router. This feature moves the voice encapsulation and the data fragmentation function into the distributed CEF path in the VIPs, increasing the overall performance and scalability of the system. This occurs by offloading the central processor from the memory and computing intensive tasks such as fragmentation and reassembly of data frames, as well as voice encapsulation. Another important advantage of confining the handling of voice and data packets to the VIP is the reduced latency by shortening the processing path inside the system

With Distributed FRF11/12 feature, the Cisco 7500 series router becomes a strong play in the multiservice and voice aggregation solution space.

Benefits

- Provides a standards-based solution for transporting voice over Frame Relay and data fragmentation in a Frame Relay network

- Improves voice quality for voice over Frame Relay, by reducing end-to-end delay
- Provides investment protection to the Cisco 7500 customers interested in migrating from TDM network to packet networks

Platforms/Considerations

Routers	7500 series routers with VIP 2-50 and higher

First appearance in a Cisco IOS Software release: 12.1(5)T.

Hardware

Cisco 3660 Router

Description

- All network modules on the Cisco 2600/3600 family are now supported on the Cisco 3660 with Cisco IOS Software Release 12.0(07)XK.
- NEW—E1 high density voice
- NEW—Fast Ethernet mixed media (NM-1FE2W, NM-2FE2W, NM-1FE1R2W, NM-2W)
- Digital and analog modems for dial access
- Channelized T1/E1/PRI
- ATM-25
- VIC-2BRI
- WIC-2A/S
- WIC-2T
- See the following URL for additional details and updated documentation on all above items: www.cisco.com/go/3600

Benefits

With the added support of all the existing 2600/3600 network modules, VICs and WICs, the Cisco 3660 offers customers a greater feature set on a higher availability, higher-density, and higher-performance platform

With the introduction of the new E1 digital voice network module, and support for QSIG signaling, advanced PBX connectivity options are now available on the Cisco 2600/3600 product family

With the introduction of the new mixed media Fast Ethernet network modules, customers have greater flexibility in their LAN/WAN connectivity options

Platforms/Considerations

Routers	C26xx, C3620, C3640, C3660

First appearance in a Cisco IOS Software “T” release: 12.1(1)T.

MC3810-V3 and MC3810-HCM6/MC3810-HCM2

Description

- The 12.1(2)T release is the first early deployment (ED) release which supports the next generation MC3810, the MC3810-V3 and it's accompanying next generation voice compression module, the MC3810-HCM6 or MC3810-HCM2.
- The MC3810-V3 introduces a higher performance processor that insures high quality, high-density voice over packet technologies. The MC3810-V3 includes 64MB of SDRAM and 32MB of Flash for long-term investment protection.
- The MC3810-HCM (High performance Compression Module) provides greater voice call density for the MC3810 series and may be used on either the MC3810-V3 or the classic MC3810-V. There are two models for the MC3810-HCM, the HCM2, which supports a maximum of 8 voice channels and the HCM6 with supports up to 24 channels. With a single MC3810-HCM6, the MC3810-V3 supports up to 24 channels of G.729a, G.711 voice or fax. Likewise, the MC3810-V or V3 supports 12 channels of G.723.1 or G.726.

Benefits

- Improved investment protection with latest technology of processing, digital signal processor and memory headroom.
- Robust architecture for support of existing and emerging voice networking technologies.
- Backward compatibility for voice compression hardware means that installed base customers benefit from the newest in voice technology without a major disruption to their network.

Platforms/Considerations

Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(2)T.

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

Description

The VPN module handles VPN security by implementing IP Security (IPsec)—an industry-wide standard for assuring the privacy, integrity, and authenticity of information crossing public IP networks. The VPN module, which fits in a slot inside the Cisco 1720 or 1750 chassis, encrypts data using Digital Encryption Standard (DES) and 3DES algorithms at speeds suitable for a single full-duplex T1/E1 serial connection (4 megabits per second for 1514-byte packets). The module together with the platform supports as many as 100 IPsec tunnels (400 security associations) for concurrent sessions with mobile users or other sites.

The Cisco 1700 series together with the VPN module and IOS Firewall Feature Sets is the perfect IPsec VPN solution for connecting small offices to other remote offices, mobile users, central-office intranets, or partner extranets.

Benefits

- Enables the secure use of public switched networks and the Internet for wide area networking
- Increases overall encryption performance over software encryption methods
- Significantly reduces the system costs, management complexity, and deployment effort over multiple box solutions
- Enables deployment of VPNs to up to 100 mobile users or sites

- Reserves critical processing resources for other services such as routing, firewall, and voice

Platforms/Considerations

Routers	Cisco 17x0

First appearance in a Cisco IOS Software release: 12.1(2)T.

OC-3/STM-1 ATM Circuit Emulation Services (CES) Network Modules for the Cisco 3600 Multiservice Access Routers

Description

Three new single-port OC-3/STM-1 ATM Circuit Emulation Services (CES) network modules for the Cisco 3600 series provide ATM Forum-compliant CES. All three ATM network modules support STS-3c and STM-1 framing standards over multimode, single-mode intermediate reach, or single-mode long reach fiber-optic interfaces. Up to two T1 or E1 trunk ports are available for private branch exchange (PBX) or video-initiated traffic using the multiflex voice/WAN interface cards (VWICs). These ATM CES network modules provide a cost-effective solution that can be deployed as service-provider customer premises equipment (CPE) for consolidating multiservice data, voice, and video services over a single ATM link.

Based on the ATM Forum Circuit Emulation specification, the Cisco 3600 CES capability provides both structured and unstructured CES for transparent channel associated signaling (CAS) and common channel signaling (CCS) support. The OC-3/STM-1 network modules provide constant bit-rate (CBR) capabilities for voice and video applications that require guaranteed bandwidth across the ATM network. Integrated echo-cancellation features can also be enabled for up to 30 DS0s in a single T1 or E1 trunk.

Benefits

- Multimode, singlemode intermediate reach and single-mode long reach fiber support
- ATM Forum Standards ATM Adaption layer 1 (AAL1) and AAL5
- ATM Forum Traffic Management with User-Network Interface (UNI) 3.0, 3.1, and 4.0
- Support for all multiflex VWICs, with the exception of the 1- and 2-port G.703 drop-and-insert VWICs
- Integrated echo cancellation with configurable parameters for voice transport beyond the metropolitan area
- Support for either 1- or 2-port T1/E1 PBX trunk or video coder/decoder (codec) connections
- Multiple clocking modes, including global, synchronous residual time stamp (SRTS), and adaptive clocking

Platforms/Considerations

Routers	Cisco 3620, 3640, and 3660

First appearance in a Cisco IOS Software release: 12.1(2)T.

DS3 and E3 ATM Network Modules for the Cisco 2600 and 3600 Multiservice Access Routers

Description

Two new single-port DS3 and E3 ATM network modules are now available for the Cisco 2600 and 3600 multiservice access routers. Both versions provide a single ATM connection of either 44 Mbps for DS3, or 34 Mbps for E3 using 75-ohm BNC connectors. Both the DS3 and E3 ATM network modules support ATM Forum-compliant framing standard AAL5. ATM traffic management classes include Unspecified Bit Rate (UBR), UBR+, Variable bit rate-realtime (VBR-rt), VBR non-realtime (VBR-nrt), available bit rate (ABR), and CBR.

The DS3 and E3 ATM network modules complete the ATM family of interfaces that include the ATM25, 4-and 8-port ATM with inverse multiplexing over ATM (IMA), and OC-3/STM-1 network modules. These DS3/E3 ATM network modules provide a cost-effective solution that can be deployed as service-provider CPE or enterprise branch offices for consolidating multiservice data, voice and video services over a single ATM link.

Benefits

- Support for ATM classes of service: UBR, UBR+, VBR-rt, VBR-nrt, ABR, and CBR (data only)
- ATM UNI 3.0, 3.1, and 4.0 traffic management
- RFC 1483 and 1577 support
- 1024 simultaneous virtual connections-(virtual path identifier [VPI] range 0-256, virtual channel identifier [VCI] range 0-1024)
- Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs)
- Physical layer convergence procedure (PLCP) and header error control (HEC) cell delineation support
- Operations and management (F5 Operation Administration and Maintenance [OAM]) cell support
- LAN Emulation (LANE) 2.0
- Integrated Local Management Interface (ILMI) 1.0
- Internet Engineering Task Force (IE TF) Point-to-Point Protocol ([PPP] over ATM)
- IP-to-ATM class-of-service (CoS) mapping feature
- Multiprotocol Label Switching/virtual private network (MPLS/VPN)
- Multiprotocol over ATM (MPOA) Client and Server
- Next Hop Resolution Protocol (NHRP)
- Online insertion and removal (OIR) on Cisco 3660
- Permanent Virtual Path (PVP) support
- ATM Bandwidth (Resource) Manager

Platforms/Considerations

Routers	Cisco 26xx, 3620, 3640, and 3660

First appearance in a Cisco IOS Software release: 12.1(2)T.

Virtual Private Network (VPN) Modules for the Cisco 2600 and 3600 Series Routers

Description

The VPN Modules handle VPN security by implementing IP Security (IPsec)-an industry-wide standard for assuring the privacy, integrity, and authenticity of information crossing public IP networks. The AIM-VPN/BP module fits in the AIM slot on any 2600 Series Router, the NM-VPN/MP fits in any NM slot on the 3620 or 3640 Series Router, and the AIM-VPN/HP fits in the AIM slot on the 3660 Series Router. These 3 Modules encrypt data using Digital Encryption Standard (DES) and 3DES algorithms at speeds 10 times the performance of software-only encryption. The modules, together with the platform, support as many as 300 IPsec tunnels on the 2600 and as many as 2000 IPsec tunnels on the 3660 for site-to-site or mobile user VPNs.

The Cisco 2600 and 3600 Series Routers, together with the VPN module and Cisco IOS Firewall Feature Sets, are the perfect IPsec VPN solution for connecting branch offices to central offices, mobile users, central-office intranets, or partner extranets.

Benefits

- Enables the secure use of public switched networks and the Internet for wide area networking VPNs.
- Increases overall encryption performance over software encryption methods
- Significantly reduces the system costs, management complexity, and deployment effort over multiple box VPN solutions
- Enables deployment of VPNs for up to 300 mobile users or sites for 2600
- Enables deployment of VPNs for up to 800 mobile users or sites for 3620/3640
- Enables deployment of VPNs for up to 2000 mobile users or sites for 3660
- Reserves critical CPU processing resources for other services such as routing, firewall, and voice

Platforms/Considerations

Routers	2600,3620, 3640, 3660,

First appearance in a Cisco IOS Software release: 12.1(3) XI(1)

1 Port Enhanced ESCON Channel Port Adapter

Description

The Cisco ESCON Channel Port Adapter (ECPA) has recently been enhanced to increase its processing capability and memory capacity. With these enhancements, CSNA, TCP/IP Offload, MPC+, and TN3270 Server customers can support more sessions through a single High-Performance ECPA. Processing capacity has been increased approximately 150 percent, while the supplied memory is increased to 128MB. The new High-Performance ECPA4 will complement the existing ECPA, and parallel channel port adapter (PCPA).

Features of the High-Performance ECPA4 include:

- 150 percent increase in CPU capacity—The increased processing capability increases the throughput for MPC+ protocols, and supports the processing requirements of SSL encryption in the TN3270 Server
- 300 percent increase in Memory capacity—increasing the number of TN3270 sessions that the ECPA4 is capable of handling.

Please access additional information on the High-Performance ECPA at:
http://www.cisco.com/en/US/products/hw/modules/ps2033/ps124/index.html

Benefits

- Support of CPU-intensive processing such as Secure Sockets Layer encryption for the TN3270 Server, and for Cisco Multi-Path Channel + (CMPC+)
- Increased memory to support larger numbers of TN3270 Server sessions
- Increased transactions per second throughput for mainframe data traffic

Platforms/Considerations

Routers	C7200

First appearance in a Cisco IOS Software release: 12.1(5)T.

AS58-324UPC-CC

Description

The current AS5800 universal access server can support up to 1344 modems. With the addition of the 324 port UPC card, the AS5800 can be populated with more than 2000 modems. In the US market this represents a change in density from two CT3s to three CT3s. In E1 countries, the AS5800 can support up to 64 E1 trunks.

The UPC modem card can be installed in an AS5800 that already includes the current 144 port modem cards or the older 72 port modem cards. Current features such as modem pooling, port level diagnostics, and hot-swap capability are available on the UPC card. The UPC card uses the Cisco Nextport modem technology which is shared with the new AS5400 access server platform.

Benefits

- It is interoperable with current modem cards protects customer investment.
- Increased density per card allows higher port densities in the AS5800 dial shelf.
- The addition of higher-density per modem cards allows more voice cards to be installed in the dial shelf when using the AS5800 as a combined voice and data platform.
- Operation of the UPC is consistent with the operation of previous modem cards, which reduces operator retraining and eases troubleshooting in mixed modem card configurations.

Platforms/Considerations

Access Servers (AS)	5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

TDM Potent: MIX-enabled 2/4/8 Port Multichannel T1/E1 Port Adapter with CSU/DSU

Description

The MIX-enabled 2/4/8 port multichannel T1/E1 port adapter supports 2, 4, 8, T1/E1 ports on the same port adapter. With a maximum of 48 ports supported on a single Cisco 7206VXR, this port adapter provides industry-leading density voice aggregation. This port adapter provides an ideal solution for New World voice applications for customers migrating from TDM networks to packet networks.

Multiservice Interchange (MIX) adds TDM connection capabilities for the Cisco 7200VXR series routers. The adapter takes advantage of the TDM connection capabilities of the Cisco 7200 VXR and provides voice, data integration on the same physical interface, Drop and Insert (Cross-Connect) TDM functionality, and DSP Farming.

Drop and Insert of DS0s and NxDS0s time-slots are provided between T1/E1 interfaces in the port adapter, providing efficient aggregation of different traffic types using fewer interfaces.

This port adapter makes efficient use of DSP farm supported on the 2 T1E1 digital voice port adapter, PA-VXC-2TE1. The DSP farm on the PA-VXC-2TE1 can now be shared with the MIX-enabled 2/4/8 port multichannel T1/E1 port adapter, providing a maximum of 20 T1 or 16 E1 digital voice interfaces. Various signaling protocols are supported, including T1 and E1 CAS, E1 R2, ISDN PRI, and QSIG.

Benefits

- *High-Density TDM Trunk Aggregation*—a maximum of 48 T1/E1 interfaces are supported
- *Drop and Insert Capability (D & I)*—DS0 D & I between any interface within the port adapter provides efficient traffic aggregation and reduction in WAN links
- *DSP Farm*—the adapters share the DSP resources on PA-VXC-2TE1 port adapters in the Cisco 7200 VXR router series, providing low-cost, high-density voice termination; 20 T1 or 16 E1 worth of voice traffic can be terminated on a single Cisco 7206 VXR router

Platforms/Considerations

Routers	7200 VXR

First appearance in a Cisco IOS Software release: 12.1(5)T.

Catalyst 4000 Access Gateway Module

Description

The Catalyst 4000 access gateway module is a modular Cisco IOS engine that provides:

- IP routing (WAN and inter-VLAN)
- Voice gateway to the PSTN or legacy PBX
- Voice network services

As an IP router the Catalyst 4000 access gateway module provides IP routing for inter-VLAN communications and a gateway to the IP WAN. As a voice gateway to the PSTN or legacy PBX, the module provides voice packetization services for delivery to or from the IP network. Enabling voice gateway functions for Cisco AVVID converged networks or simply providing toll by-pass functions for VoIP WAN solutions.

The third level of functionality provided by the Catalyst 4000 access gateway module is voice network services for Cisco AVVID converged networks. Voice services include ad hoc and meet-me conferencing services and, compression and transcoding services. The Catalyst 4000 switch shares this unique capability with Catalyst 6000 family and extends the benefits of IP based converged business applications from the large corporate head quarters to the branch office.

The WAN and voice interface flexibility is provided through support for the Cisco 1750, 2600 and 3600 WAN and voice interface cards (WICs, VICs, and VWICs). The high-density analog interfaces are supported in a wide FlexSlot while DSPs and WAN encryption modules are supported on board.

Benefits

The Catalyst 4000 access gateway module allows users to install a fully integrated router into a Catalyst 4000 switch chassis. The integrated router:

- Reduces rack space requirements in the enterprise branch
- Simplifies administration
- Simplifies cabling and installation

The modularity of the Catalyst 4000 access gateway module provides:

- WAN and voice interface flexibility through support for the Cisco 1750, 2600 and 3600 WAN and voice interface cards (WICs, VICs, and VWICs)
- Digital signal processor (DSP) slots to enable voice network services including Voice codec transcoding (G.711 to G.729a), conferencing, and other features
- Support for high density analog interfaces (future) in a wide Flexslot
- Support for a WAN encryption module (future)

Platforms/Considerations

Catalyst Switches (Cat)	Cat4000

First appearance in a Cisco IOS Software release: 12.1(5)T.

Note: The access gateway module is available in two configurations. First, it can be configured as a basic IP router running Cisco IOS Software, equivalent to a 3600 router on-a-blade in the Catalyst 4000 switch. Second, it can be a voice gateway for IP telephony and includes support for analog and digital voice interfaces as well as DSP services support.

Cisco 2600/3600 10/100 Ethernet/Token Ring Mixed Media NMs

Description

This release of Cisco IOS Software enables four new 3600/2600 network modules (NMs), all with two high-performance WIC slots and optional LAN. The LAN can be one or two 10/100 Autosensing Ethernet (full/half-duplex) ports or one Ethernet port with 1 4/16 Token Ring (full/half-duplex) port.

These new 2600/3600 network modules allow Cisco 2600 and 3600 owners to benefit from the increased performance and density capabilities delivered by this new range of NMs. Features also include new TDM capabilities.

Benefits

- Supported on complete range of Cisco 2600 and 3600 series multiservice platforms
- Supports all available WICs and VWICs
- Greater network module slot efficiency than currently available
- Increase WIC density in Cisco 2600 series
- Support for up to 8MB throughput on a WIC interface
- 10/100 autosensing full/half duplex FE LAN versions for 3600 series (full and half duplex)
- Full and half duplex Token Ring support (3600 only)
- TDM enabled

Platforms/Considerations

Routers	2600
The number relates to how many NMs are supported per chassis	3620
	3640
	3660
	NM-1FE2W
	N/A
	2
	4
	6
	NM-2FE2W
	N/A
	2
	4
	6
	NM-1FE1R2W
	N/A
	2
	4
	6
	NM-2W
	1
	1
	3
	6

First appearance in a Cisco IOS Software “T” release: 12.1(1)T.

ICS 7750 Multiservice Route Processor 200

Description

The Cisco Integrated Communications System (ICS) 7750 is an advanced IP telephony solution that delivers easily expanded managed Web-based communications applications that will transform branch-office and midmarket business environments into dynamic and responsive e-businesses.It gives businesses a cost-effective platform for quick deployment of powerful New World applications such as unified messaging, integrated Web call centers, data/voice collaboration and networked video—key solutions for becoming a competitive e-business.

The ICS 7750 is a six-universal-slot, industry-grade chassis system. Each universal slot accepts a resource card-the multiservice route processor (MRP) or the system processing engine (SPE)-to address the widest range of data and voice connectivity and application needs for a business.

The MRP is the multiservice router/voice gateway card running industry-proven Cisco hardware and Cisco IOS technology to support both digital and analog voice trunk gateways and WAN interfaces-all on a single modular card. It offers a wide selection of data and voice interfaces, allowing you to match bandwidth to the needs of each site as you grow. This also enables you to take advantage of all existing Cisco services such as virtual private network (VPN), firewall, IP Security (IPSec), and quality of service (QoS) to ensure quality voice and data transmission. In addition, proven Cisco voice trunk and station interface cards make it easy to link your Cisco ICS 7750 system to the Public Switched Telephone Network (PSTN) and existing private branch exchanges (PBXs), as well as the most common analog devices (including fax machines and teleconferencing stations). Each MRP card has two slots that accept any of the existing Cisco Voice Interface Cards (VICs) and WAN interface cards (WICs). The Cisco ICS 7750 puts you in control of your data and voice needs now and in the future.

Please see additional information on the ICS 7750 Multiservice Route Processor 200 at:
http://www.cisco.com/en/US/products/hw/voiceapp/ps967/ps968/index.html

Benefits

- Delivers powerful, full featured Cisco IOS capabilities for IP data routing and voice trunking
- Provides the flexibility to choose the WAN and PSTN/PBX interfaces that best suit your bandwidth and traffic needs
- Ensures end-to-end QoS for voice and data traffic
- Leverages consolidated (shared) facilities for voice and data traffic, optimizing the use of bandwidth for reduced operating costs
- Enables easy upgrades to new WAN technologies as they become available

Platforms/Considerations

- Integrated Communications System (ICS) 7750
- Multiservice Route Processor 200

First appearance in a Cisco IOS Software release: 12.1(3)XI.

IBM Support

TN3270 Server Connectivity Enhancements

Description

Release 12.1(5)T of Cisco IOS Software offers new TN3270 Server features that enhance security, simplify configuration, and supportability for Cisco TN3270 users. These new features include:

- Logical Unit (LU) Name nailing in load-balanced and redundant configurations
- Assignment of LU names using domain name services symbolic names in a Dynamic Host Configuration Protocol environment
- Secure Socket Layer (SSL) encryption between the TN3270 Client and TN3270 Server
- Support for more “native” 3270 functions such as SNA Sense Codes and Keyboard Restore Indications

These features extend the industry-leading, channel-attached Cisco TN3270 Server products, continuing the Cisco commitment to IBM mainframe access using standards-based IP solutions.

Benefits

- The enhanced Cisco LU nailing support allows the TN3270 Server to pass a logical unit name to VTAM, and to ask VTAM to dynamically create an LU with that name. The new support allows the TN3270 Client to connect to any of the available TN3270 Servers, and for the selected TN3270 Server to request a specific LU name on the client’s behalf.
- Secure Sockets Layer (SSL) is a de facto standard for protecting TCP/IP data transmitted between a server and a client. When used with an SSL capable TN3270 emulator, such as Host on Demand, SSL provides secure message integrity and confidentiality.
- Inverse nailing support from Cisco uses the directory name service in routers to look up the symbolic name associated with an IP address. The TN3270 server for the CIP and CPA then uses this symbolic address to assign a predefined LU name for the user. This eliminates the need for TN3270 clients to have statically defined IP addresses.
- The TN3270 and TN3270E RFCs do not always simulate the actions of a “real” 3270. This can cause problems when an end-user changes TN3270 emulators, or moves from a real 3270 terminal to a TN3270 emulator. Enhancements to the TN3270 Server allow it to more closely mimic the actions of a “real” TN3270.

Platforms/Considerations

Routers	C7x00

First appearance in a Cisco IOS Software release: 12.1(5)T.

IP and Routing

DHCP Relay Support for Unnumbered Interfaces

Description

RFC 2131 outlines how DHCP should work, but does not account for handling interfaces within a routing devices that are configured as IP Unnumbered. Point to point connections can be configured as IP Unnumbered, that is the interface does not have an IP Address of its own but shares the IP address of another interface within the same physical device.

This allows customer to conserve IP Addresses, by associating 1 or more IP Unnumbered interfaces with a Numbered interface.

Cisco has enhanced the DHCP Relay feature within Cisco IOS Software so that it in addition to numbered interfaces, IP Unnumbered interfaces can now be supported to send and receive DHCP requests.

The ability to support IP Unnumbered interfaces:

- Allows DHCP clients across multiple IP Unnumbered interfaces to share pools (scopes) of IP Addresses, which conserves IP Addresses and allows IP Addresses to be used more efficiently
- Removes the requirement for static host route information, this is handled dynamically by DHCP Relay

DHCP Relay keeps track of DHCP “clients” and is able to add and delete routing information dynamically. Optionally you can configure DHCP Relay to save client information that is tracked to a local file (for those devices supporting FlashDisk storage) or remotely to a workstation via TFTP. This information will be read in by DHCP Relay at (re)start time.

Benefits

- IP dhcp database command has been enhanced for use with the DHCP Relay feature http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cddhcp.htm#xtocid1494021
- IP Unnumbered interfaces are now supported
- Conserves IP Addresses
- Eases provisioning, by removing the requirement to configure static routes per interface.

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(2)T.

DHCP Server Import Capability

Description

Previously network administrators had to manually configure Cisco IOS DHCP Server, on each Cisco device enabled with this feature. This can be labor intense and, after a router has been deployed, can be extremely time consuming and expensive.

With this in mind Cisco has enhanced Cisco IOS DHCP Server to allow configuration information to be updated automatically by either PPP or, in future releases, by Cisco IOS DHCP Client. Network. Administrators can use one or more centralized DHCP Servers to update specific options within the DHCP Pools configured in Cisco IOS router.

Working in conjunction with PPP/IPCP changes outlined in CSCdk01128 [12.1(2)T], a network administrator can enable PPP to automatically configure Domain Name System (DNS) and Windows Internet Name Service (WINS, aka NetBios Name server - NBNS) Server IP Address information within a Cisco IOS DHCP Server Pool(s).

Benefits

- Saves time and expense by enabling centralized configuration of DHCP pools

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

Caveats:

- DHCP Server Import Capability DDTS CSCdp71173
- The [no] import all command must be configured per pool that is to be dynamically configured. Typically a single pool is configured. This command was introduce in 12.1(2)T
- Associated PPP enhancements are covered by DDTS CSCdk01128
- There are 2 new PPP configuration commands:
  - ppp ipcp dns accept
  - ppp ipcp wins accept

They tell the NAS to not NAK the peer's IPCP Configure Request if the peer sends non-zero addresses in the DNS and WINS options as defined in RFC 1877. Without this command, the NAS would respond to the peer with a NAK containing the addresses it felt the peer should use. That caused confusion with some PPP clients.

- To control which parameters are configured dynamically, configure the appropriate PPP command outlined above.
- If multiple interfaces are configured to use this enhanced PPP feature, each interface will write the configured parameters to the pool configured with the [no] import all command. In the case where both interfaces are configured to write the same fields, the last interface to write wins. Typically there is only 1 interface using this enhanced PPP functionality.

First appearance in a Cisco IOS Software release: 12.1(2)T.

DHCP Client

Description

In 12.1(2)T we are adding a DHCP Client to Cisco IOS Software, which can be used dynamically assign an IP Address to an Ethernet interface on a router.

A new command [no] ip address dhcp can be configured per Ethernet interface.

This new feature adheres to RFC 2131 as it defines the DHCP protocol.

This new DHCP Client within Cisco IOS Software can also be combined with the DHCP Server and NAT features in Cisco IOS Software, referred to EasyIP. An IP Address configured using DHCP can be used as input to the Port Address Translation (PAT or Overload) feature of Cisco IOS NAT, and used as the "public" address for all sessions to the outside world through this router. The user does not configure the IP Address but simply configures NAT to use "name" of the Ethernet interface using the new DHCP Client.

Benefits

- Enables customers to centrally control the IP address assigned to a Cisco IOS router, making management of 00's or 000's of routers much more manageable. Common scenario is the deployment of a router behind a DSL or Cable modem connected via Ethernet, where the ISP wants to dynamically assign an IP Address to the routers Ethernet interface.

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

Caveats:

- Each interface configured to obtain an IP Address via DHCP must have reachability to a DHCP Server. The DHCP Client will send the DHCP packets out the configured interface and not through another interface in the router
- In this initial release only Ethernet interfaces are supported. Further interface support is planned.

First appearance in a Cisco IOS Software release: 12.1(2)T.

NAT—Support for PPTP in an Overload (Port Address Translation) Configuration

Description

Microsoft PPTP tunneling is widely deployed and used to enable remote users to connect back to their corporate network in a secured fashion across the public internet.

Currently Cisco IOS Network Address Translation (NAT) only supports PPTP tunneling when configuring “Static or Dynamic” 1 to 1 address translation. The Overload, or Port Address Translation (PAT) configuration is not supported. So each individual PPTP tunnel requires its own IP address.

IP address translation is performed on the external IP headers. Any IP addressing “embedded” inside packets within the tunnel is not translated.

1. We assume the IP source address of the PPTP user is “locally” significant to the network the user is tunneling or connecting to, therefore no translation will be required on any embedded IP addresses
2. Encryption can be used on data payload but cannot be applied to GRE control flows inside the PPTP tunnel. NAT must be able to inspect the GRE control flows, if they are encrypted NAT will not be able to support PPTP tunnels with a Port Address Translation (PAT) configuration

Multiple entries per PPTP tunnel are generated in the NAT translation table to properly support translation and deliver back to the inside user.

- 1 TCP entry is generated per Tunnel
- 2 GRE entries per session within the tunnel

Benefits

- Customers can conserve their “public” IP Addresses by allocating a single IP address to a remote location, and allow multiple users to establish PPTP connections simultaneous to the same or different locations

Platforms/Considerations

Routers Universal Broadband Routers (UBR)	800–7200, C64xx, C7x00, andC8500 UBR7200
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software T release: 12.1(4)T.

DHCP Server—Easy IP Phase 2

Description

EasyIP is a marketing bundle combining 3 individual features within Cisco IOS Software:

1. Cisco IOS DHCP Server
2. Cisco IOS Network Address Translation (NAT) “Overload” configuration
3. Use of PPP/IPCP to dynamically obtain and configure an IP Address for a Serial/WAN interface.

The combination of these 3 features provides the optimal use of “public” IP address space they have purchased, the ability to factor in room for growth in any remote location without directly impacting their public IP address space, the ability to re-use routers for other locations and central control of the IP Address assigned to the remote location.

Cisco now adds a DHCP Client to Cisco IOS Software, which can be used dynamically assign an IP Address to an Ethernet interface on a router. A new command [no] ip address dhcp can be configured on an Ethernet interface.

This new DHCP Client within Cisco IOS Software can also be combined with the DHCP Server and NAT features in Cisco IOS Software. An interface assigned using DHCP can be dynamically read in by NAT and used as the “public” address for all sessions to the outside world through this router. The user does not configure the IP Address but simply tells NAT to use “name” of the Ethernet interface being configured using DHCP.

Benefits

With Release 12.1(3)T Cisco will enable corporate customers and ISP’s to centrally configure the following information on a per pool basis within the Cisco IOS DHCP Server:

- DNS Server Addresses
- WINS (NBNS) Server Addresses
- Domain Name
- Option 150 TFTP Server IP Address

Additionally Cisco adds:

- Support for a Bridged Virtual Interface (BVI) interface
- Ability to add a Default IP Route statement of “0.0.0.0 0.0.0.0 <DHCP Option 3 info>”
- A Static Route entry for each route provided in DHCP Option 33

All of this information will be extracted from the DHCP Server response, when using the Cisco IOS DHCP Client to configure an Ethernet or Bridged Virtual Interface (BVI) interface. If any of the above information is not present in the response form the DHCP Server then no information will be configured in the DHCP Server pool.

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

Caveats:

- The [no] import all command must be configured per pool that is to be dynamically configured. Typically a single pool is configured. This command was introduced in 12.1(2)T.
- Currently either all parameters are configured or none. To control which parameters are configured dynamically you simple exclude the appropriate information from the DHCP Server response. Future enhancements will provide additional granulator

- If multiple interfaces are configured to use DHCP Client, each interface will write these parameters to the pool configured with the [no] import all command. Last interface to write wins. Typically there is only 1 interface using the DHCP Client today. Future enhancements will provided additional control

First appearance in a Cisco IOS Software release: 12.1(3)T.

HSRP Support for MPLS VPNs

Complete feature description pending, to be updated ASAP

MPLS Traffic Engineering Enhancements

Benefits

MPLS traffic engineering offers benefits in two main areas:

- Higher return on network backbone infrastructure investment: Specifically, the best route between a pair of POPs is determined taking into account the constraints of the backbone network and the total traffic load on the backbone. This enables the spreading of inter-POP traffic over all available links leveraging higher utilization of network bandwidth than is capable in a pure IP network.
- Reductions in operating costs: Costs are reduced because numerous important processes are automated. These include path selection, tunnel setup, tunnel monitoring, rerouting in the event of a change in topology, and traffic forwarding onto a traffic engineered tunnel.

Platforms/Considerations

Routers	Cisco 7200 Series—POS interfaces only Cisco 7500/RSP Series—POS interfaces only

First appearance in a Cisco IOS Software release: 12.1(3)T.

AutoInstall Using DHCP for LAN Interfaces

Description

Currently, Cisco IOS Software uses the following mechanisms to automatically obtain an IP address for one or more of its network interfaces when the NVRAM is invalid (no startup configuration): RARP, BOOTP-based AutoInstall, and download of default configuration file. With the trend of DHCP becoming the more common method of IP address allocation, this is the first in a series of phases to streamline the router configuration initialization process.

This initial phase implements the following:

- Convert BOOTP-based LAN AutoInstall to DHCP-based mechanism

There are two parts to this:

1. Move IP address procurement function of AutoInstall to be handled by DHCP client (for LAN interface only in this phase)
2. Manage the uploading of configuration file, within the DHCP-based AutoInstall process. This also allows for the uploading of configuration file whose name is passed on as option 67 (Configuration filename) in the DHCP Offer from the server.

- Enhance current DHCP client to recognize replies coming from regular BOOTP server (to provide seamless transition for customers who have been using BOOTP server to service the LAN AutoInstall)

Benefits

- Router address initialization and TFTP process now work together in a proper initialization sequence as opposed to being separate tasks
- Initial move from Bootp to DHCP based on standard RFC 2131 (for LAN Autoinstall)
- Includes support for RFC 1534 Interoperation between DHCP and Bootp

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst® Switches (Cat) Route Switch Module (RSM) LightStream® Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

NAT—Support of IP Phone to Cisco CallManager

Description

Cisco IP phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco CallManager (CCM) server. When an IP phone registers, and while it is connected and using the services of the CCM, messages flow back and forth. These messages include IP address and port information, used to identify other IP phone users with which a call can be placed.

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

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

Benefits

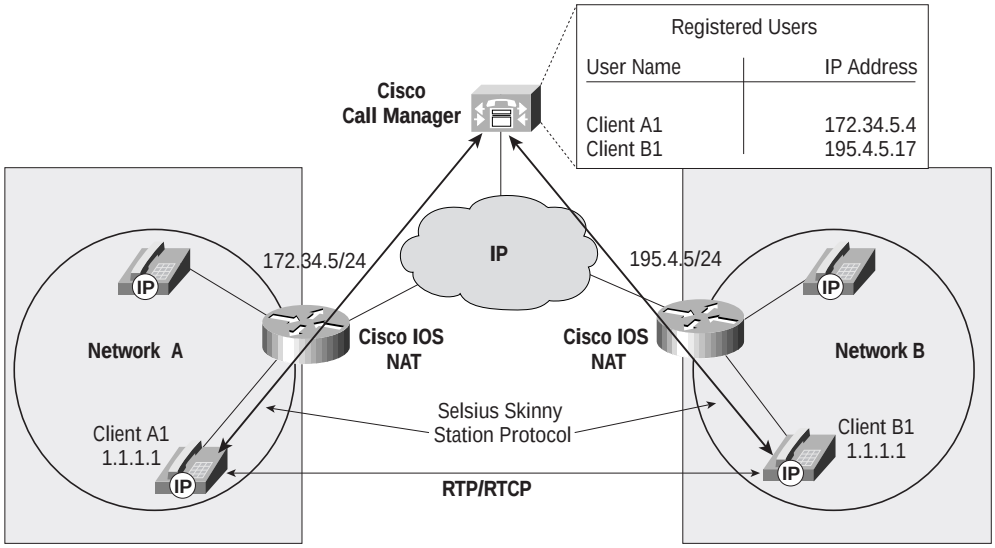
- Allow Network Address Translation (NAT) to “dynamically” perform IP address translation instead of having to manually configure an IP address within NAT for each IP phone
- Enables services providers and Enterprise customers to deploy IP phones to remote offices (SOHOs) and maintain centralized Cisco CallManager servers at the head office or a major regional center, while using NAT between the IP phone and CCM

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, andC8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Figure 6
Cisco IOS NAT Supporting IP Phone to Cisco Call Manager



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

Description

Cisco IOS Network Address Translation (NAT) now supports all H.225 and H.245 message types, including FastConnect and Alerting, as part of H.323v2 specification.

Before this enhancement, NAT only supported H.323v1, and that was specific only to the NetMeeting application. With this enhancement, any product that uses these message types can pass through a Cisco IOS NAT configuration with no static configuration.

One such product is the Cisco voice gateway. As of 12.1(1)T implemented support for H.323v2 and the FastConnect message type.

Note: Cisco IOS NAT currently does not support RAS (Registration/Admission/Status) so voice gateway to voice gateway connectivity was tested with out the use of RAS to resolve a destination.

Benefits

- Ability use the Cisco voice gateway product through a Cisco IOS NAT configuration (applies to any product making use of H.323v2 H.225/H.245 messages)
- Ability to perform IP address translation on traffic flowing between voice gateways, which could be from
  - Networks with the same IP addressing scheme
  - Private address scheme connecting to the outside or public
  - Networks want to hide their real IP addresses from the public
- No static configuration required within NAT for H.225/H.245 products

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

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

Description

Microsoft NetMeeting is a Windows-based application that enables multiusers interaction and collaboration from a users PC, over the Internet or an intranet to:

- Connect directly with one another, if they know the other clients destination IP address
- Connect with another client by selecting clients from a directory (ILS-Internet locator service) maintained by NetMeeting of registered NetMeeting clients
- Search for other NetMeeting clients not in the same directory
- Establish “phone” connections with “real” telephones, by configuring NetMeeting to connect to an H.323 gatekeeper such as the Cisco MCM

Current support for NetMeeting within Cisco IOS Network Address Translation (NAT) only supports direct user to user connectivity through a NAT device. NAT does not support the ability of using the directory (ILS) function built into NetMeeting.

This lack of support inherently limits the scalability of a NetMeeting solution with NAT in a network that includes more than 10 or 20 users, not to mention ISP's looking to use NetMeeting for early voice-over-IP (VoIP) services. With this enhancement to Cisco IOS NAT, ISPs and enterprise customers alike can build and deploy privately addressed NetMeeting environments and services that will scale to any customer base.

Benefits

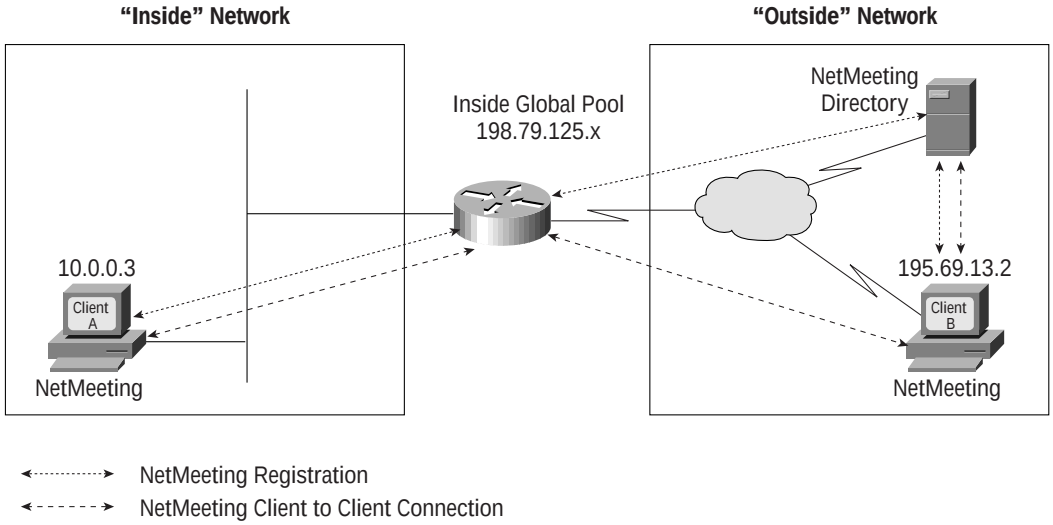
- ISPs and enterprise customers can deploy a scalable solution with NetMeeting and NAT
- Use of the NetMeeting Directory (ILS) makes NetMeeting useable for customers
- The NetMeeting Directory (ILS) enables users to request a connection by name instead of IP address

Platforms/Considerations

Routers Universal Broadband Routers (UBR)	800–7200, C64xx, C7x00, and C8500 UBR7200
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Figure 7
Network Address Translation NetMeeting ILS Support



Trace Route Enhancement for MPLS

Description

This feature is useful when expired TTL packets do not return to a source if there is a break in the Interior Gateway Protocol (IGP) path. Currently, MPLS forwards the expired TTL packets by re-imposing the original label stack and forwarding the packet to the end of a label switch path (LSP). For provider edge routers forwarding traffic over a virtual private network (VPN), this is the only way to get the packet back to the source. If there is a break in the IGP path to the end of the LSP, the packet never reaches its source.

Packets that have a single label are usually a global address or terminal VPN labels. Those packets can be forwarded using the global IP routing table. Packets that have more than one label can use the original label stack.

Benefits

- Better trace-route and debug capabilities: This command provides reliable trace-route capabilities by providing the support for packets to be forwarded either using the label stack or using the global routing tables depending on the number of labels present.

Platforms/Considerations

Routers	C 2600, C36xx, C4x00, and C7x00

First appearance in a Cisco IOS Software release: 12.1(5)T.

MPLS Scalability Enhancement for LSC and ATM LSR

Description

Edge LSRs connected to an MPLS-enabled ATM backbone may potentially create multiple VCs to ATM LSCs depending on the number of IP addresses in the core network. This may result in the creation of unnecessary virtual circuits to numbered addresses inside the core, regardless of adjacency, as each IP address in the core creates an entry into the routing table. Since VC is valuable resource, the utilization of VC space is inefficient

This feature reduces the number of VCs created by ATM LERs (label edge routers) and LSCs (label switch controllers) specified via the access list that can permit or deny the initiation of head-end label requests.

Benefits

- Enhanced scalability: a fewer VCs are required in the network to run the same services
- Easier management: fewer VCs and label switched paths to manage
- Efficiency: reduces the number of VC setups

Platforms/Considerations

Routers	C72xx and C75xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

Frame Relay Switching Enhancements: Shaping and Policing

Description

The Frame Relay (FR) switching enhancements functionality provides added FR switching features to enable a router to behave as a Frame Relay Switch. The previous support on the routers enabled only simple FR switching behavior via static map configurations.

The router, acting as a virtual FR switch, will now have the ability to set the FECN/BECN forward explicit congestion notification/backward explicit congestion notification (FECN/BECN) bits in switched packets when network congestion is present. This will allow the far ends of a PVC to be notified of congestion in the data path and potentially reduce data transmission into the PVC.

The router will also have the ability to set the discard eligibility (DE) bit for switched packets that may need to be potentially discarded when there is network congestion. In addition, the router will have the ability to police traffic based upon the committed information rate (CIR) when acting as a FR switch. Finally, FR switching will now also be supported on ISDN interfaces as well as serial interfaces, as before.

Benefits

- Router can act as a commercial FR switch
- FECN/BECN/DE/CIR support as a FR switch
- FR switching over ISDN support

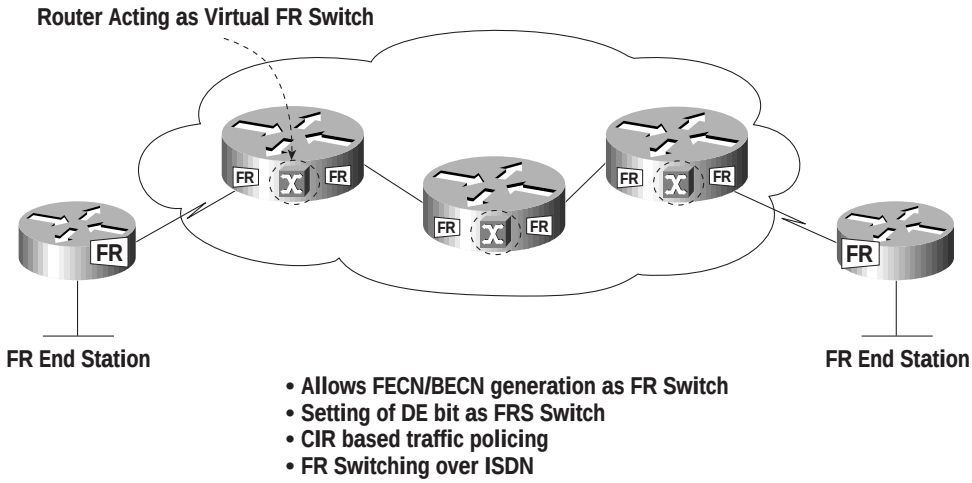
Platforms/Considerations

This feature is platform independent for router platforms currently supporting Frame Relay.

Routers	Cisco 1400, 160x, 17X0, 25xx, 26xx, 36xx, 4x00, and 7x00

First appearance in a Cisco IOS Software release: 12.1(2)T.

Figure 8



Management

Service Assurance Agent Enhancements

Description

- *Service Assurance Agent*—The Cisco IOS Software Service Assurance (SA) Agent is an application-aware synthetic operations agent that monitors network performance by measuring key service level agreement (SLA) metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, packet loss, and application performance.

With the increasing importance of mission-critical applications and networks linking global enterprises, customers are demanding SLAs that guarantee minimum acceptable levels of service. The challenge for the network operators is to create a reliable mechanism for accurately monitoring and ensuring contractual levels of service. Measurement features of the SA Agent built into Cisco IOS Software enable customers to provide assurances for the managed or delivered services.

The SA Agent allows users to monitor network performance between a Cisco router and a remote device, which can be another Cisco router, an IP host or a multiple virtual storage (MVS) host. This feature enables users to perform troubleshooting, problem analysis, and notification based on the statistics collected by the SA Agent.

The SA Agent was previously known as the Response Time Reporter (RTR). The response time and availability monitoring capabilities of RTR have been extended to include support for voice over IP (VoIP), quality of service (QoS), and the Web, and thus RTR has evolved into the SA Agent, starting with Cisco IOS 12.0(5)T.

Benefits

With this release of Cisco IOS Software, the following additional features of SA Agent are supported:

- *Service-Level Monitoring*—Enhanced UDP latency reporting, one-way latency measurement is supported to enable more accurate assessment of round-trip response times.
- *Application-Level Monitoring*—A new operation is now supported to measure FTP download time.

- *Ease of use*—The Round-Trip-Time-Monitoring (RTTMON) MIB has been enhanced to allow network management applications to configure the SA Agent responder capability. Previously, the SA Agent responder could only be configured using the Cisco IOS command-line interface.

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C100x, C14xx, C16xx, C17xx, C25xx, C26xx, C36xx, C4x00, C6400, and C7x00 UBR7200 MC3810
Catalyst Switches (Cat)	5000 RSM, 6000 RSM
Access Servers (AS)	AS5300, AS5800

First appearance in a Cisco IOS Software "T" release: 12.1(1)T

Virtual Switch Interface Master MIB

Description

The Virtual Switch Interface (VSI) Master MIB supports the following VSI components:

- *VSI Controllers*—Each controller represents an instance of the VSI Master control protocol. A controller communicates with a set of VSI slaves across a control interface. The controller, which runs the VSI protocol, supports a network control application. The application can perform the following functions with the help of the VSI:
  - Control the virtual circuit cross-connect table inside an ATM switch.
  - Monitor the status of and collect statistics from interfaces and virtual circuits on the switch
  - Discover switch configuration information
- *VSI Sessions*—Each VSI controller managers a set of VSI slaves through a protocol instance called a session. VSI slaves reside on the controlled ATM switch. The VSI controller uses the VSI protocol to discover the number and characteristics of the VSI slaves. The table includes an entry for each VSI slave the controller discovers.

- *Logical Interfaces*—Logical interfaces represent external ATM interfaces that are available for connections. When you pair two external interfaces (represented by two logical interfaces), these interfaces provide physical paths through the switch. These physical paths support cross-connects.
- *Cross Connects*—Cross connects are virtual links across two interfaces.

Benefits

- Implementing the VSI Master MIB enables the management of virtual switch interfaces through SNMP commands and traps.

Platforms/Considerations

Routers	Cisco 7200 Series (PA-A3 and PA-A1 only) Cisco 7500/RSP Series (PA-A3 and PA-A1 only)

First appearance in a Cisco IOS Software release: 12.1(3)T.

MSDP MIB

Description

Multicast Source Discovery Protocol (MSDP) is a mechanism used to propagate active source information either within a single domain or across multiple domains. It can be used in conjunction with PIM Sparse Mode to allow information about multicast sources for a group to be shared amongst Rendezvous Points (RPs). This management information base (MIB) describes managed objects used for monitoring MSDP.

Benefits

- Improved monitoring capability for MSDP

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4500, C7100, C7200, C7500, C8850 UBR7200 MC3810
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Trace Route Support in a MPLS Network

Description

This feature enhances the debugging and CLI-based management tools by providing a mechanism to control MPLS TTL on locally originated trace route in a MPLS-enabled network

By executing the command on the router, the network manager can display all MPLS hops between PE-PE in a PE-PE trace route, or display MPLS cloud as one hop in CE-CE trace route.

Benefits

- Enhances trace route debugging capabilities in MPLS networks allowing network managers to better manage MPLS networks for both locally generated and forwarded packets.

Platforms/Considerations

Routers	Cisco 7200 Series Cisco 7500/RSP Series Cisco 3600 Series

First appearance in a Cisco IOS Software release: 12.1(5)T.

NTP MIB

Description

Current Cisco IOS Software releases have no method of retrieving network timing information via SNMP.

This feature NTP MIB now provides a method through which management applications can retrieve the information via SNMP. This is a critical feature because when applications are retrieving information from various different network devices, they must use the same clock time in order to synchronize data and draw conclusions.

Benefits

- Provide a standard method (SNMP) of accessing network timing information
- Application providers can now easily and accurately perform end-to-end network monitoring by retrieving and comparing network performance data at any instance of time

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Interface Index Persistence

Description

In current Cisco IOS Software releases, assigned interface index numbers are not kept persistently after rebooting. Whenever an interface is rebooted, a new interface index number is re-assigned, making applications relying on this information unable to keep track of the logical interface number associated with the physical interface.

This new feature keeps the interface number assigned to the port on initial power up in nonvolatile RAM, even after reboot, so that applications can rely on the this information.

Benefits

- Management application can now rely on consistent interface index information via SNMP to produce applications after system reboot.
- Long-term SNMP monitoring was once difficult to implement because of the fluctuating ifIndex as network devices reboot. Often applications have to maintain a separate technology to maintain consistent data if long-term monitoring is desired. Cisco IOS Software now maintains the ifIndex in nonvolatile RAM to keep the index number consistent.

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, C7x00, and C8500 UBR900, UBR7200 MC3810
Catalyst Switches (Cat) Route Switch Module (RSM) LightStream Switch (LS)	Cat8500, Cat6000, Cat2900, Cat2900 XL, Cat4000 Cat5000RSM LS1010
Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Monitoring Resource Availability on Cisco AS5x00 Universal Access Servers

Description

The features available through this development will improve the visibility into the line and modem status of the AS5xxx Universal Access Server. This is achieved by providing enhancements to a number of the MIBs and CLI commands.

The following new traps have been introduced:

- DS1 Loopback Trap
- DS0 Busyout Trap
- ISDN PRI Requested Channel Not Available Trap
- Modem Health Trap

In addition to these traps enhanced CAS state information is available through a new “show controllers” CLI command.

A detailed functional description of these features can be found at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080281.html

Benefits

- New trap-based fault notification will highlight system faults to a network operator to facilitate early resolution of network problems
- Comprehensive health monitoring of network device allows an operator to identify faults before they become customer effecting

- Trap notification reduces the need frequent polling of device status, saving bandwidth on the management network and improving performance

Platforms/Considerations

Access Servers (AS)	5300

First appearance in a Cisco IOS Software release: 12.1(5)T.

Multimedia

Bidirectional PIM

Description

Bidirectional PIM (Protocol Independent Multicast) is an optimized solution facilitating many-to-many or N-way multicast sessions. Some applications of this technology are multimedia conferencing, chat groups, distance learning, multiplayer games, and distributed interactive simulations.

Bidirectional PIM is an extension to the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. If a router joins a bidirectional tree on behalf of a group member, that branch of the tree is used not only for the member to receive data, but also to send data if the member is also a sender.

For more information, refer to: ftp://ftpeng.cisco.com/ipmulticast/bidir/index.html

Benefits

- *Network Scaling*—bidirectional PIM reduces the amount of state a router has to keep; this helps reduce memory, bandwidth, and CPU requirements
- *Easier Maintenance*—because the router needs to maintain less state information, it is easier to troubleshoot problems

Platforms/Considerations

Routers	C1003, C1004, C1005, C16xx, C25xx, C26xx, C28xx, C29xx, C36xx, C38xx, C4000, C4000-M, C4500, C4500-M, C4700, C4700-M, C72xx, and C75xx

First appearance in a Cisco IOS Software “T” release: 12.1(2)T.

Source Specific Multicast (SSM)

Description

Source-specific multicast is an extension to the IP multicast service available in Cisco IOS Software since version 10.2. It provides a super-scalable, performance-optimized, thin network solution primarily for one-to-many applications such as Internet broadcast. SSM includes two Cisco unique solutions, URD and IGMP v3lite, which will bootstrap the development of SSM-aware applications and the deployment of SSM in networks for both content developers and distributors. Cisco IOS Software is committed to deploying and fully supporting IGMPv3 for both SSM and traditional IP Multicast service.

Currently, a receiver joins a multicast group but has no ability to specify a source. Multiple sources can exist and all data from them will be received. SSM enables the selection of a particular source for multicast data. This prevents traffic from other sources for the same group from being forwarded to the host. SSM requires well-known sources and is most useful for static applications.

Benefits

- *Comprehensive solution*—provides a complete solution for SSM services and jumpstarts deployment.
- *Seamless migration*—facilitates a seamless migration to IGMPv3 based on customer timelines and demands.
- *Reduced latency*—eliminates cut-over to the shortest path tree.
- *Simplification*—much less routing complexity and greatly reduces the need for multicast address management and improved ability to provision it with very little complexity in the network.
- *Improved security*—no DoS attacks from unknown sources.

Platforms/Considerations

Routers	C80x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4500, C4700, C71xx, C72xx, C75xx, UBR7200, UBR920
Catalyst Switches	RPM
Access Servers (AS)	AS5800, MC3810

First appearance in a Cisco IOS Software Release: 12.1(3)T.

IGMP Version 3

Description

IGMP is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, Version 3 adds support for “source filtering,” which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS Software only forwards traffic that is requested by the host (or by other routers via PIM) to that network. In addition to restricting traffic on the receiver host’s network, IGMP v3 membership information may also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

The newest thing in the multicast space is Source Specific Multicast (SSM), introduced in 12.1(3)T, in which hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMP v3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases in which IGMP v3 cannot be used (for example, if it is not supported by the receiver host or its applications), two other mechanisms enable SSM: URL Rendezvous Directory (URD) and IGMP v3lite, both introduced with SSM in 12.1(3)T.

Please access additional information on IGMP Version 3 at: ftp://ftpeng.cisco.com/ipmulticast.html#IGMPV3

Benefits

- Enables new multicast services-channel subscription
- Optimized bandwidth utilization-traffic is only forwarded from permitted sources

- Improved security-no denial of service attacks from unknown sources

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4500, C7100, C7200, C7500, C8850 UBR7200 MC3810
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

PIM Dense Mode State Refresh

Description

State refresh is an extension to PIM Dense Mode (DM). PIM-DM traditionally operates with a periodic flood-and-prune behavior that occurs every 3 minutes. This enhancement prevents the periodic timeout of prune state in routers, keeping state alive longer. This eliminates the reflooding of multicast traffic down pruned branches that expire periodically. It also allows topology changes to be realized more quickly than with the traditional 3-minute timeout.

Please access additional information on PIM-DM State Refresh at: ftp://ftpeng.cisco.com/ipmulticast.html#SR

Benefits

- *Increased scalability*—eliminates re-flooding onto pruned branches of PIM-DM clouds
- *Faster convergence*—topology changes are realized more quickly

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	C800, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4500, C7100, C7200, C7500, C8850 UBR7200 MC3810
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Router-Port Group Management Protocol (RGMP)

Description

Cisco Group Management Protocol (CGMP) and Internet Group Management Protocol (IGMP) Snooping constrain multicast traffic that exits through switch ports to which hosts are connected. They do not constrain traffic that exits through ports to which multicast routers are connected.

This is particularly important in the backbone environment, where there are switches in the core and routers around them. RGMP allows multicast traffic in switched Ethernet backbone networks to scale with the number of switched router ports, which is similar to unicast traffic. Without RGMP, the multicast traffic in such networks is limited by the speed of the slowest switched port to a router.

With RGMP, network congestion is reduced by only forwarding multicast data to routers that are interested in receiving it. A router must be configured with RGMP so that the protocol can signal its interest in receiving the traffic. RGMP runs between Cisco routers and Layer 2 Catalyst switches, and therefore must be enabled on both devices.

Please access additional information on RGMP at: ftp://ftpeng.cisco.com/ipmlticast.html#RGMP

Benefits

- *Scalability*—eliminates flooding of multicast data
- *Reduced latency*—no unwanted multicast traffic delaying production multicast traffic

Platforms/Considerations

Routers	C800, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4500, C7100, C7200, C7500, C8850
Universal Broadband Routers (UBR)	UBR7200
Multiservice Access Concentrator (MC)	MC3810
Catalyst Switches (Cat)	Cat4000, Cat6000
Route Switch Module (RSM)	Cat5000RSM
Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software release: 12.1(5)T.

Multimedia Conference Manager with Voice Gateway image with RSVP to ATM SVC

Description

The Saguaro project is a Cisco IOS Software image that will integrate H.323 Cisco MCM (Multimedia Conference Manager—H.323 gatekeeper and H.323 proxy), H.323 VoIP gateway and routing. Saguaro will initially be supported on the MC3810, 2600 and 3600 series (including the 3660). It will allow enterprise customers to reduce costs by incorporating these features into a single chassis. Installed chassis can be easily upgraded via a software download to obtain this functionality. This solution helps further position Cisco as the leader in multi-service networking. This image will also incorporate the mapping of H.323 RSVP requests to ATM VBR SVCs as well.

Benefits

- One-Box Solution
  - By incorporating the gateway into the MCM image, customers can reduce overall cost of ownership. What was historically a two-box solution is now reduced to one. Not only is this a cost savings to the customer, but customers have one less box to manage.
- Bandwidth and Resource Management

  - Users can stipulate bandwidth limits for each videoconferencing connection as well as an aggregate bandwidth limit for all videoconferencing sessions. This is not an attempt to provide line conditioning, rather the ability to provide notification to endpoints of bandwidth limitations.
- NetMeeting Capabilities
  - The Proxy can now forward T.120 connections, thus enhancing real-time data conferencing capabilities.
- Load-Balancing
  - The gatekeeper has been enhanced to perform load-balancing functionality for external H.323 v2 gateways.
- Call Accounting
  - The MCM supports call-accounting functionality for proxied calls as well. Proxied calls will be recorded into call history to provide additional call detail information.
- Call Manager Environments
  - Use of an H.323 gatekeeper is recommended for use with multiple CallManager or CallManager cluster domains. This provides critical Connection Admission Control (CAC) between domains to guarantee that the number of calls between locations does not exceed available bandwidth. In addition, the gatekeeper can support dial backup to allow IP calls to be placed over the PSTN in the event of link failure. Thus, integration of necessary gatekeeper functionality within a Cisco IOS gateway device saves costs and increases reliability of IP telephony systems.

Platforms/Considerations

Routers	C26xx, C36xx, C7200
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(3)XI and 12.1(5)T.

Quality of Service

Express Resource Transport Protocol and TCP Header Compression (CRTP)

Description

Bandwidth is at a premium on low-speed WAN links, and voice traffic sent over these links requires compression. Compressed Resource Transport Protocol (CRTP) is required to ensure voice-over-IP (VoIP) scalability. The size of VoIP packets, including the IP header, the UDP header, and the RTP header, in addition to the voice payload, creates extensive network overhead.

For example, a G.729 (8K codec) VoIP call expands to 24 kbps when the IP/UDP/RTP headers are added. Considering that another 5 to 7 bytes of overhead are incurred per packet at Layer 2, a VoIP call could require up to 26 kbps. CRTP can compress the IP/UDP/RTP headers to as little as 2 bytes, resulting in a 12-kbps G.729 call.

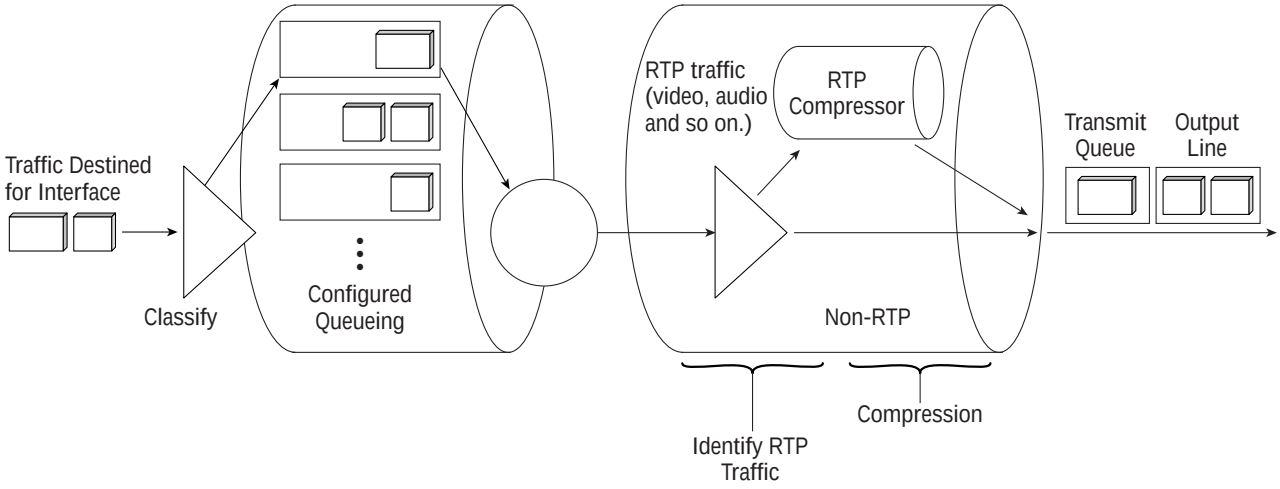
CRTP is especially beneficial when the RTP payload size is small, as is the case for compressed voice payloads. The payload of a typical voice packet using RTP is 20 bytes, while the header is often twice this size-the minimal 12 bytes of the RTP header, combined with 20 bytes of IP header (IPH) and 8 bytes of UDP header, create a 40-byte IP/UDP/RTP header. Given the size of the IP/UDP/RTP header combinations, it is inefficient to send the IP/UDP/RTP header without compressing it.

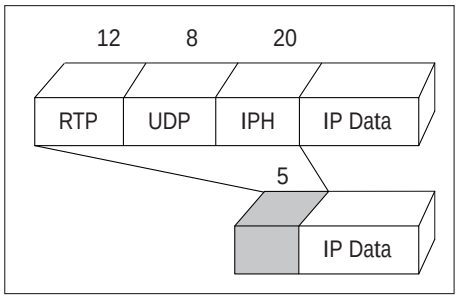
CRTP has been available for some time in Cisco routers, but, with this release, it has been added into Fast and CEF switching path, resulting in better performance and more scalability.

Please access additional information on Express RTP and TCP Header:

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

Figure 9
Express RTP and TCP Header Compression





Efficiencies	Payload	Packet Size Reduction*
VoIP	20 bytes	– 240%
SQL	256 bytes	– 13%
FTP	1500 bytes	– 2.3%

*Also 5-ms reduction in serialization delay at 64 kbps

Benefits

- Reduces network overhead by compressing the header
- Allows users a greater number of voice calls on an interface
- Express CRTP speeds the transmission of packets with a lot less overhead on CPU compared to the process switched CRTP, resulting in better utilization of available network resources such as bandwidth

Platforms/Considerations

Routers	Cisco 2600 Cisco 3600 Cisco 4000-M Cisco 7200 series

This feature is currently not supported on all the interface port adapters and media types on the above-listed platforms.

First appearance in a Cisco IOS Software “T” release: 12.1(1)T

COPS for RSVP

Description

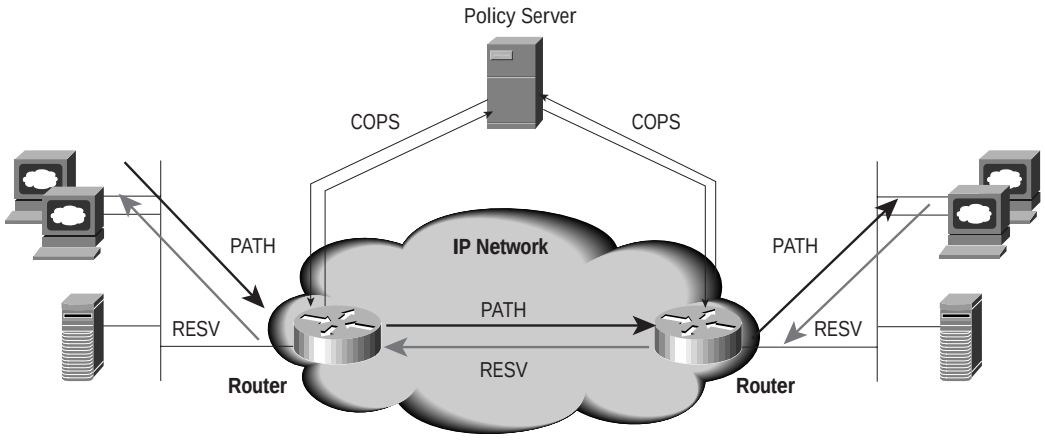
Common Open Policy Service (COPS) is a protocol to communicate policy information to network devices. It uses a client/server model for supporting policy control over Quality of Service (QoS) signaling protocols and provisioned QoS where policy servers return decisions to requests from policy clients.

COPS for RSVP uses a request-decision model to convey policy information. When an RSVP message arrives at the network device, the network device requests a decision from the policy server for the flow and implements the decision it receives. The validation of flows against the policy is done on a per RSVP request basis. This RSVP request could correspond to a single data flow or an aggregate data flow.

COPS for RSVP provides a framework for admission control i.e. acceptance or denial of requests, based on policy in addition to network resources. For example, a resource reservation request of 100-kbps bandwidth from Host X can be denied as Host X is not allowed to make a request more than 50-kbps. This policy decision is taken at the policy server, and the router understands the decision and sends an appropriate accept or deny request. This feature allows prioritization bandwidth requests and even preemption of low priority requests to accommodate higher priority requests.

For detailed configuration information, please check the documentation Web site: www.cisco.com/univercd/cc/td/doc/product/software/ios121/121/newft/121t1/copsrsvp.htm

Figure 10
COPS for RSVP



Benefits

- Policy-based admission control for RSVP requests that allow admission or denial of requests based on policy in addition to resource availability
- Allows centralized administration and control of the policies
- Enables billing and management of calls from centralized location
- Ensures adequate bandwidth and jitter and delay bounds for time-sensitive traffic such as voice transmission
- Prevent bandwidth-hungry applications from delaying top priority flows or harming the performance of other applications customarily run over the same network In so doing, COPS for RSVP supports the following crucial RSVP features:
  - *Admission control*—the RSVP reservation is accepted or rejected based on end-to-end available network resources
  - *Bandwidth guarantee*—the RSVP reservation, if accepted, will guarantee that those reserved resources will continue to be available while the reservation is in place
  - *Media-independent reservation*—an end-to-end RSVP reservation can span arbitrary lower layer media types
  - *Data classification*—while a reservation is in place, data packets belonging to that RSVP flow are separated from other packets and forwarded as part of the reserved flow
  - *Data policing*—data packets belonging to an RSVP flow that exceed the reserved bandwidth size are marked with a lower packet precedence

Platforms/Considerations

Routers	C7200, C7500 (Non-VIP mode only)

First appearance in a Cisco IOS Software "T" release: 12.1(1)T

DOCSIS 1.0+ Quality-of-Service Enhancements

Description

DOCSIS 1.0+ quality-of-service enhancements add several new capabilities to the UBR7200 series broadband routers, providing support of real-time services such as voice and fax from a DOCSIS 1.0+ capable CPE device such as the Cisco UBR924. This support has been designed and implemented over the current DOCSIS 1.0-based implementation using a minimal feature set derived from the DOCSIS 1.1 interim specification. It was designed as an extension to the current DODCSIS 1.0 architecture with easy migration towards a future, full-featured DOCSIS 1.1 implementation.

DOCSIS 1.0+ quality-of-service enhancements add the following features:

- *Concatenation Support*—DOCSIS concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, as well as increase transmission efficiency. Using concatenation, a DOCSIS RF CPE device need only make one bandwidth request for a concatenated packet, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for bursty real-time traffic such as voice calls. Concatenation is only supported with RF CPE devices that support DOCSIS concatenation.
- *Embedded Client Signaling (dynamic SIDs)*—Supports the dynamic creation, configuration, and deletion of service identifiers (SIDs) to accommodate different classes of service. This allows RF CPE devices to request high-priority or high-bandwidth data streams as needed, such as when a VoIP call is made. Dynamic SIDs can be used only with RF CPE devices that also support this feature. Otherwise, RF CPE devices must use the static SIDs supported in previous releases.
- *IP Precedence-Based Rate Limiting*—In addition to the currently supported traffic shaping techniques, Cisco IOS Software Release 12.0(7)XR2 supports a new configuration field that associates a maximum bandwidth (in kbps) with a particular setting of the IP type of service (ToS) bits. This can be used to ensure that certain traffic such as data does not exceed a preset rate limit and thereby interfere with higher-priority real-time traffic such as VoIP calls.

More information can be found at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xr/docsis1p.htm and
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xr/concat.htm

Benefits

- Concatenation reduces packet overhead and overall latency, thereby increasing per-modem upstream transmission efficiency
- IP type of service (ToS) bits provide independent rate limits for different traffic streams as desired, preventing lower-priority data from interfering with higher-priority, real-time traffic, such as voice-over-IP (VoIP) calls
- Embedded client signaling offers reliability and scalability for voice and video connections, allowing cable modems to request high-priority or high-bandwidth data streams as needed, such as when a VoIP call is made
- Through unsolicited grants, the UBR7200 router has very precise control over potential delay and jitter, thereby maintaining a Constant Bit Rate (CBR) traffic flow for real-time traffic such as voice and fax calls

Platforms/Considerations

Routers Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	UBR900, UBR7200

First appearance in a Cisco IOS Software "T" release: 12.1(1)T.

DOCSIS 1.0+ (UBR924)

Description

DOCSIS 1.0+ adds several new capabilities to the UBR924 allowing it to support real-time services such as voice and fax. It also adds capabilities to improve upstream performance. New capabilities allow for the creation of constant-bit-rate service classes that can include delay/jitter bounds as well as data rate. In addition, the service classes can be created and deleted dynamically. This capability is important to supporting voice and fax services on a real-time basis. Concatenated MAC frames are also supported in DOCSIS 1.0+ improving upstream performance.

Prior to DOCSIS 1.0+, the UBR924 was able to utilize two types of service, statically defined tiered best-effort and committed information rate (CIR). Although this capability is sufficient in a data-only DOCSIS 1.0 environment, these capabilities are not sufficient for the UBR924 to offer toll-quality voice and fax services. DOCSIS 1.0+ adds new capabilities allowing a UBR924 to dynamically request service classes with guaranteed data rate and delay/jitter bounds that support toll-quality voice service. In addition, concatenated MAC frames were not supported, limiting UBR924 throughput because it was required to explicitly request bandwidth for every packet of data sent upstream. DOCSIS 1.0+ improves upstream throughput by allowing the UBR924 to concatenate MAC frames.

Benefits

- *Dynamic Services*—allows for real-time service class creation supporting data, voice and fax services
- *Constant Bit Rate Service with Delay/JitterBounds*—allows for the support of real-time services such as voice and fax by guaranteeing data rate and quality of service
- *Concatenation Support*—improves UBR924 upstream performance

Platforms/Considerations

Universal Broadband Routers (UBR)	UBR924

First appearance in a Cisco IOS Software "T" release: 12.1(1)T.

Class-Based Shaping

Description

Generic Traffic Shaping (GTS), when configured on an interface allows you to control the traffic leaving an interface in order to match its transmission to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Traffic adhering to a particular profile can be shaped to meet downstream requirement, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Prior to this release, when GTS queued packets that, when transmitted, caused the traffic flow to violate the configured rate, only flow-based WFQ was supported for the queued packets.

Using the Class-Based Shaping feature, class-based WFQ (CBWFQ) is supported for the queued packets. Using CBWFQ, it is possible to configure classes of queued traffic and provide relative or absolute bandwidth guarantees to those classes. Note that the relative or absolute bandwidth guarantees are with regard to the configured CIR.

You can specify two types of traffic shaping; average rate shaping and peak rate shaping. Average rate shaping limits the transmission rate to the committed information rate (CIR). Using the CIR ensures that the average amount of traffic being transmitted conforms to the rate expected by the network. Peak rate shaping allows the router to burst higher than average rage shaping. However, using peak rate shaping, the traffic transmitted above the CIR (the delta) has the potential of being dropped if the network becomes congested.

For detailed information, please refer to:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/clsbsshp.htm

Benefits

- Traditionally, GTS is configured with ACLs to specify the traffic to shape. Now, combining traffic classes with GTS yields a very powerful and versatile way to shape traffic. Along with access control lists, NBAR/DSCP can also be used to specify traffic for shaping.
- Since peak-rate shaping can now be performed on a class, more data than the CIR can be transmitted if physical bandwidth is available on the interface. This feature makes GTS more versatile.
- CBWFQ allows specification of the exact amount of bandwidth to be allocated for a specific class (that can be controlled by using GTS), and you can configure up to 64 classes. This powerful combination allows for a much more scalable solution, than WFQ/GTS by itself.

Platforms/Considerations

Routers	C160x, C25xx, C26xx, C36xx, C4x00, C7x00

First appearance in a Cisco IOS Software Release: 12.1(3) T.

Class-Based Marking

Description

This Cisco IOS Software release allows you to classify packets based on their DSCP (Differentiated Services Code Point / IP-precedence values within the type of service (TOS) field in the IP-header. Within each class, you can also set the outgoing packet's new DSCP/IP-precedence value.

Using DSCP/precedence based classification, a customer can specify various policies that need to be applied to various types of traffic. This also makes the Cisco QoS/packet marking and matching implementation compliant with the RFC 2474 definition of the differentiated services (DS) field, allowing users to define various per-hop behaviors (PHBs) based on the DSCP.

Benefits

- This feature enables you to classify and modify packets based on the DSCP/IP-precedence values in the IP header. Packets can be queued based on incoming DSCP/IP-precedence values, and colored to different values when moving on to the downstream network node.
- Users can define PHBs for various DSCP values. A packet can now be classified using its DSCP value, and given the appropriate priority, scheduling, and forwarding behavior at each hop along the path it takes. Toward this end, Low-Latency Queuing (LLQ) and Generic Traffic Shaping (GTS) are two of the techniques that can be used on a per-class basis.

Platforms/Considerations

Routers	C26xx, C36xx, C4x00, C7x00

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Distributed Low Latency Queuing

Description

The Low Latency Queuing (LLQ) feature brings strict priority queueing to Class-Based Weighted Fair Queuing (CBWFQ). Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without LLQ, CBWFQ provides Weighted Fair Queuing (WFQ) based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

This feature distributes LLQ functionality across multiple processors in a distributed processing system, such as the Versatile Interface Processor (VIP) on the Cisco 7500 series router and the Flexwan module for the Catalyst 6000 family. A distributed architecture ensures high packet throughput as network speeds and route complexities increase by moving the packet forwarding decisions and services from the central routing engine out to the network line cards.

See http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt2/qcdconmg.htm#xtocid2865024 for general information on Low-Latency Queuing.

And see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/llqvipe.htm for details on Distributed Low-Latency Queuing.

Benefits

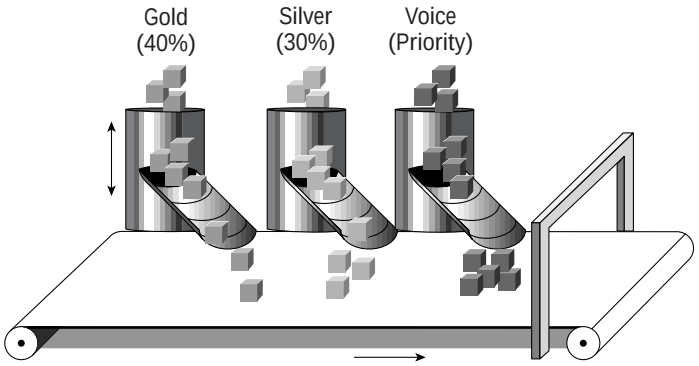
- Reduces latency of voice packets transported across the network, increasing voice quality
- Enables critical applications to be transported with high priority across the network
- Enables simultaneous transport of prioritized data using class-based queuing alongside voice and video traffic
- Provides high-capacity low-latency queuing by distributing the feature across multiple line cards

Platforms/Considerations

Routers	C7500
Catalyst Switches	Cat6000 Flexwan Module

First appearance in a Cisco IOS Software release: 12.0(5)XE.

Figure 11
Distributed Low-Latency Queuing enables the simultaneous transport of voice and prioritized data



Distributed Traffic Shaping

Description

The distributed Traffic Shaping (dTS) feature uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate, which ensures that traffic behaves in accordance with the configured descriptor.

This feature distributes traffic shaping functionality across multiple processors in a distributed processing system, such as the Versatile Interface Processor (VIP) on the Cisco 7500 series router and the Flexwan module for the Catalyst 6000 family. A distributed architecture ensures high packet throughput as network speeds and route complexities increase by moving the packet forwarding decisions and services from the central routing engine out to the network line cards.

Distributed traffic shaping (DTS) combines the benefits of GTS and Frame Relay traffic shaping (FRTS) into one tool. In networks where Distributed Cisco Express Forwarding is the preferred mode of switching, DTS is the logical choice for traffic shaping.

DTS configures traffic shaping at the interface level, subinterface level, or logical interface level for ATM/Frame Relay permanent virtual circuits (PVCs). Shaping can be based on the following criteria:

- All traffic on the physical or logical interface
- Traffic classified via simple and extended IP access control lists (ACLs) (IP addresses, TCP/UDP ports, IP Precedence)
- Traffic classified by QoS group (an internal packet label applied upstream by CAR or QPPB)

In a Frame Relay network, DTS recognizes the forward explicit congestion notification (FECN) and backward explicit congestion notification (BECN) bits to automatically adjusts the traffic descriptors

Unlike regular traffic shaping (GTS), DTS does not require that Weighted Fair Queuing (WFQ) be enabled. Instead DTS uses fair queuing or distributed first-in, first-out (FIFO) for the shaped queue.

Benefits

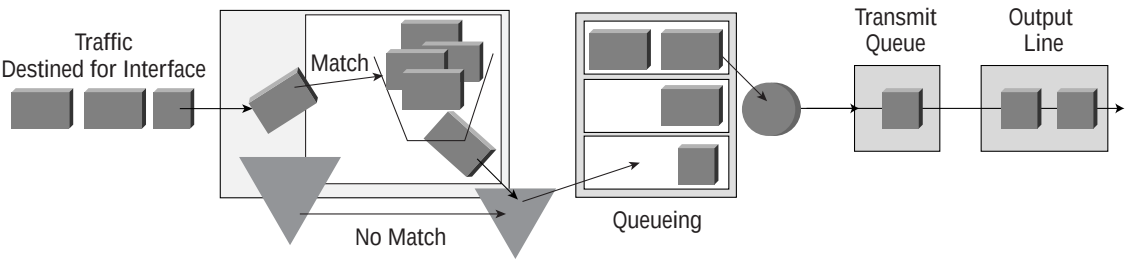
- The primary reasons to use traffic shaping are to control access to available bandwidth, ensure that traffic conforms to the policies established for it, and regulate the flow of traffic to avoid congestion when the sent traffic exceeds the access speed of its remote, target interface.
- Control access to bandwidth when, for example, policy dictates that the rate of a given interface should not on the average exceed a certain rate even though the access rate exceeds the speed.
- Configure traffic shaping on an interface if you have a network with differing access rates. Suppose that one end of the link in a Frame Relay network runs at 256 kbps and the other end of the link runs at 128 kbps. Sending packets at 256 kbps could cause failure of the applications using the link.
- Configure traffic shaping if you offer a subrate service. In this case, traffic shaping enables you to use the router to partition your T1 or T3 links into smaller channels.
- Configure traffic shaping in Frame Relay networks because the switch cannot determine which packets take precedence, and therefore which packets should be dropped when congestion occurs

Platforms/Considerations

Routers	C7500
Catalyst Switches	Cat6000 Flexwan

First appearance in a Cisco IOS Software release: 12.0(4)XE.

Figure 12
Distributed Traffic Shaping



Network-Based Application Recognition (NBAR)

Description

As IP quality-of-service (QoS) technology matures and customers begin QoS deployment in production networks, new requirements for packet classification have emerged. Today's applications require high performance to ensure competitiveness in an increasingly fast-paced business environment. Networks provide a variety of services to ensure that mission-critical applications receive the required bandwidth for high performance. Today's Internet-based client-server applications make it difficult for networks to identify and provide the proper level of control.

The Network-Based Application Recognition (NBAR) engine solves this problem by adding intelligent network classification to network infrastructures. NBAR is a new classification engine that recognizes a wide variety of applications, including Web-based and other difficult-to-classify protocols that utilize dynamic port assignments. When NBAR recognizes an application, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features such as:

- Guaranteed bandwidth for critical applications
- Bandwidth limits for noncritical applications
- Traffic shaping
- Packet coloring

Benefits

- Classification of applications that dynamically assign Transport Control Protocol/User Datagram Protocol (TCP/UDP) port numbers
- Classification of HTTP traffic by URL, HOST, or Multipurpose Internet Mail Extension (MIME) type
- Classification of application traffic using subport information
- A special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.
- Classification of Citrix ICA traffic by application name

Platforms/Considerations

Routers	C26xx, C36xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

RSVP Support for Frame Relay

Description

Queuing is useful to manage congestion on the interface or VC. In a Frame Relay environment, the congestion point may not be the interface itself, but the virtual circuit due to the CIR value. This means that fancy queuing must now run on the virtual circuit to provide the QoS guarantees for the traffic.

This feature allows RSVP to work with per VC queuing when traffic shaping is enabled in a Frame Relay environment, performing accurate admission control and reservation of resources at the congestion point, such as in the virtual circuit itself.

RSVP support for Frame Relay allows reservation of resources, such as queues and bandwidth in both Point-to-Point and Point-to-Multipoint configurations allowing better guarantees for reserved/high-priority traffic.

For more details on RSVP and queuing features refer to Cisco QoS configuration guide, Cisco IOS documentation.

Benefits

- Accurate admission control based on the virtual circuit CIR value as opposed to the interface bandwidth

- Better QoS guarantees for high-priority traffic by reservation of resources at the point of congestion, for example, VC as opposed to the interface
- Flexibility in configuration with support for both Point-to-Point and Point-to-Multipoint configuration, enabling deployment of services such as voice over IP (VoIP) in Frame Relay environments
- Extension of IP QoS features seamlessly from IP to Frame Relay environments

Platforms/Considerations

Routers	Cisco 7200 Series Cisco 7500/RSP Series Cisco 3810 Cisco 3600 Series Cisco 2600 Series Cisco 1700 Series

First appearance in a Cisco IOS Software release: 12.1(5)T.

Class Based Policer for the DiffServ AF PHB

Description

Class Based Weighted Fair Queuing (CBWFQ) in Cisco IOS Software is a powerful mechanism to carve out QoS policies across multiple traffic classes, using the Modular QoS CLI (MQC). It allows you to specify the amount of bandwidth allocated to each class, use Low Latency Queuing (LLQ) for strict priority traffic such as VoIP, and shape (smoothen out by buffering) traffic of other classes, among many other functionality.

This release adds to the MQC and CBWFQ by allowing you to police traffic within a class to specified parameters. In supporting the IETF standard for Differentiated Services (DiffServ), this policer conforms to RFC-2697, and allows you to implement the Assured Forwarding Per-Hop Behavior (AF PHB), defined in RFC-2597.

The policer is called a Single-Rate Three-Color Marker (srTCM), since the AF Drop-Precedence bits can be set based on the Committed Burst Size (CBS-Bc), and the Excess Burst Size (EBS - Be). Packets within an AF class can be marked with different drop-precedence bits, depending on (a) the current packet's size is less than or equal to the CBS (conform), (b) the current packet's size is between CBS and EBS (exceed), or (c) the current packet's size is greater than EBS (violate). In addition to coloring the packets with the drop-precedence bits, other actions such as marking the packet to another class (completely different DiffServ Code Point [DSCP]), transmitting, or dropping the packets may be performed.

Benefits

- The Class Based Policer allows you to fully implement the DiffServ-Compliant Assured Forwarding (AF) Per-Hop Behavior (PHB), and along with other MQC tools allows you to construct a DiffServ-Compliant network
- Policing a class with the conform, exceed, and violate actions (tricolor marker) allows you to simulate WRED-like (Weighted Random Early Detect) behavior for flows within the class, and reduce the chances of a multitude of TCP/UDP sessions being dropped in the presence of congestion.

- Class Based Shaping and Class Based Policing, combined with Class Based WRED complete the tool-chest for non strict-priority classes. These mechanisms can be used to implement the DiffServ AF PHB, as well as to perform Traffic Conditioning (policing or shaping).

Platforms/Considerations

Routers	C25xx, C26xx, C36xx, C4x00, C72xx, C75xx (RSP Only)

First appearance in a Cisco IOS Software release: 12.1(5) T.

Class Based QoS MIB

Description

Class Based Weighted Fair Queuing (CBWFQ) in Cisco IOS Software is a powerful mechanism to carve out QoS policies across multiple traffic classes, using the Modular QoS CLI (MQC). It allows you to specify the amount of bandwidth allocated to each class, use Low Latency Queuing (LLQ) for strict priority traffic such as VoIP, and shape (smoothen out by buffering) traffic of other classes, among many other functionality.

This release of the Cisco IOS Software introduces the Class Based QoS Management Information Base (MIB). The MIB, a database of relevant QoS counters serves as the basis for monitoring the MQC features using SNMP (Simple Network Management Protocol).

Using SNMP, the Class Based QoS MIB (abbreviated as CBQM) allows you to monitor traffic shaping, traffic policing, traffic queuing (CBWFQ), WRED (Weighted Random Early Detection), and NBAR (Network-Based Application Recognition) protocol-discovery, and generic traffic counters.

As an example, you can obtain incoming Packet & Byte Counts for a particular class, and Conformed & Exceeded Packet & Byte Counters for another class configured to be Policed on an outbound basis.

Benefits

- CBQM adds management support to the Modular QoS CLI features.
- Detailed information on each configured class, such as packets/sec and bytes/sec can be gleaned using the CBQM.
- Provisioned QoS, using the MQC can be improved upon, based on CBQM collected statistics.

Platforms/Considerations

Routers	C25xx, C26xx, C36xx, C4x00, C7x00, C75xx

First appearance in a Cisco IOS Software release: 12.1(5) T.

DiffServ Compliant WRED

Description

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destinations, indicating that congestion is cleared. This mechanism is highly useful to achieve better utilization of congested links and avoid the global synchronization problem associated with TCP traffic.

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher-priority traffic is delivered with a higher probability than lower-priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

This release of Cisco IOS Software allows you to configure WRED to look beyond the three IP precedence bits, and make decisions based on the DiffServ (Differentiated Services) Code Point (DSCP) field in the ToS (Type of Service) byte of the IPv4 header. Up to three drop precedence levels are defined with the AF (Assured Forwarding) PHB (Per-Hop Behavior) in DiffServ, using the two drop-precedence bits in the DSCP. WRED min and max drop-thresholds can now be configured based on the DSCP field. Thus, the AF PHB defined in RFC-2597 can be implemented using policing/shaping, and WRED.

Benefits

- WRED is no longer limited to the IP Precedence scheme. It can utilize all six bits of the DSCP field, to make a decision on packet drop probability.
- Using WRED in conjunction with the DSCP field allows for a full implementation of the drop-precedence scheme in the DiffServ AF PHB.
- Setting the minimum and maximum thresholds for each drop precedence level (by using the DSCP field) within an AF class allows for a finer degree of control/predictability in dropping packets of a particular AF Class during congestion.

Platforms/Considerations

Routers	C800, C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C72xx, C75xx (RSP only)

First appearance in a Cisco IOS Software release: 12.1(5) T.

Distributed cRTP

Description

Real Time Protocol (RTP) is the Internet-standard protocol for the transport of real-time data. It provides end-to-end network transport functions for applications that support audio, video, or simulation data over multicast or unicast network services.

RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification. The header portion of RTP is considerably large. The minimal 12 bytes of the RTP header, combined with 20

bytes of IP header and 8 bytes of UDP header create a 40-byte IP/UDP/RTP header. For compressed-payload audio applications, the RTP packet typically has a 20-byte to 160-byte payload. Given the size of the IP/UDP/RTP header combinations, it is inefficient to transmit the IP/UDP/RTP header without compressing it.

Cisco has supported Compressed Real Time Protocol (cRTP) since Cisco IOS Software Release 11.3. This version now extends the functionality to the versatile interface processor (VIP) cards on the 7500 series of routers (hereafter referred to as Distributed cRTP or dCRTP). Because of the ability to compress the IP/UDP/RTP header on each VIP card, the route switch processor (RSP) is no longer burdened with this task. dCRTP thus scales to support cRTP for large enterprise and service provider networks, with the 7500 series router acting as the aggregation point.

Benefits

- dCRTP on the 7500 series of routers offloads the IP/UDP/RTP header compression from the route switch processor (RSP), scaling it for other functionality
- dCRTP achieves scalability to support cRTP for large enterprise and service provider networks on a single 7500 series router acting as an aggregation point
- dCRTP allows for more VoIP streams to be supported, without any performance degradation on the RSP, due to compression of RTP packets

Platforms/Considerations

Routers	C75xx with Versatile Interface Processor (VIP) Cards

First appearance in a Cisco IOS Software release: 12.1(5) T.

QoS Device Manager

Description

Cisco IOS Software Release 12.1(5)T supports Cisco Quality of Service Device Manager (QDM) 2.0. QDM is a Web-based Java application that provides an easy-to-use graphical user interface to configure and monitor the advanced IP-based quality-of-service (QoS) functionality within Cisco routers. QDM is supported on the 7XXX, 2600, and 3600 Cisco router platforms.

The QDM application is stored in the Flash memory of the Cisco router, and it can be uploaded to any client workstation with proper Web browser and JAVA support. QDM runs as a JAVA application under a JAVA-enabled Web browser on the client workstation. Once the QDM application is uploaded to the client workstation, a user can both configure and monitor any of the advanced QoS features supported by Cisco IOS Software Release 12.1(5)T. The monitoring capability of QDM is particularly valuable, as it allows the user to easily observe a real-time graph of the bandwidth utilization by QoS traffic class based on the QoS configuration specified for each interface on the router.

For more information about QDM, please refer to the following CCO documents:
http://www.cisco.com/en/US/products/sw/netmgtsw/ps2063/index.html
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/index.htm

Benefits

- Greatly simplifies the configuration and monitoring of QoS features within Cisco IOS Software

- Allows rapid confirmation of the effectiveness of QoS configurations using the QoS monitoring capabilities

Platforms/Considerations

Routers	C26xx, C36xx, C7x00

First appearance in a Cisco IOS Software release: 12.1(1)E.

Reliability

PGM Host

Description

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers.

PGM router assist is a feature that allows Cisco routers to support the optimal operation of PGM. The PGM Reliable Transport Protocol is implemented on the customers' hosts.

PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. It is network-layer independent; the Cisco PGM router assist supports PGM over IP.

This feature uses a transport session identifier (TSI) that identifies a particular PGM session. This feature is based on the Internet draft PGM Reliable Transport Protocol Specification. The draft can be found at http://www.ietf.org/internet-drafts/draft-speakman-pgm-spec-03.txt.

Please access additional information on PGM support at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/pgmscale.htm

Benefits

- *Bandwidth Savings*—The PGM router assist feature saves bandwidth by substantially reducing the number of negative acknowledgments (NAKs) to the source and by constraining the retransmissions to only those receivers that experience data loss
- *Improved PGM Efficiency*—The PGM router assist feature is not absolutely required for hosts that implement PGM, but PGM operates optimally in conjunction with routers that have this feature enabled

Platforms/Considerations

Routers	Cisco 1600 series Cisco 2500 series Cisco 2600 series Cisco 3600 series Cisco 3800 series Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M) Cisco 7200 series Cisco 7500 series

First appearance in a Cisco IOS Software "T" release: 12.1(1)T.

Cisco 7500 Single Line Card Reload

Description

The Single Line Card Reload (SLCR) feature is the first of several high availability initiatives planned for the Cisco 7500. SLCR will enable the Cisco 7500 to isolate faults to a single line card, and also accelerate the recovery time of the overall system.

The benefits of SLCR are twofold: First, by isolating a fault to a single line card in the chassis, the rest of the system is free to continue forwarding traffic. The second benefit of SLCR is that line card recovery time is accelerated by more than a factor of 10, therefore dramatically improving mean time to restoration (MTTR).

The SLCR feature is disabled by default. To enable SLCR, the configuration command is:
service single-slot-reload-enable

Benefits

- *Greater System Availability*—Through fault isolation to a single line card, the rest of the system is free to continue forwarding traffic
- *Faster Recovery Time*—Recovery of line cards is accelerated by more than 10x due to both fault isolation and recovery path improvements resulting in dramatic mean time to restoration (MTTR) savings

Platforms/Considerations

Routers	All Cisco 7500 models

First appearance in a Cisco IOS Software release: 12.1(5)T.

Security

SSH Version 1 Server Support

Description

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

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

This feature was previously released on Cisco IOS Software version 12.0(5)s, see:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm

More information about SSH can be found at the SSH Frequently Asked Questions Web site:
http://www.employees.org/~satch/ssh/faq/ssh-faq.html

Benefits

- This feature provides a secure connection to a Cisco router

Platforms/Considerations

Routers	C17x0, C25xx, C26xx, C36xx, C4x00, C7x00

First appearance in a Cisco IOS Software “T” release: 12.1(1)T.

Preauthentication

Description

The Cisco IOS Software Preauthentication feature in a network access server provides the A-V pairs in authentication, authorization, and accounting (AAA) Remote Access Dial-In User Service (RADIUS) that enable user or user group preauthentication based on any combination of dialed-number identification string (DNIS), calling line identification (CLID), and call type. The supporting application must be running in a RADIUS server.

The ISDN interface between the public network switch and a network access server provides the DNIS or dialed number, CLID or calling party number, and the call type or bearer capability as part of the initial call setup message for each incoming call to the network access server (NAS) from the Public Switched Telephone Network (PSTN).

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

In the event the RADIUS server application becomes unavailable, a guard timer is set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without the authorization.

When preauthentication is used, an affirmative response from the RADIUS server may include vendor-specific attributes to provide a modem string for management of modem settings for the call. The modem parameters are minimum speed, maximum speed, modulation, error correction, and compression.

Benefits

- Preauthentication enables service providers to add Cisco dial ports to their existing networks and to manage the ports with the installed base of RADIUS server solutions.
- Preauthentication enables user authorization and user authentication prior to answering the call.

- Coupled with a preauthentication RADIUS server application, service providers can efficiently manage the use of shared resources to offer differing service-level agreements and oversubscription rates.

Platforms/Considerations

Access Servers (AS)	Cisco 5300 and 5800

First appearance in a Cisco IOS Software release: 12.1(2)T.

Preauthentication with ISDN PRI and Channel Associated Signaling

Description

With ISDN Primary Rate Interface (PRI) signaling and Channel Associated Signaling (CAS), information about an incoming call is available to the network access server (NAS) before the call is answered. The available call information includes the Dialed Number Identification Service (DNIS) number, the Calling line ID number (CLID), and the call type.

The Preauthentication with ISDN PRI and CAS feature in a network access server provides the A-V pairs to the AAA RADIUS server for determination-on the basis of the DNIS number, CLID number, or the call type-whether to answer an incoming call.

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

In the event the RADIUS server application becomes unavailable a guard timer is set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without authorization.

When preauthentication is used, an affirmative response from the RADIUS server may include vendor specific attributes to provide a modem string for management of modem settings for the call. The modem parameters are minimum speed, maximum speed, modulation, error correction, and compression.

Benefits

- The Preauthentication with ISDN PRI and CAS feature enables service providers to add Cisco dial ports to their existing networks and manage the ports with the installed base of RADIUS server solutions.
- Enables user authentication and authorization before a call is answered.
- Coupled with a preauthentication RADIUS server application, service providers can efficiently manage the use of shared resources to offer differing service level agreements and over-subscription rates.

Platforms/Considerations

Access Servers (AS)	5300, 5400, 5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Secure Shell Version 1 Integrated Client

Description

Secure Shell (SSH) protocol provides a secure connection between network devices. Two versions of SSH are available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS Software.

The SSH server feature has been in Cisco IOS Software since Release 12.1(1)T and it enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides an interface that is similar to an inbound Telnet connection. The SSH server in Cisco IOS Software will work with publicly and commercially available SSH clients. The SSH integrated client feature in 12.1(3)T will allow an SSH session to be initiated from a router to another router, or to any other device that supports an SSH server.

Before SSH, security was limited to Telnet security. SSH allows strong encryption to be used with Cisco IOS authentication to secure this channel. More information about SSH may be found at the Frequently Asked Questions site for SSH: http://www.employees.org/~satch/ssh/faq/ssh-faq.html

Benefits

- SSHv1 provides encryption of the remote terminal session so that it cannot be viewed by anyone observing the packets on the wire.
- An SSH server was implemented in Cisco IOS Software to allow for SSH sessions to be formed to the router from SSH clients workstations.
- An SSH client has been integrated into Cisco IOS Software Release 12.1(3)T to allow SSH sessions to be formed to other routers and/or to any other SSH server.

Platforms/Considerations

Routers	C17x0, C25xx, C26xx, C36xx, C4x00, and C7x00
Universal Broadband Routers (UBR) Multiservice Access Concentrator (MC)	UBR900, UBR7200

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Switching

Media Gateway Control Protocol for the Cisco AS 5300 Voice/Gateway

Description

The Media Gateway Control Protocol (MGCP) is protocol developed by the IETF that defines the call control protocol between call agents and gateways in a packet telephony system. The first release of MGCP allows the AS5300 to support trunking gateway functions. A trunking gateway provides the capability to interface to both the PSTN and the packet telephony network, allowing voice traffic to pass back and forth between the packet telephony network and the circuit-switched PSTN. Calls transported in the packet telephony network are transferred via RTP/UDP/IP.

Benefits

- A trunking gateway using MGCP allows integration of packet telephony networks and circuit-switched networks

- MGCP allows VoIP networks to be deployed by providing external call control capabilities that offer functionality once only possible within the closed interfaces of a monolithic circuit switch
- MGCP enables centralized call control within the packet telephony architecture, facilitating deployment in networks that require centralized OA&M
- MGCP is an open protocol and is part of the Cisco Open Packet Telephony strategy. As an open protocol, MGCP allows the operator to build best-of-breed solutions and prevents an operator from being locked into proprietary, single-vendor solutions

Platforms/Considerations

Access Servers (AS)	5300

First appearance in a Cisco IOS Software Release: 12.1(1)T

Voice

Cisco Signaling Link Terminal (SLT)

Description

The Cisco Signaling Link Terminal (SLT) is an integral part of the Cisco Signaling Controller SC2200 or the Cisco Virtual Switch Controller VSC3000 (VSC) architecture, acting as the interface between the SS7 network and Cisco SC or VSC node.

The Cisco SLT enables reliable transport of Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 SLT feature set to provide smooth interoperability with the Cisco Switching Controller or VSC. The SLT feature uses the Cisco Reliable User Datagram Protocol (RUDP) to backhaul, or transport, upper-layer SS7 protocols across an IP network, including:

- Message transfer part Level 3 (MTP 3)
- Integrated Services Digital Network User Part (ISUP)
- Signaling connection control part (SCCP)
- Transaction capabilities application part (TCAP)
- Advanced Intelligent Network (AIN)
- Intelligent network application part (INAP)

The SLT is responsible for terminating the MTP 1 and MTP 2 layers of the SS7 protocol stack. Accordingly, the SLT supports the following MTP Layer 1 and Layer 2 functions:

Layer 1 functions:

- Terminate up to two 64 or 56-kbps SS7 signaling links
- T1, E1, V.35, EIA/TIA-449, or EIA/TIA-530 physical interfaces to the SS7 network

Layer 2 functions:

- *Signal-unit delimitation*—Detecting individual signal units
- *Signal-unit alignment*—Enforcing signal-unit encoding rules and bit patterns
- *Error detection*—Detecting bit errors in signal units by using the cyclic-redundancy-check (CRC) field

- *Error correction*—Using positive and negative acknowledgments and retransmitting errored signal units
- *Link state control (LSC)*—Provides the overall coordination of the session
- *Initial Alignment Control (IAC)*—Provides the link alignment processing
- *Transmit control*—Provides transmit flow control and processing
- *Receive control*—Provides receive flow control and processing
- *Congestion control*—Provides congestion onset and abatement processing
- *Signal unit error rate monitor (SUERM)*—Provides monitoring of signal unit events
- *Alignment error rate monitor (AERM)*—Provides monitoring of link alignment errors.

Session Manager software manages the communication sessions between the SLT and the SC or VSC. When the SLT feature is used with a redundant pair of controllers, the Session Manager maintains separate communication sessions with each controller in the pair. The session between the SLT and the active controller transports the SS7 traffic, while the session between the SLT and the standby controller provides backup.

The Session Manager uses RUDP to communicate between the SLT and the controller. RUDP is a simple, connection-oriented, packet-based transport protocol that is Cisco proprietary and based on RFC 908 (Reliable Data Protocol) and RFC 1151 (Version 2 of the Reliable Data Protocol).

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.

Benefits

- *SS7 link termination on a high-availability platform*—SS7 network access and interconnection requires a high degree of reliability in the signaling links and associated equipment. The Cisco SLT provides the reliability of a dedicated signaling link termination device and maximizes the availability of the SS7 signaling links.
- *Distributed SS7 MTP processing*—Processor-intensive parts of the SS7 MTP2 are off-loaded from the SC or VSC to the SLT. This distributed MTP model allows the controller to better utilize its resources to provide optimal call control.
- *Call control*—Signaling backhaul provides a means for combining gateways into a virtual switch with the call control intelligence centralized in the SC or VSC system.
- *Standard physical interfaces*—Interconnection with SS7 network elements is supported using the following SS7 physical interface standards: T1, E1, V.35, EIA/TIA-449, and EIA/TIA-530
- *Drop and insert*—T1/E1 interface cards support the drop and insert feature (also called TDM cross connect), which allows individual T1/E1 channels to be transparently passed, uncompressed, between T1/E1 ports. This feature enables direct termination of SS7 F-links in T1 or E1 carriers, while the remaining bearer channels are passed on to a gateway device for processing

Platforms/Considerations

Routers	The Cisco SLT is supported only on the Cisco 2611 platform

First appearance in a Cisco IOS Software "T" release: 12.1(1)T.

VPN

Inter-Autonomous System for MPLS VPNs

Description

The inter-autonomous system (AS) feature extends the functionality of the Multiprotocol Label Switching (MPLS) virtual private network (VPN) to support interservice provider communication using external Border Gateway Protocol (EBGP) routing. This feature adds support for the exchange of IPv4 network layer reachability information (NLRI) as VPN-IPv4 addresses across autonomous system boundaries using external BGP (EBGP) routing. This means that MPLS VPN services may now span multiple VPN service providers running in separate autonomous systems (running under separate network administrations) or between multiple subautonomous systems (grouped as a confederation within a single service provider).

Through the inter-AS feature, the routes distributed by a border router to a peer router in the VPN include the proper sequence for label switching. The next-hop and MPLS labels are appropriately rewritten by each border edge router (see “Label Distribution Using EBGP Between Multiple Autonomous Systems” for background details).

With the feature Inter-AS MPLS VPNs, service providers can now jointly offer these VPN services seamlessly. With this feature, VPNs can start at one customer site and traverse a set of different service provider backbones before arriving at another site of the same customer. Previously, the VPN traversed only one (BGP AS) service provider backbone. In addition, service providers may engineer their backbones into BGP confederations to optimize IBGP meshing, and they can still offer MPLS VPNs across their backbones. VPN traversing multiple service providers is transparent to the end customer.

Benefits

- This feature allows an MPLS VPN to span multiple BGP autonomous systems.
- This enables smaller service providers to provide MPLS VPNs to customers who are geographically dispersed in areas that have no service providers.
- Service providers who have engineered their backbones into BGP confederations for optimization can now use this feature to provide MPLS BGP VPNs to end customers over their backbones.

Platforms/Consideration

Routers	C2600, C36xx, C4500, and C7x00

First appearance in a Cisco IOS Software release: 12.1(5)T.

Settlements for Packet Voice, Phase 2

Description

Packet telephony service providers interested in expanding their geographic coverage have been faced with limited options. To help alleviate this problem, Cisco has implemented the Open Settlements Protocol (OSP), a client server protocol defined by the European Telecommunications Standards Institute (ETSI) TIPHON standards organization. OSP allows service providers to exchange traffic with other service providers without establishing multiple bilateral peering agreements.

The clearinghouse provides route selection, call authorization, call accounting, and intercarrier settlements for member service providers. P-based clearinghouses provide least-cost and best-route selection algorithms based on a variety of parameters their subscriber carriers provide, including cost, quality, and specific carrier preferences.

Cisco IOS version 12.1(1)T has additional enhancement to allow the clearinghouses to provide roaming support to their subscribers. Subscribers may access the same affordable Internet telephony services when they roam outside of their home ITSP service area and into another ITSP that belongs to the same clearinghouse service.

This new solution is available on the Cisco AS5300 access server/ voice gateway, the Cisco AccessPath VS3/ voice gateway, the Cisco 3600 series, and the Cisco 2600 series using Cisco IOS Software.

This feature also works in conjunction with prepaid calling.

Benefits

- End-to-end Voice over IP (VoIP) support
- Cost-effective worldwide calling coverage
- Guaranteed settlement of authorized calls
- Incremental revenue increase by terminating calls from other service providers
- Simplified business and credit relationships
- Outsourced complex rating and routing tables
- Flexibility in selecting appropriate termination points
- Secure transmission using widely accepted encryption for sensitive data
- Roaming-same services when traveling outside of home areas

Platforms/Considerations

Access Servers (AS)	AS5300, 36xx, 26xx

First appearance in a Cisco IOS Software “T” release: 12.1(1)T.

H.323 Version 2 Support Phase 2

Description

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS® software by adding several optional features of the H.323 Version 2 specification:

- *H.323v2 fast connect*—The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened.
- *H.245 tunneling*—Through H.245 tunneling, H.245 messages are encapsulated within Q.931 messages without using a separate H.245 TCP connection.
- *H.450.2 call transfer*—Call transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco gateways support H.450.2 call transfer as the transferred and transferred-to party.
- *H.450.3 call deflection*—Call deflection is a feature under H.450.3 call diversion (call forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 call deflection as the originating, deflecting, and deflected-to gateway.
- *Hookflash relay*—A “hookflash” indication is a brief on-hook condition during a call. In H.323 Version 2 Phase 2, a foreign exchange station (FXS) hookflash relay is generated only if the following two conditions are met:

  - The other endpoint must support the reception of an H.245 hookflash and advertise this using the “receive User Input Capability” message during H.345 capabilities exchange;
  - The call must be established with either the “H345-alpha” or “h345-signal” variant of dtmf-relay.
- *H.235 security*—Security for RAS signaling between H.323 endpoints and gatekeepers is enhanced by including secure endpoint registration of the Cisco gateway to the Cisco gatekeeper and secure per-call authentication.
- *Gateway support for alternate endpoints*—The alternate endpoint feature allows a gatekeeper to specify alternative destinations for a call when queried with an admission request (ARQ) by an originating gateway.
- *Gateway support for a network-based billing number*—This feature informs the gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway.

Benefits

- H.323v2 fast connect and H.345 tunneling allow faster call connection times by reducing the number of transactions needed to establish a call.
- H.450.2 call transfer without consultation and H.450.3 call deflection provide a limited subset of features to support Internet call waiting.
- H.235 security allows only duly authorized and authenticated gateways to access gatekeeper resources.
- Translation of FXS hookflash to H.245 user input plus translation of H.245 user input to foreign exchange office (FXO) hookflash provides end-to-end hookflash relay in FXS-to-FXO configurations.
- Gateway support for the alternate endpoint field in the Advanced Communications Function (ACF) allows third-party gatekeepers to provide more robust call establishment.
- Gateway support for a network-based billing number on a per-interface basis allows third-party gatekeepers to obtain per-call interface usage information for billing or other purposes.

Platforms/Considerations

The gatekeeper and proxy features apply to the following platforms:

Routers	Catalyst 25xx, C26xx, C36xx
Multiservice Access Concentrator (MC)	MC3810

The gateway features apply to the following platforms:

Routers	Catalyst 26xx, 36xx
Access Servers (AS)	Cisco 5300

First appearance is a Cisco IOS Software release: 12.1(1)T.

VoATM, digital VoFR, and T1/E1 QSIG voice on Cisco 2600 and 3600, VoIP on Cisco 3810, and voice feature parity between Cisco 2600, 3600 and 3810

Description

High-Density Voice Network Module (E1 and T1 voice/fax support)

- Supports one or two E1 or T1 interfaces for connections to private branch exchanges (PBXs) and/or the Public Switched Telephone Network (PSTN)
- Uses Voice WAN interface cards (VWICs) to supply physical interface:
  - VWIC-1MFT-E1
  - VWIC-2MFT-E1-DI
- T1 CAS or QSIG signaling only
- E1 ISDN Primary Rate Interface (PRI) QSIG signaling only (requires Cisco IOS Release 12.0(7)XK1 or 12.1(2)T)
- Each PVDM-12 contains three TI 549 digital signal processors (DSPs)
- Supports up to 60 voice calls using a low-complexity coder/decoder (codec) (G.711, G.729a/b, G.726, fax)
- Supports up to 30 voice calls using a high-complexity codec (G.729, G.728, G.723.1)
- PVDM-12 fits into single-in-line memory module (SIMM) sockets on the NM-1HDV network module
- Five PVDM SIMM sockets on the NM-1HDV network module

New Software Features in Release 12.1(2)T

The following software features are available for the Cisco 3600 series in Cisco IOS Release 12.1(2)T.

Voice over ATM on Cisco 3600 Routers

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

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

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

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

Voice over IP on Cisco MC3810

Voice over IP (VoIP) on Cisco MC3810 multiservice router extends support for VoIP, previously available only on the Cisco 2600 and 3600, to the Cisco MC3810 multiservice router. VoIP enables a Cisco MC3810 multiservice router to carry voice traffic (for example, telephone calls and faxes) over an IP network.

Voice-Port Testing Enhancements

New voice-port testing commands force voice ports into specific states for testing:

- Testing detector-related functions
- Loopback tests
- Tone injection tests
- Testing relay-related functions
- Fax/voice mode tests

Voice-Port Enhancements

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

Configuring permanent connection options—Configure a voice-port connection mode and destination telephone number for permanent connections. This feature was unified across the Cisco MC3810, 2600, and 3600 platforms in Cisco IOS Release 12.0(7)XK1 and 12.1(2)T.

Configuring ring cadence—Specify on and off times for ringing pulses on an foreign exchange station (FXS) voice port. The ability to specify ring cadence is a new feature on the Cisco 2600 and 3600 platforms, and the syntax for configuring the ring cadence is new in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T.

Configuring auto-cut-through options—Disable or enable the auto-cut-through feature on ear and mouth (E&M) voice ports. When enabled, this feature makes call completion possible when a PBX does not provide an M-lead response. This feature is enabled by default on E&M voice ports. This is a new feature on the Cisco 2600 and 3600 platforms in Cisco IOS Release 12.0(7)XK.

Configuring E&M signaling bit functioning—Modify the functioning of transmit and receive signaling bits for E&M and E&M MELCAS voice signaling. These are new features on the Cisco 2600 and 3600 platforms in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T.

Manipulating signaling bits—Force individual transmit and receive signaling bit states on any voice port type. This is a new feature on the Cisco 2600 and 3600 platforms in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T.

Configuring disconnect acknowledgment—Configure an FXS or FXS MELCAS voice port to return an acknowledgment upon receipt of a disconnect signal. This is a new feature on the Cisco 2600 and 3600 platforms in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T.

Configuring playout delay—This feature enables the tuning of the playout buffer to accommodate packet jitter caused by switches in the WAN. This is a new feature on the Cisco 2600 and 3600 platforms in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T.

Configuring voice-port timing characteristics—Change various timing characteristics on voice ports, including:

- Configuring guard-out time on FXO voice ports
- Changing the timing percent break of dialing pulses
- Changing the ringing timeout on a voice port
- Changing the wait release delay on a voice port
- Configuring the Voice Activity Detection (VAD) silence detection time

These are new features on the Cisco 2600 and 3600 platforms in Cisco IOS Release 12.0(7)XK1 and 12.1(2)T.

Using voice-related show commands—These commands have enhanced functionality on the Cisco 2600 and 3600 platforms in Cisco IOS Releases 12.0(7)XK1 and 12.1(2)T:

- Displaying voice port information
- Displaying voice call information
- Displaying voice channel DSP information
- Displaying the active voice call table

- Displaying the voice call history table

Battery polarity reversal for FXS and foreign exchange office (FXO) voice interfaces provides the ability to signal supervisory disconnect (and other features) to (using the VIC-2FXS) or from (using the VIC-2FXO-M1 or VIC-2FXO-M2) a PBX, key system, or the PSTN.

QSIG Protocol Support on Cisco MC3810, 7200, 2600, and 3600 Series Routers

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

The Cisco voice packet network appears to the traditional QSIG PBXs as a distributed transit PBX that can establish calls to any PBX, non-QSIG PBX, or other telephony endpoint served by a Cisco gateway, including non-QSIG endpoints. When originating and terminating on QSIG endpoints, the QSIG messages are passed transparently across the network; the PBXs are responsible for processing and provisioning the supplementary services. When linking QSIG and non-QSIG endpoints served by a Cisco packet voice gateway, only basic calls are supported. In addition, all switched voice connections must be established and torn down in response to QSIG control messages.

QSIG support includes the following capabilities:

- Enables digit forwarding on plain old telephone service (POTS) dial peers
- On Cisco 3600 series routers, enables QSIG-switched calls VoFR, VoIP, and VoATM for T1/E1 and Basic Rate Interface (BRI) voice interface cards (NM-HDV and VIC-2BRI-S/T-TE)
- On Cisco 2600 series routers, enables QSIG-switched calls over VoFR and VoIP for T1/E1 and BRI voice interface cards (NM-HDV and VIC-2BRI-S/T-TE)
- On Cisco 7200 series routers, enables QSIG-switched calls over VoFR and VoIP on T1/E1 voice interface cards
- On Cisco MC3810, enables T1 or E1 Primary Rate Interface (PRI) and BRI QSIG-switched calls over VoFR, VoIP, and VoATM for Cisco MC3810 digital voice modules (DVMs) and BRI voice module (BVM); QSIG support on the Cisco MC3810 was introduced in Cisco IOS Release 12.0(2)T

Benefits

- Provides enterprises with the ability to place voice and fax traffic on to their data networks using standardized QSIG signaling
- Allows enterprises to take advantage of telephony toll-bypass
- Provides E1 voice connectivity to the PSTN for off-net telephony and fax calls
- Provides enterprises with the option to deliver VoIP, VoATM, or VoFR
- Allows users to utilize battery polarity reversal for supervisory disconnect on FXO and FXS voice interfaces

Platforms/Considerations

Routers	Cisco 26xx and Cisco 36xx
Multiservice Access Concentrator (MC)	Cisco MC3810

First appearance in a Cisco IOS Software release: 12.0(7)XK1.

Caveats—Limitations and Restrictions

Cisco IOS Release 12.1(2)T contains the following limitations and restrictions. Unless otherwise indicated, these limitations and restrictions apply to all previous software releases as well.

Voice over ATM on Cisco 3600 Routers

VoATM on the Cisco 3600 series requires one of the following modules to be installed:

- Multiport T1/E1 ATM network module with IMA—The multiport T1/E1 ATM network module with IMA supports up to 8 T1/E1 lines. For more information, see the Cisco IOS Release 12.0(5)T online document “Configuring Multiport T1/E1 ATM Network Modules with Inverse Multiplexing over ATM on Cisco 2600 and 3600 Series Routers.”
- OC-3 ATM network module—The OC-3 ATM network module supports one OC-3 line. For more information about the digital T1/E1 packet voice trunk network modules, see the Cisco IOS Release 12.0(3)T online document “ATM OC-3 Network Module for the Cisco 3600 Series Routers.”

Voice over ATM on the Cisco 3600 series supports ATM encapsulation ATM Adaptation Layer 5 (AAL5) only. AAL2 is not supported.

Voice over ATM switched virtual circuits (SVCs) are not supported in this release.

Voice over ATM is not supported on the Cisco 2600 series multiservice routers.

Voice over Frame Relay

The Cisco 2600 series and 3600 series routers cannot terminate calls initiated by a Cisco MC3810 using VoFR implementations prior to Cisco IOS Release 12.0(3)XG or 12.0(4)T.

Cisco MC3810 concentrators running Cisco IOS releases prior to 12.0(3)XG or 12.0(4)T cannot tandem VoFR calls from Cisco 2600, 3600, or 7200 series routers.

It is currently not possible to translate from the VoIP transport protocol to other protocols such as VoFR. As a result, a call coming in on a VoIP connection might not be (tandem) switched to a VoFR connection.

Hookflash for dial-tone recall from the router is not supported. However, the router can pass-through hookflash on FXO/FXS permanent connections using the [connection trunk voice-port configuration] command.

Note: Caution; VoATM SVCs were first supported on the Cisco MC3810 in Cisco IOS Releases 12.0(5)XK and 12.0(7)T. If upgrading a Cisco MC3810 from Cisco IOS Release 12.0(5)XK or 12.0(7)T to this release to obtain VoFR improvements, you will lose support for your VoATM SVCs.

Voice over ATM with AAL2 Trunking

Description

Voice telephony over ATM (VtoA), ATM Adaption Layer 2 (AAL2), provides a standards-based, bandwidth-efficient transport mechanism to carry voice, voice-band data, circuit mode data, frame mode data, and fax traffic over ATM infrastructures. This voice transport supports both compressed voice and noncompressed voice together with silence suppression for flexibility in meeting the requirements of varying environments.

The AAL2 trunking function provided on the MC3810 in Release 12.1(2)T complies with the ATM forum standard str-vtoa-lltaat2-1.0 spec. The capability utilizes the residential gateway function in the simple gateway control protocol (SGCP) model to meet the service provider market requirement.

The voice signaling termination, call routing, and customer billing functions may be handled either internally by the MC3810, or by an external call control function (Call Agent), that uses the SGCP to control the MC3810 routers.

Benefits

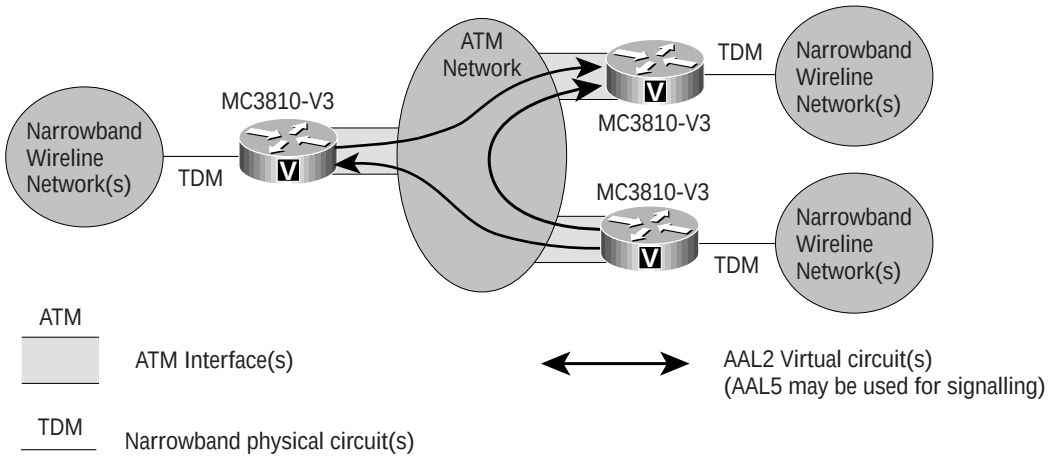
- VtoA AAL2 provides improved bandwidth optimization and lower delay, that equates to high voice quality.
- VtoA AAL2 offers flexibility; support can be provided either internally or by an external call agent; voice can be compressed or uncompressed.
- Standards-based compressed voice provides interoperability.
- VtoA AAL2 is a robust ATM architecture with inherent Quality of Service (QoS).

Platforms/Considerations

Multiservice Access Concentrator (MC)	Cisco MC3810

First appearance in a Cisco IOS Software release: 12.1(2)T.

Figure 13
The networks at the narrowband side depicted below, may be PBXs, key systems, analog telephones, or a public or private network of switch



VoFR/VoIP/VoATM feature parity for 26XX,36XX and 3810

Description

Release 12.1(2)T provides VoIP, VoATM and VoFR feature parity on Cisco's award winning multiservice access routers, the Cisco 2600, Cisco 3600 and Cisco MC3810. The introduction of common software to power these flexible routers provides unparalleled end-to-end voice capabilities in the networking industry.

The 12.1(2)T release introduces standards based H.323 VoIP support for the Cisco MC3810. The Cisco MC3810 joins a complete portfolio of VoIP enabled routers from Cisco including the Cisco 1750, 2600, 3600, and 7200 series. In the 12.1(2)T release, additional Quality of Service (QoS) mechanisms including IP RTP Priority, per queue weighted fair queuing, and compressed RTP (cRTP), are added to the multiservice access routers to insure the highest level of voice quality delivered.

With Release 12.1(2)T the Cisco 3600 joins the MC3810 by providing VoATM (AAL5) on the Cisco 3600 series IMA (Inverse Multiplex over ATM) and OC-3 interfaces. The MC3810 supports VoATM on a T1/E1 interface. With this feature the Cisco 3600 is the logical solution for providing ATM aggregation in a VoATM—AAL5 network. ATM provides inherent QoS for voice and other multimedia network traffic.

The MC3810, Cisco 2600 and Cisco 3600 have, for sometime, supported standards based VoFR through the implementation of FRF.11 and FRF.12. Cisco IOS Software release 12.1(2)T now provides this same standards based technologies on all of T1/E1 interfaces offered for these products. The introduction of this feature further enhances interoperability and flexibility and choices.

Benefits

- Increased QoS is provided for VoIP by providing IP RTP Priority, per queue weighted fair queuing, and cRTP
- Greater flexibility in service choices as the Cisco MC3810, 2600, and 3600 all support VoIP, VoATM and VoFR on a large range of analog and digital voice interfaces.
- Ease of management—a common code base and set of CLI means that management and administration is simplified. Dial plan, call progress tones, fxo/fxs disconnect supervision, and signaling enhancements are also provided in this release

Platforms/Considerations

Routers	Cisco 26xx and Cisco 36xx
Multiservice Access Concentrator (MC)	Cisco MC3810

First appearance in a Cisco IOS Software release: 12.1(2)T.

Caller ID on 2600, 3600 and MC3810

Description

Caller ID on analog voice interfaces provides the ability to receive caller ID over analog voice FXO interfaces and transmit caller ID over analog FXS interfaces. This features is supported only on the 2600, 3600, and MC3810 platforms and not on other Cisco platforms using these voice interfaces.

Benefits

- Support for end-to-end caller ID support across VoIP, VoFR, or VoATM
- Ability to connect to existing analog phones supporting caller ID
- Ability to receive caller ID information over FXO connections to the PSTN

Platforms/Considerations

Routers	C26xx, C36xx,
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(2a)XH.

Media Gateway Control Protocol Residential Gateway Support

Description

The Media Gateway Control Protocol (MGCP) is protocol developed by the IETF that defines the call control protocol between call agents and gateways in a packet telephony system. Previous Cisco IOS Software releases introduced support of trunking gateway (TGW). This release introduces support of residential gateway (RGW), a generic term referring to customer premise equipment that provides connectivity to the packet telephony system, in addition to POTs connections via a FXS interface. For this release, RGW is supported on the Cisco uBR924 and 2600 series.

The supplementary services supported on the uBR924 include call waiting, CLID, call forward, and distinctive ringing. The 2600 supports call waiting only.

Previously, the only TGW supported was the 5300. This release expands support for TGW to include the 3660.

Note: This feature introduces supplementary service support on the gateway only. An MGCP solution delivering supplementary services requires corresponding support on the call agent.

Benefits

- Allows services providers to offer both basic POTs and supplementary services via a call agent architecture based on the MGCP protocol.
- By providing RGW and TGW capability on a standardized protocol, it allows service providers to build multivendor, best-of-breed packet telephony networks.
- Enables basic integrated access solutions via RGW on the 2600.
- Enables basic cable telephony solutions via RGW on the uBR924.
- Expands TGW deployment options by introducing TGW on the 3660.

Platforms/Considerations

Routers	C26xx (RGW), C36xx (TGW)
Universal Broadband Routers (UBR)	UBR924 (RGW)
Access Servers (AS)	5300 (TGW)

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Modem PassThrough over Voice over IP

Description

VoIP modem passthrough transports modem-over-packet networks using PCM-encoded packets. This feature disables the following voice processing functions while the modem is being transported-compression, echo cancellation, high-pass filter, and voice activity detection. Also, redundancy is enabled to help protect against random packet drops. VoIP modem passthrough requires a relatively low packet loss rate in order to prevent modem retrains and call termination. Refer to the VoIP modem passthrough documentation for suitable network characterizations.

VoIP modem passthrough:

- Detects modems at speeds up to V.90
- When modem is detected, both the ingress and egress gateway roll over to G.711
- Optional payload redundancy

Benefits

The VoIP modem passthrough feature completes the wholesale VoIP solution-bearer channel transparency for all types of telephony traffic.

VoIP modem passthrough offers the following benefits:

- Detects modem speeds up to V.90
- Passes mode over a wide area network (WAN)
- Performs switchover to pass mode traffic on a bearer channel

Platforms/Considerations

Access Servers (AS)	5300

First appearance in a Cisco IOS Software release: 12.1(3)T.

Interworking Signaling Enhancements for H.323 and SIP VoIP

Description

The Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) and specified in RFC 2543 Version 2.0. SIP is an application layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. This feature allows the Cisco IOS gateway to be configured as a SIP user agent in accordance with the Session Initiation Protocol RFC 2543 Version 2.0. This feature provides enhancements to the initial Cisco IOS SIP implementation introduced in 12.1 (1) T.

Key features in this release include the ability to support interaction with SIP proxies, call hold, call redirection (transfer), configurable SIP timers, interoperability with DNS servers to look up SIP URLs, support of a variety of signaling protocols such as ISDN PRI and CAS, analog and digital interfaces, and integration with many Cisco IOS billing and security features.

Additional information on the Cisco IOS SIP implementation, including call flows and a SIP Protocol Compliance Table can be found at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtsipgv2.htm

Benefits

The SIP feature enhancements enable SIP gateways to:

- Enable Cisco voice-enabled platforms to provide RFC 2543 compliant user-agent client gateways
- Support proxy-routed calls
- Redirect an unaswered call to another SIP gateway or SIP-enabled IP phone
- Support call hold and call transfer service
- Hide the calling party identity based on the ISDN presentation indicator

Platforms/Considerations

Access Servers	Cisco AS5300
Series Routers	Cisco 2600
Series Routers	Cisco 3600

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Hoot'n Holler over IP

Description

Traditionally, Hoot'n Holler has been used in various industries as a means to provide a one-to-many or many-to-many conferencing service for voice communications, using point-to-point telco circuits and a Hoot'n Holler bridging/mixing functionality provided either by the customer or as a service of the PSTN carrier. The most common usage of Hoot' n Holler is a broadcast audio network that is used throughout the brokerage industry. All users can talk simultaneously with each other, but more commonly a broker in a field office will shout an order to the trading floor, and a floor trader will confirm the transaction.

With the Hoot'n Holler over IP feature, this functionality can be implemented using Cisco VoIP technology, leveraging voice, quality of service (QoS) and IP multicasting technologies. Four-wire E&M lines (either analog or via T1 connections) are used to obtain continuous VoIP connections across a packet network through the connection trunk mechanism. By using the inherent point-to-multipoint nature of IP multicasting, the routers can take several inbound voice streams from the traditional Hoot devices, and forward the packetized voice over the IP network to all parties within a defined Hoot' n Holler group.

Benefits

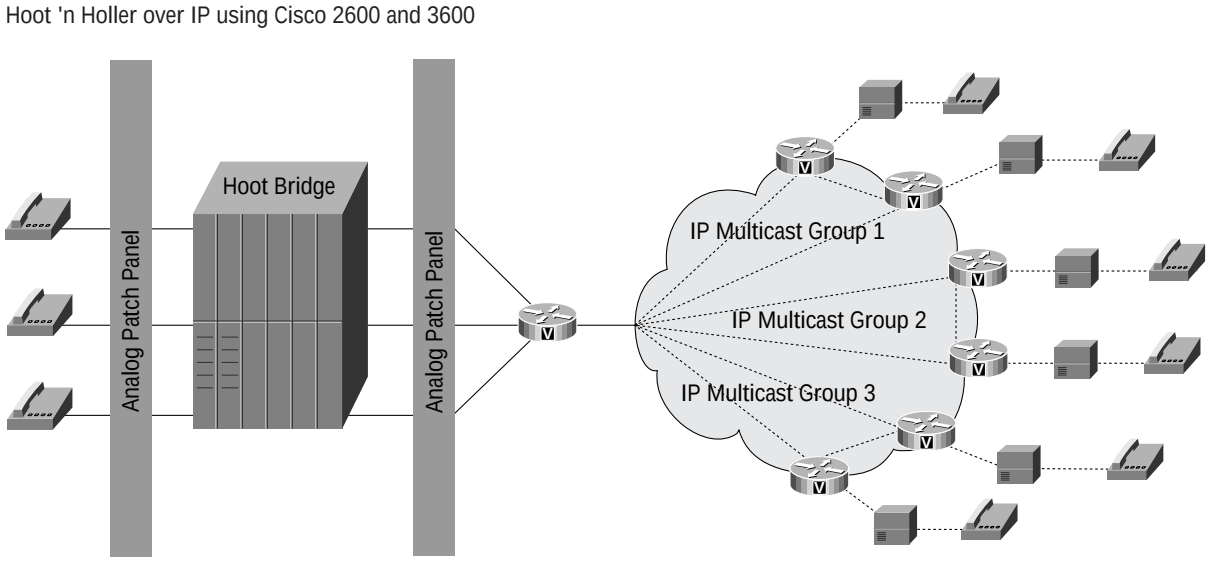
- Eliminate multidrop circuit expense
- Eliminate hoot-bridge expense (DSPs perform mixing of audio channels)
- Improve manageability
- Leverage existing multiservice networks
- Transparent to end users (traders)
- Move towards open, standards-based architecture
- Integrate new applications such as IP phones, IP turrets, high fidelity codecs (G.722), dial-in hoot, hoot-to-home and multicast clients

Platforms/Considerations

Routers	C26xx, C36xx

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Figure 14
Hoot'n Holler over IP using Cisco 2600 and 3600



Dial Peer Enhancements for Cisco AS5800 Access Server H.323 VoIP Gateways

Description

The AS5800/Voice Gateway Service Enhancement project is designed to add services and functionality for H.323-related applications. This project complemented with the SC2200 support for SS7 signaling in VoIP applications, enables carriers and service providers to deploy a wide range of packet telephony services with the AS5800/voice gateway.

Some of the new features added in this release are:

- Support for R2, FG-D (EANA) and NFAS signaling
- Debit card, Internet call waiting, and click-to-dial applications
- Support for the Open Settlements Protocol (OSP) applications
- H.323 V3 including Annexes E and G.

Benefits

- Higher Reliability-with the call denial feature, calls are denied under stressful network conditions without service disruption.
- Increased Revenues-by deploying and offering additional and lucrative packet telephony services such as debit card, Internet call waiting, and click-to-dial applications, carriers and service providers can differentiate themselves from the competition and increase their revenue.
- Higher Level of Interoperability-enhanced signaling functionality makes the AS5800/voice gateway compatible with a broad range of central office (R2, FG-D, NFAS) and packet telephony (H.323 V3) signaling environments.

Platforms/Considerations

Access Servers (AS)	5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Support for Cisco CallManager

Description

This is a special Cisco IOS release supporting the VG200 VoIP gateway.

The Cisco VG200 is designed to provide easy integration between voice over IP (VoIP) network resources, especially the Cisco IP telephony solution, and the public switched telephone system (PSTN). The current release of the Cisco VG200 gateways provides the following main features:

- 10/100Base-T Ethernet connection for connecting to VoIP network resources
- Support for one-slot or two-slot analog or digital voice network modules, useable with the Foreign Exchange Station (FXS), Foreign Exchange Office (FX0), and T1 voice interface cards (VICs).
- Support for the Media Gateway Control Protocol (MGCP) when used with the analog voice network module and Cisco CallManager Release 3.0 or other MGCP call agents.
- Support for the H.323 standard when used with the digital voice network module and H.323 end points.

Benefits

- This release enables deployment of the VG200 voice gateway, a simple, standalone gateway for use with IP telephony applications.
- MGCP protocol support allows the CallManager server to assume state control on a per-port basis, enabling VG200 connections to legacy voice mail systems.
- CallManager failover support detects when a CallManager is unreachable and automatically registers with a backup CallManager. Graceful revert switching allows the gateway to resume connection to the primary CallManager when it returns.
- Support for H.323v2 VoIP gateway protocols allows the VG200 to operate in a peer-to-peer H.323 VoIP gateway in other applications.
- Both analog (FXS and FXO) and Digital (T1-CAS) connections are supported, providing maximum flexibility in configuration.

Platforms/Considerations

VG200 Voice Gateway
Cisco IOS Software Version 12.1(1)XE only runs on a VG200 voice gateway. The VG200 cannot run any other software, nor can this software be run on any other device. However, features from this release will be rolled into Cisco IOS Version 12.1(3)T later, which will then support the 2600 and 3600 routers.

PSTN Fallback

Description

PSTN Fallback provides a measurement-based call admissions control mechanism to monitor congestion in the IP network and either redirect or reject calls when network congestion is detected and exceeds configured thresholds. This feature uses RTR (Response Time Reporter) probes to IP destinations to monitor the delay and loss characteristics of the network. ICPIF (ITU G.113) values are calculated and thresholds can be configured to redirect or reject calls.

A cache of “current” VoIP destinations is kept and probes are sent at configurable intervals to monitor these destinations. When calls to a cached destination cease, the entry is removed from the cache. If a call is set up to a destination that does not exist in the cache, a new probe is started.

Preference dial-peers can be used to:

- Redirect a call to an alternate IP destination
- Redirect a call to the PSTN using a trunk on the GW
- Reject a call to PBX/PSTN (BRI/PRI/QSIG)
- Hairpin a call to PBX/PSTN (analog and CAS protocols)
- Reject the call with reorder tone

This feature does not do bandwidth reservation for the call, nor measure available bandwidth in the network. It is a congestion detection method to trigger Call Admissions Control.

Benefits

- Provides a measurement-based call admission control mechanism by detecting IP congestion in the network

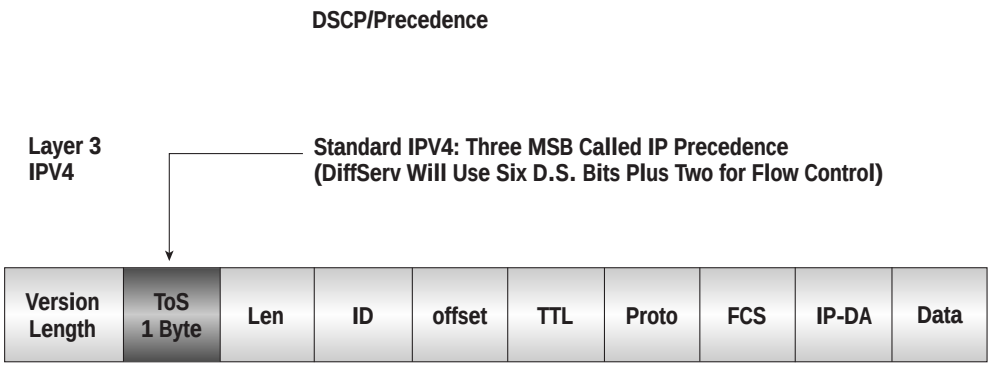
- It is a ping-like mechanism, but is secure, and mimics voice packets in terms of size, protocol and QoS treatment
- Allows adjustable thresholds and probe intervals
- A call is automatically redirected or rejected when the IP network is congested at the time of the call setup
- Threshold values for IP destinations are cached (a new call does not have to wait for probe results before it is admitted
- Uses ITU G.113 to gauge network transmission impairments

Platforms/Considerations

Routers	C26xx, C36xx,
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(3)T.

Figure 15
DSCP/Precedence.



Advanced Voice Busyout Monitor (AVBO)

Description

The Advanced Voice Busyout (AVBO) feature expands the Local Voice Busyout (LVBO) feature introduced in an earlier release.

LVBO provides a way to busy out a voice port or DS0 group (timeslot) based on a monitored local network interface (or interfaces) on the platform. The PBX can then attempt to select an alternate route.

AVBO adds to this functionality the ability to monitor network congestion to remote IP destinations and to busy out selected voice interfaces based on the results. Service Assurance Agent (SAA) probes are sent periodically to IP destinations, and if the returned values exceed the configured thresholds, the voice interface will be busied out.

Benefits

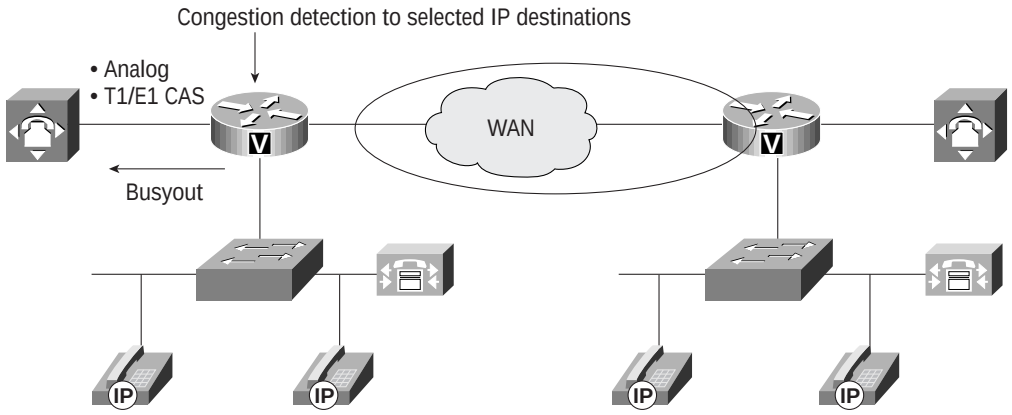
- Increases the available voice busyout triggering conditions

Platforms/Considerations

Routers	C26xx, C36xx
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(3)T.

Figure 16
Advanced Busy-Out Monitor (AVBO).



Trunk Conditioning for FRF.11 and Cisco Trunks

Description

Trunk conditioning is applicable to permanent point-to-point voice connections (Cisco “connection trunk” configurations), and provides the capability to busy out a voice port interfacing with a local PBX if a network PVC or trunk is down or out of service (OOS). This feature applies to analog telephony connections and digital T1/E1 using CAS “ABCD” signaling.

An OOS condition to a PBX can be signaled using an ABCD bit pattern that may be different from the busy or seized state. This allows the PBX to differentiate between OOS and congestion (all circuits in use) if the PBX supports this functionality.

Benefits

- Enables busy out or OOS signaling to a PBX if the network connection to the destination fails on an IP, Frame Relay, or Asynchronous Transfer Mode (ATM) network.
- Enables permanent connection configurations to provide fault indication (OOS) to the PBX so that it can select an alternate path to route calls.
- Enables detection of OOS conditioning applied by the PBX.

Platforms/Considerations

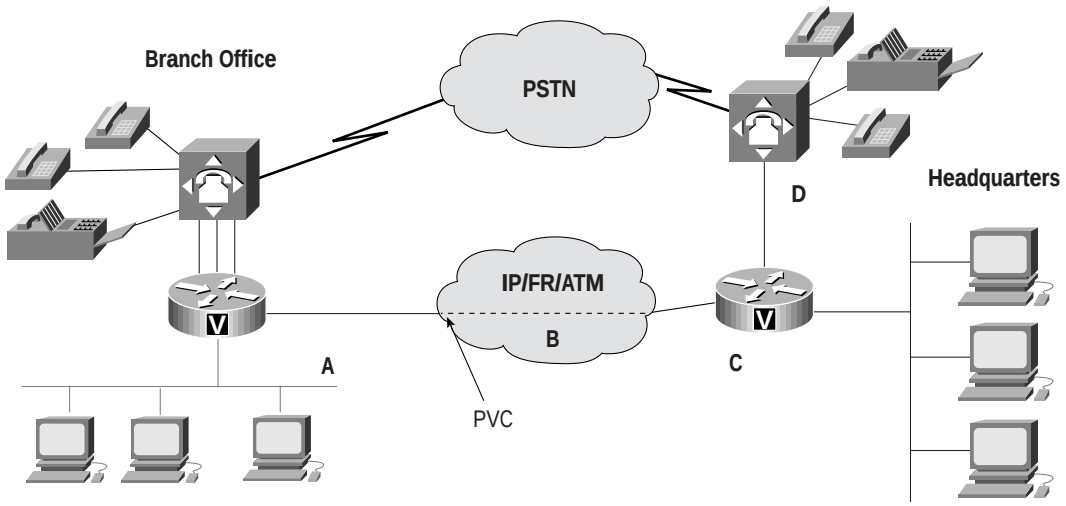
Routers	C26xx, C36xx,
Multiservice Access Concentrator (MC)	MC3810

First appearance in a Cisco IOS Software release: 12.1(3)T.

Caveats

- Trunk Conditioning is applicable to “connection trunk” configurations only.
- Trunk Conditioning is applicable to analog and T1/E1 CAS voice trunks only.

Figure 17
Trunk Conditioning for FRF.11 and Cisco Trunks



Fax Relay Packet Loss Concealment

Description

Fax Relay packet loss concealment improves real-time fax over IP implementation in Cisco voice gateways. This feature also includes enhanced real-time fax debug capabilities and statistics. These debugs and statistics give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.

Facsimile machines use the T.30 protocol to communicate and exchange scanned page information. Fax over IP involves demodulation of these signals at the ingress gateway, transporting the data across the IP network in packets, and remodulation of the data by the egress gateway. Packets containing page data that are lost in the network result in line errors being detected by the receiving fax machine.

By disabling error correction mode (ECM) between the two fax machines, the voice gateways conceal packet loss from the receiving fax machine. Using this mechanism, fax transmission will not disconnect prematurely because of packet loss. This feature does not address page quality due to lost packets. This feature supports two page compression techniques used by fax machines—Modified Huffman (MH) and Modified Read (MR).

Benefits

- Fax Relay performance improves in networks experiencing packet loss.
- The egress gateway conceals packet loss from the receiving fax machine.
- Gateways can display fax relay messages in real time to support troubleshooting. These time-stamped messages contain T.30 state information printed to the router console, such as the beginning of a page transmission, and lost packet events.

Platforms/Considerations

Access Servers (AS)	5300, 5800

First appearance in a Cisco IOS Software Release: 12.1(3)T.

Interactive Voice Response Version 2.0 on Cisco VoIP Gateways

Description

In the current Cisco IOS Software releases, IVR applications can be triggered from the IP call leg in additional to the telephony call leg.

With IVR enhancements, the voice gateway can also handle extended prompts through a Real Time Streaming Protocol (RTSP) client on the gateway. Extended prompts and messages can be stored on an RTSP server and streamed to the gateway upon request.

The IVR engine is enhanced to allow event-triggered instead of state-driven [need NOUN here]. The IVR engine does not have to wait for one command to finish before processing another command. For example, the IVR can direct the system to playback advertisements to a caller while waiting for the remote gateway to connect to the called party.

An MGCP call agent can control the IVR application. Using the MGCP application packages, the call agent can direct the IVR application to play message to the caller or collect information from the caller.

Benefits

- Allows the IVR application to be run from the terminating gateway. ITSP can offer service on the terminating gateway and does not require the originating gateway to preauthorize the caller.
- Using an RTSP client, the gateway can a play longer prompt without sacrificing time of the first download that prompts to the gateway. The extended prompts or messages can be streamed to the gateway in real time. Leveraging content on the Internet, rich information can be streamed to the caller via the RTSP server.
- For an ITSP implementing an MGCP call agent, the call agent can also direct the IVR application via the application packages built in the MGCP.
- Increase performance on IVR by converting from state driven to event driven. This allows the IVR script to perform a second task while waiting a previous task to complete. For example, in the event driven task, the IVR application can instruct the originating gateway to set up a call to the terminating gateway. Before the call is properly set up, the caller does not hear any progress tone such as ringing. At this time, the IVR script can instruct the gateway to stream advertisements from the RTSP server to the caller.

Platforms/Considerations

Access Servers (AS)	AS5300

First appearance in a Cisco IOS Software release: 12.1(3)T.

Link Fragmentation and Interleaving (LFI) for Frame Relay and ATM Virtual Circuits

Description

Link Fragmentation and Interleaving (LFI) is important for FR and ATM PVCs when both real-time traffic, such as voice, as well as non-real-time traffic, such as FTP data packets, are present on data paths. In these situations, it is important to minimize the delay and jitter between voice packets to maintain voice quality. This problem is particularly important for the typical hub and spoke networks present in Frame Relay and ATM environments with a high-speed link (typically DS1 or higher speeds) at the head-end of the network and where there are slow speed links (typically DS0 lines) present at the remote sites or branch offices of a network.

To support the different types of FR and ATM networks (FR-FR, ATM-ATM, FR-ATM), the fragmentation and interleaving method in Multilink PPP was chosen as the LFI technique and adapted for FR and ATM environments. Multilink PPP allows the same approach to be used for FR and ATM and avoids the FR only approach of FRF.12.

Benefits

- LFI improves quality for voice traffic when data packets are also present
- LFI utilizes the fragmentation and interleaving method in Multilink PPP
- LFI allows the same technique to be used for FR and ATM environments
- LFI works for FR-FR, ATM-ATM, and FR-ATM networks

Platforms/Considerations

Routers	C26xx, C36xx, C7200
Universal Broadband Routers (UBR)	UBR7200
Multiservice Access Concentrator (MC)	MC38xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

T.37/T.38 Fax Gateway

Description

The T.37/T.38 Fax Gateway functionality provides store-and-forward fax and fax relay support on the voice ports of the AS5300 voice gateway. These capabilities are available on both the C542 and C549 voice ports. This functionality allows dynamic switching from one application to another in the same call (IVR, fax relay, and fax store and forward).

T.38 preserves the semantics of faxing over the PSTN by establishing a real-time fax connection across the IP infrastructure. T.37 converts fax data to a TIFF attachment of an e-mail message and forwards via SMTP.

Benefits

- Use of standard protocols such as T.38 facilitate interoperability with other vendor's fax products
- Rather than bearing the cost of maintaining two architectures, one for voice and one for fax, service providers can use a single port for voice, fax relay, and store-and-forward fax. For smaller POPs, the ability to use a single port for both technologies is even more significant. This is due to greater efficiencies of handling mixed traffic over a single pool of ports versus splitting traffic across two pools (whose combined total number of ports would exceed the number in the mixed traffic case).
- Service providers can offer applications that require toggling from voice to fax—for example, providing an IVR front-end to a fax application. Also applications such as never-busy fax service can be addressed as the gateway has the ability to dynamically switch from fax relay to fax store and forward.

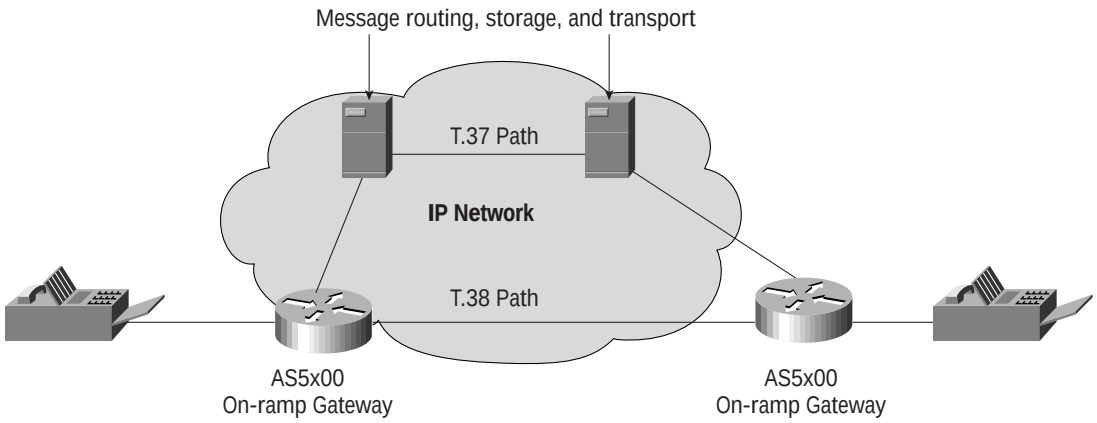
Platforms/Considerations

Access Servers (AS)	5300

First appearance in a Cisco IOS Software release: 12.1(5)T.

Note: In order to support the maximum of 120 fax store and forward sessions, the Cisco AS5300 must be equipped with 128 MB of RAM.

Figure 18
Real-time Fax (T.37) versus Store-and-Forward Fax (T.38)



Enhanced Voice Services for Japan for Cisco 800 Series Routers, Cisco 813

Description

The affordable Cisco 810 series routers offer the performance, reliability, and security that small offices need to take advantage of "always-on ISDN" access. Part of the Cisco 800 family, Cisco 810 routers bring the power and advanced features of Cisco IOS technology to small offices, with a built-in dynamic firewall that protects always-on ISDN connections from intruders

and eliminates the need for separate security devices. With support for secure, high-performance virtual private networks (VPNs), Cisco 810 series routers can also provide full Internet and WAN connectivity for small offices, without need for costly dedicated lines. They're the next-generation solution for transforming small offices into full-fledged e-businesses.

In addition, the 810 series supports the popular INS-64 voice features. These features include:

- ISDN Voice Priority
- Distinctive Ringing
- Caller ID
- Call Blocking on Caller ID
- Nariwake
- Voice Warp
- Voice Warp Select
- Call Waiting
- E Ya Yo
- Troublesome Call Refusing
- I Number

Benefits

Cisco 810 Series Router Benefits

- *The most affordable, advanced secure access solution*—"Always-on ISDN service" provides the convenience of an uninterrupted Internet connection but also exposes that connection to outside intruders. Cisco 810 series routers answer this challenge with integrated dynamic firewall services, to provide enhanced security while simplifying installation and management. And because there is no need to buy separate security devices, Cisco 810 routers are a very cost-effective solution for secure Internet and WAN access.
- *High performance*—The RISC-based processor, the field expandable memory in the Cisco 810 series, provides a level of performance optimized to support advance quality of service (QoS) features, which VPNs need. In addition, the 810 series provides small businesses the benefit of high-performance data compression. With compression enabled, small offices can save on usage charges by achieving throughput up to 512 kbps.
- *Reliable connectivity*—Because Cisco 810 series routers are based on the same proven Cisco IOS technology used throughout the Internet, small offices can depend on them day after day, year after year. With more than 3 million access routers installed, Cisco reliability has been proven in demanding network environments in Japan and worldwide.
- *Cost-effective alternative to expensive dedicated services*—Cisco 810 series access routers are optimized for VPNs, which allow customers to leverage the Internet to connect branch offices, without costly dedicated WAN services such as leased lines. Through Cisco IOS technology, the Cisco 811 and 813 provide the sophisticated QoS support needed to ensure consistent response times for multiple applications by intelligently allocating bandwidth. These QoS features, working in parallel with Cisco advanced security, provide a complete VPN solution that is ready to deploy today.

Platforms/Considerations

The Features are supported on the Cisco 810 Series

First appearance in a Cisco IOS Software release: 12.1(5)T.

ISDN Progress Indicator Support for SIP Using 183 Session Progress

Description

This feature addresses issues related to handling of inband treatments, such as call progress tones and announcements, when Session Initiation Protocol (SIP) is used as the session protocol to establish call connections.

The feature ensures that the media stream is established correctly through the SIP network to allow for any inband treatments that may ingress from a PSTN node on a SIP gateway or egress to a PSTN node to be successfully transported.

This feature supports both SIP to or from PSTN cases as well as PSTN transit cases. The PSTN transit cases include:

- ISDN to SIP to ISDN interworking
- ISDN to or from SIP from or to CAS internetworking
- CAS to SIP to CAS internetworking

Benefits

- Ensures that inband treatments initiated in the PSTN are successfully transported through the SIP network
- Allows for internetworking of features between the PSTN and the SIP network so that the correct inband feedback is provided to the feature user.

Platforms/Considerations

Routers	C26xx, C36xx,
Access Servers (AS)	5300

First appearance in a Cisco IOS Software release: 12.1(3)XI.

WAN Optimization

Frame Relay Fragmentation with Hardware Compression

Description

The Frame Relay fragmentation with hardware compression functionality allows interoperability between FRF.12 and FRF.11 Annex C fragmentation techniques and the hardware-based compression available on the Cisco 2600/3600/7200 product families. The major benefit is the ability to reduce voice traffic delay (either VoFR or VoIP over FR) when voice and data traffic are both present on a single permanent virtual circuit (PVC) or multiple PVCs. By using hardware-based compression, data packets reduce in size. This reduction in size, coupled with the fragmentation and interleaving of the data packets with voice packets, allows the effective delay between voice packets to be less variable and hence less jittery. Compression techniques supported are FRF.9 and STAC. Previously, only software-based compression could be used with fragmentation.

Benefits

- Improved voice quality
- Hardware-based compression can now be used with fragmentation.
- FRF.12 and FRF.11 Annex C Fragmentation supported
- FRF.9 and STAC compression supported

Platforms/Considerations

Routers	C26xx, C36xx, C7200

First appearance in a Cisco IOS Software release: 12.1(5)T.

PPP Over Fast Ethernet 802.1Q

Description

Cisco currently supports PPP over Ethernet over ATM and PPPoE over Ethernet and Fast Ethernet encapsulations. This feature adds support for running PPP over Ethernet over IEEE 802.1Q. IEEE 802.1Q is used to interconnect a VLAN capable router with another VLAN capable device. The packets on the 802.1Q link contain a standard (fast) Ethernet frame and the VLAN information associated with that frame.

The PPPoE Enable command is added under 802.1Q encapsulated VLAN subinterfaces. Configuration of PPP over Ethernet over dot1q VLANs is very similar to configuring PPPoE over Ethernet or Fast Ethernet interfaces, except that the PPP over Ethernet configuration is now entered under the subinterface using 802.1Qvlan encapsulation. The configuration involves creating a dot1q encapsulated vlan (subinterface), and then configuring PPP over Ethernet just like configuring PPPoE over Ethernet/FastEthernet interfaces.

Benefits

- Ability to run PPP over VLAN over Fast Ethernet

Platforms/Considerations

Routers	C2600; C3660; C36x0; C4x00/m; C72xx; C75xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

CEF Switching for Routed Bridge Encapsulation

Description

ATM Routed Bridge(RBE), also known as ATM half-bridging, is the process of routing traffic from a bridged LAN without the use of integrated routing and bridging (IRB). The feature was scheduled to be implemented into 12.1(2)T and it currently supports only fast and process switching paths. To take advantage of the benefits such as resilience, scalability, and improved performance offered by Cisco Express Forwarding (CEF), CEF switching support needs to be added for RBE feature. This feature adds that new switching path support for RBE.

A stub router is the periheral router in a hub-and-spoke network topology. Stub routers commonly have a WAN connection to the hub router and a small number of LAN network segments (stub networks) that are connected directly to the stub router. RBE provides a routed-bridge interface to stub networks. CEF switching increases router's performance by making use of Forwarding Information Base (FIB) and adjacencies tables. The combination, THE RBE CEF feature, allows a router with one or more ATM interfaces, to use CEF switching instead of process or fast switching. CEF switching is designed primarily for use in high-performance backbone routers. However, it will work in any part of the network.

Benefits

- CEF switching increases router's performance by making use of Forwarding Information Base (FIB) and adjacencies tables

Platforms/Considerations

Routers	C36x0; C72xx; C75xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

WAN Services

CUG Selection Facility Suppress Option

Description

This feature is useful for networks in which CUGs are prevalent in existing networks but legacy equipment that does not support CUGs needs to remain as part of XoT migration.

The new feature allows the Cisco routers to remove the CUG selection facility in some specific cases when switching an X25 call from the network side to the user side.

Benefits

- DTEs that don't support CUGs can remain as part of XOT network by suppressing CUG selection option for calls from network side to user side.

Platforms/Considerations

Routers	C160x, C25xx, C26xx, C36xx, C4x00, C7x00

First appearance in a Cisco IOS Software release: 12.1(5)T.

Frame Relay Switching Diagnostics and Troubleshooting

Description

The Frame Relay switching diagnostics functionality provides enhancements for troubleshooting and debugging the FR switching functionality provided in the 12.1(2)T release. The functionality provides additional detail into why switched Frame Relay packets are being dropped. It will also provide a Debug Frame Relay Switching command to get detailed status about switched PVCs for analyzing packet flows. Finally, this functionality will provide information regarding the local operational status of a network-to-network interface (NNI) PVC.

Benefits

- Ability to debug and troubleshoot Switched FR PVCs.
- Provide detailed status regarding a failed switched FR PVC
- Receive information regarding the local operational status of a NNI PVC

Platforms/Considerations

Routers	C100x, C1400, C160x, C17x0, C25xx, C26xx, C36xx, C4x00, C64xx, and C7x00
Universal Broadband Routers (UBR)	UBR7200

First appearance in a Cisco IOS Software release: 12.1(5)T.

PPPoE RADIUS Port Identification

Description

This feature provides NAS-port and NAS-port-type RADIUS attributes for PPPoA, PPPoE, and PPPoE over VLAN. It also provides these two RADIUS attributes available through LAC and LNS.

Cisco IOS Software currently supports PPPoE (PPP over Ethernet) protocol over ATM, Ethernet and 802.1Q VLAN encapsulations. While using RADIUS, NAS-port and NAS-port-type attributes send the port details to RADIUS. NAS-port attribute value is only 32 bits long. We have different ways of formatting/interpreting this port, which is controlled by CLI.

There is also another feature to transfer NAS-port from LAC (NAS) to LNS (HGW), enabled by the following CLI command: router(config)# vpdn aaa attribute nas-port vpdn-nas

When this feature is enabled on LNS, LNS sends LAC NAS-port information (that has been forwarded to it from LAC) to the RADIUS server. This function currently does not work for format-d extension of the NAS-port. This feature extends this to work with format-d extension. To summarize, this feature adds NAS-port format-d extension for PPPoE (PPPoEoA and PPPoVLAN) on LAC and enables LNS to use format-d NAS-port.

Benefits

- Ability to send port and VPI/VCI details to RADIUS in PPPoA, PPPoE, and PPP over VLAN environments
- Ability to authenticate and account based on port details

Platforms/Considerations

Routers	C36x0; C72xx; C75xx

First appearance in a Cisco IOS Software release: 12.1(5)T.

Wireless

MICA PIAFS

Description

MICA PIAFS allows the Cisco AS5300 access server to support wireless data connectivity with users calling in from personal handyphone system (PHS) service providers. PHS wireless networks, found mainly in Japan, use a data link protocol called PIAFS. This Cisco IOS feature works with a special version of MICA Portware (DM-SW-8.2.1.0), which is required to be loaded into the MICA DSP modules. Use of MICA PIAFS requires the purchase of a Cisco Wireless License.

Benefits

- Supports connectivity with PHS phone sets supporting PIAFS 2.0 on AS5300
- Data rates of 32K and 64 Kbps are supported
- V.42bis compression enhances net data rates
- Special PIAFS RADIUS attributes supported

Platforms/Considerations

Access Servers (AS)	AS5300

First appearance in a Cisco IOS Software Release: 12.1(3)T.

GSM Enhanced Full Rate Codec (EFR)

Description

Enhanced Full Rate (EFR) is the latest and highest-quality, speech transcoding specified by ETSI GSM cellular standard. EFR is being deployed in virtually all of the GSM systems around the world, due to its near landline quality. It is also included in all GSM mobile phones being produced today. Cisco multiservice gateways support GSM EFR, ensuring Cisco gateways are deployed as part of Cisco Mobile Office Solution (MNET), the voice quality offered to mobile user is near landline quality.

Benefits

- *Toll-quality voice*—Mobile users expect near landline voice quality when they use their cell phones within enterprises. When Cisco multiservice gateways are used as part of the Cisco Mobile Wireless Network Solution, GSM EFR Codec offers this capability.

Platforms/Considerations

Routers	26xx, 36xx, 72xx
Voice Gateway	VG200
Access Servers (AS)	AS5300

Caveats:

GSM EFR is not a standalone feature. This only applies when a Cisco router is used as part of Cisco Mobile Office Network Solution for enterprises. The implementation of GSM EFR feature in Cisco multiservice gateways ensures that near-land-line voice quality can be offered to mobile users.

First appearance in a Cisco IOS Software release: 12.1(5)T.

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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

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

ETMG 203152—SH 01/04