Cisco IOS Software Release 12.4T Features and Hardware Support

PB3001

Last Updated: February 2009

This Product Bulletin introduces Cisco IOS Software Release 12.4T, and includes the following sections:

1) Introduction

Cisco IOS® Software is the world's premiere network infrastructure software, delivering seamless integration of technology innovation, business-critical services, and hardware support. Currently operating on millions of active systems, from small home office routers to the core systems of the world's largest service provider networks, Cisco IOS Software is the most widely leveraged network infrastructure software in the world.

Cisco IOS® Software Release 12.4T integrates a comprehensive portfolio of new capabilities, including security, voice, and IP services, with powerful hardware support to deliver advanced services for Enterprise and access customers.

Release 12.4(24)T, the latest release of the 12.4T family, adds Cisco IOS BGP Support for 4-byte Autonomous System Numbers (ASN), Application-Based Routing for Mobile Router (MR) Multi-Path Support, Web Services Management Agent (WSMA), for advanced embedded capabilities to

provision, manage, configure and adapt Cisco devices, Smart Call Home Support for the Cisco 7200 Series Router, and Cisco Unified Communications Manager Express and Cisco Unified SRST 7.1 enhancements.

Release 12.4(22)T provided QoS support for IPSec tunnels, Trusted Relay Point (TRP) IOS firewall security for Unified Communications, Flexible NetFlow enhancements, and support for the Cisco 880 SRST and 880G Integrated Services Routers.

Release 12.4(20)T added significant embedded management enhancements, category-based productivity and security ratings support, multi-level Quality of Service (QoS) scheduling, and support for the Cisco 860, 880, and 1861 Routers.

Release 12.4(15)T streamlined the Cisco IOS Software upgrade process, provided sub-second link failure detection and faster convergence, delivered next-generation Layer 2-7 flexible packet classification, enhanced intrusion protection (IPS) and SSLVPN capabilities, and support for the new Cisco 7201 Router.

Release 12.4(11)T delivered new Layer 2 VPN transport over MPLS capabilities, enhanced MPLS management, mobile IPv6 authorization and identity support, and support for the high performance Network Processing Engine G2 (NPE-G2) and VPN Service Adapter (VSA) for the Cisco 7200 Series Router.

Release 12.4(9)T delivered improved manageability, integrated IP communications capability, enhanced HTTP and P2P security, and faster routing protocol convergence.

Release 12.4(6)T delivered highly available firewalls, comprehensive endpoint and network security for SSL VPN environments, and optimized bandwidth management for improved VoIP call quality.

Release 12.4(4)T enhanced threat protection against malicious worm and virus attacks, improved performance monitoring of VoIP networks, and extended support for secure concurrent services on the Cisco 1800 Series router.

1.1) Migration Guide

Cisco recommends that customers running Release 12.3T, 12.3, or prior releases upgrade to Release 12.4T or 12.4. Customers should determine their functionality needs and choose the appropriate release.

Note: Release 12.3 reached End of Software Maintenance on March 15, 2008. For additional information please visit:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6947/ps5187/prod_end-of-life_notice0900aecd8052e110.html

Release 12.4(15)T will receive extended bug fix support through December 2010. Cisco is taking this action to indicate that Release 12.4(15)T maintenance releases are treated in a similar manner as Release 12.4. Both undergo comprehensive testing and review cycles to continuously improve and increase reliability, quality, and stability. As per Cisco policies, no new technologies or features are added to either Release 12.4 or maintenance rebuild releases of Release 12.4(15)T. For more information please visit:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/ps8258/product_bulletin_c25-496283.html

AppleTalk Support Discontinuation in IOS T

Due to a significant decrease in AppleTalk usage and demand among its customer base, and given the fact that Apple now fully supports the TCP/IP family of protocols, Cisco has reached the decision to discontinue AppleTalk support on Cisco IOS. The AppleTalk feature removal will be permanent and will apply to future IOS releases after Release 12.4(24)T.

Refer to the following product bulletin for more details:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/product_bulletin_c25-520459.html

Cisco Service Selection Gateway (SSG) Feature Discontinuation in IOS T

The Cisco Service Selection Gateway (SSG) feature will no longer be available after Cisco IOS Software Release 12.4(24)T. Refer to the following product bulletin for more information:
http://www.cisco.com/en/US/prod/collateral/routers/ps341/end_of_life_notice_c51-501483.html

Figure 1 illustrates the current migration path from Cisco IOS Releases 12.3T, 12.3, and prior releases to Release 12.4T or Release 12.4.

Figure 1. Release 12.4T Migration Plan

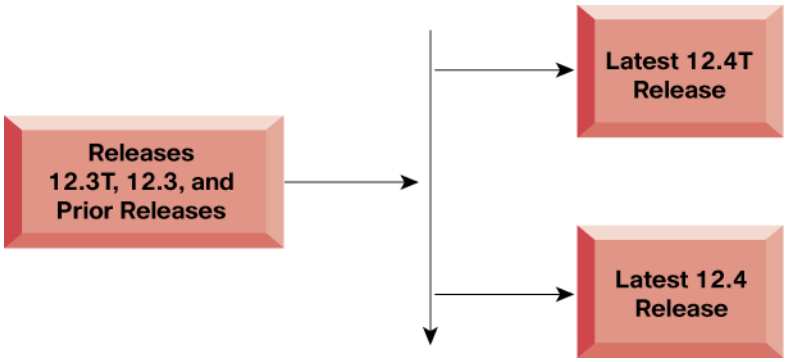
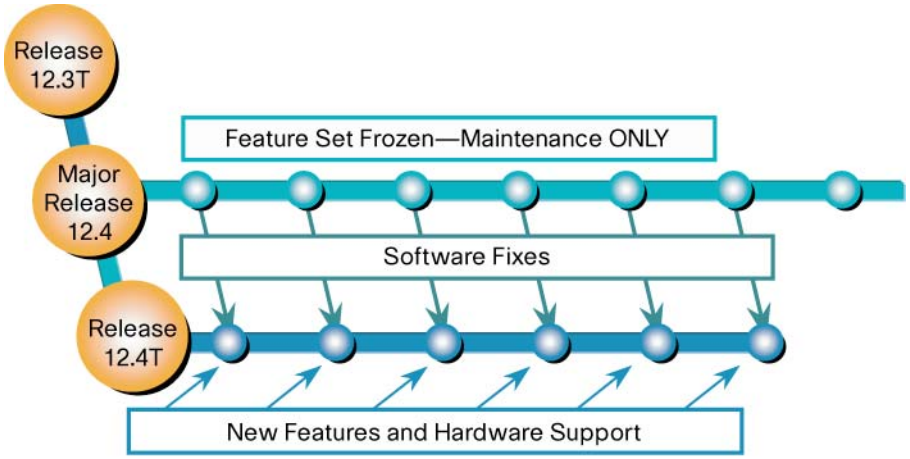


Figure 2 below illustrates the relationship between Release 12.4T and Release 12.4.

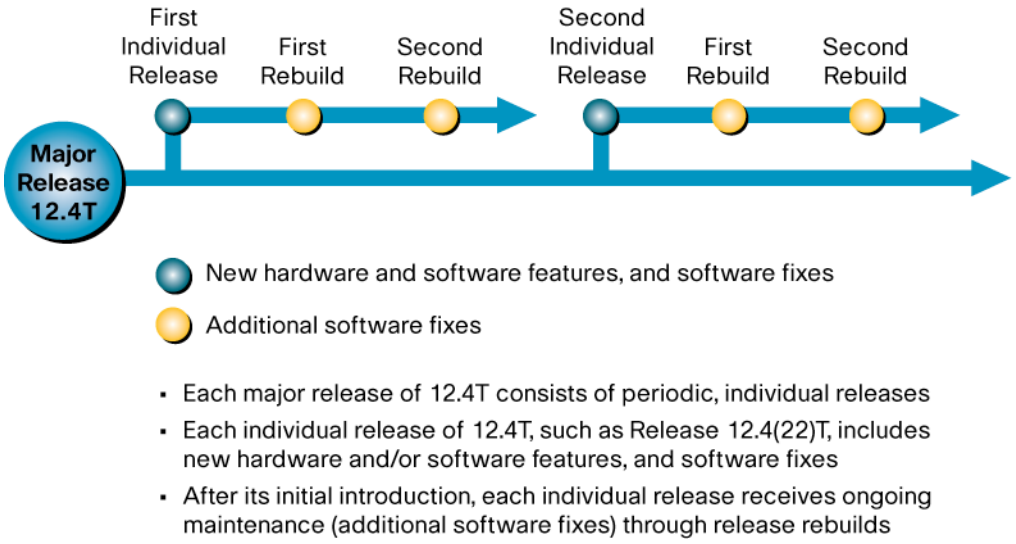
Figure 2. Release 12.4T and Release 12.4 Relationship



Note: Technology releases are those Cisco IOS Software releases that introduce new features, functionality, and hardware support.

Figure 3 below shows the relationship between Release 12.4T and individual 12.4(n)T new feature releases.

Figure 3. Release 12.4T and Individual 12.4(n)T Release Relationship



Note: Cisco IOS Software Release 12.4(20)T and later Release 12.4T releases do not support several Cisco hardware platforms that were supported in Release 12.4(15)T and prior releases. These platforms will be supported by Release 12.4(15)T via regularly scheduled software maintenance rebuilds and bug fix support until the end of software maintenance date for the respective platform is reached.

- Cisco SOHO 90 Series
- Cisco 831, 836, 837, and 850 Series
- Cisco 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760 Series
- Cisco 2610XM-2611XM, 2620XM-2621XM, 2650XM-2651XM, and 2691 Series
- Cisco 3631 and 3660 Series
- Cisco 3725 and 3745 Series
- Cisco 7400 Series
- Cisco AS5850 Universal Gateway

For more information refer to the following product bulletins:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/product_bulletin_c25_466578.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/ps8258/product_bulletin_c25-496283.html

The Cisco release delivery process, rigorous software testing, and regularly scheduled software maintenance results in significant incremental enhancements and improvement to the quality, stability, and resiliency of Cisco IOS Software Release 12.4T and Release 12.4.

1.2) Release 12.4T Additional Information

- **Release 12.4T**

  Cisco IOS Software Releases 12.4 T—Products & Services—Cisco Systems
- **Cisco IOS Software Product Lifecycle Dates & Milestones, Product Bulletin No. 2214**

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd801eda8a_ps6441_Products_Bulletin.html

- **Changes to Cisco IOS Software Product Support in Release 12.4T, Product Bulletin No. 3000**

  http://www.cisco.com/go/124thardware/

- **Cisco IOS Software Download Center**

  Download Cisco IOS Software releases and access software upgrade planners.

  http://www.cisco.com/public/sw-center/sw-ios.shtml

- **Cisco Feature Navigator**

  A web-based application that allows you to quickly match Cisco IOS Software releases to features, to hardware.

  http://www.cisco.com/go/fn/

- **Cisco Software Advisor**

  Determine the minimum supported software for selected hardware.

  http://tools.cisco.com/Support/Fusion/FusionHome.do

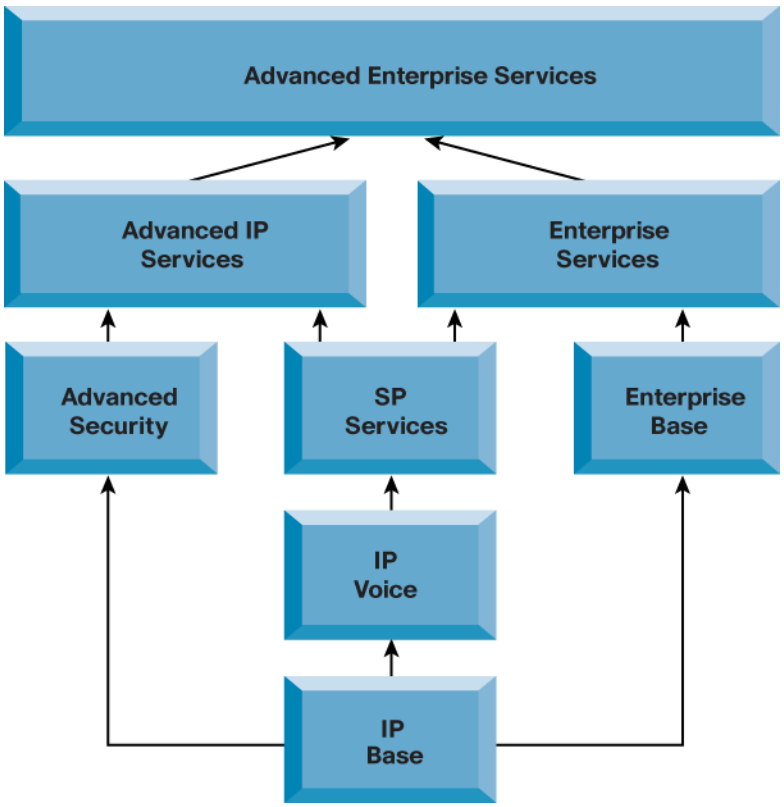
- **Cisco IOS Upgrade Planner**

  View all major releases, hardware, and software features from a single interface.

  http://www.cisco.com/pcgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

1.3) Cisco IOS Packaging Consideration

Figure 4. Cisco IOS Packaging for Cisco Routers



2) Release 12.4(24)T Highlights

Table 1. Release 12.4(24)T Feature Highlights

2.1) IP Routing	2.2) IP Services	2.3) Embedded Management	2.4) Voice
2.1.1) BGP 4-byte ASN Support 2.1.2) Mobile IP—Policy and Application-Based Routing for Mobile Router Multi-Path Support 2.1.3) Multi-VRF Selection using Policy-Based Routing (PBR)	2.2.1) Secure Neighbor Discovery (SeND) 2.2.2) DHCPv6 Individual Address Assignment	2.3.1) Web Services Management Agent (WSMA) 2.3.2) Smart Call Home Support for the Cisco 7200 Series Router	2.4.1) Cisco Unified Communications Manager Express 7.1

2.1) IP Routing

2.1.1) Cisco IOS BGP Support for 4-byte Autonomous System Numbers (ASN)

Border Gateway Protocol (BGP) is an Internet Engineering Task Force (IETF) standard, and the most scalable of all routing protocols. BGP is the routing protocol of the global Internet, as well as for enterprise and service provider private networks. BGP has expanded upon its original purpose of carrying Internet reachability information, and can now carry routes for Multicast, IPv6, VPNs, and a variety of other data. Cisco supports all IETF BGP standards, as well as the majority of Internet Drafts for BGP. In addition, Cisco is an active participant in the Inter-Domain Routing (IDR) Working Group at IETF, and a frequent contributor of new BGP extensions.

Cisco IOS Software Release 12.4(24)T release adds BGP Support for 4-byte ASN.

At the early time of BGP development and standardization, it was assumed that availability of a 16 bit binary number to identify the Autonomous System (AS) within BGP would have been more than sufficient. The 16 bit AS number, also known as the 2-byte AS number, provides a pool of 65,536 unique Autonomous System numbers. The Internet Assigned Numbers Authority (IANA) manages the available BGP Autonomous System Numbers (ASN) pool, with the assignments being carried out by the Regional Registries.

The current consumption rate of public AS numbers suggests that the entire 2-byte ASN pool will be fully depleted by early to middle 2011. A solution to this depletion is the expansion of the existing 2-byte AS number to a 4-byte AS number, which provides a theoretical 4,294,967,296 unique AS numbers. ARIN has made the following policy changes in conjunction with the adoption of the solution.

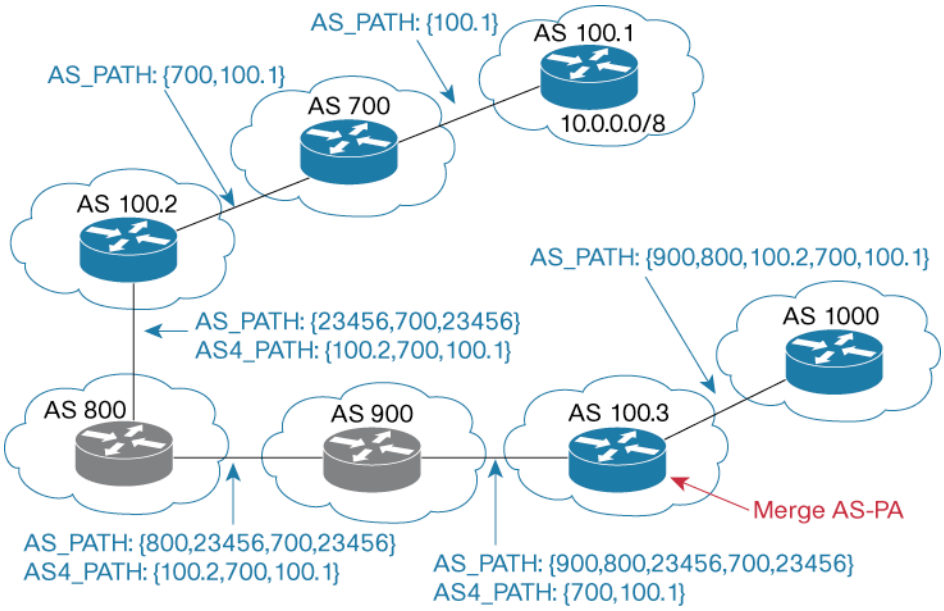
As of January 1, 2009, per the American Registry for Internet Numbers (ARIN), all new Autonomous System Numbers (ASNs) issued will be 4-byte by default, unless otherwise requested. For more information please visit: https://www.arin.net/announcements/2008/07242008.html

The Cisco IOS BGP 4-byte ASN feature allows BGP to support the ASN encoded as a 4-byte entity. The addition of this feature allows an operator to use an expanded 4-byte AS number granted by IANA.

As shown in Figure 5 below, backwards compatibility is provided between the 4-byte and 2-byte AS numbers, since BGP and Multiprotocol BGP is already widely deployed in ISP and MPLS VPN environments. Specifically, advertisement via standard based BGP capability code, two new “optional transitive” attributes: AS4_AGGREGATOR and AS4_PATH, and a newly reserved AS TRANS#: 23456 for interoperability between 4 bytes ASN capable and non-capable BGP speakers are introduced to a smooth migration from a 2-byte to a 4-byte ASN environment.

The implementation is in compliance with IEFT RFC 5396 and RFC 4893 standards.

Figure 5. Use Case Example of Both 4-byte Capable and 2-byte ASN BGP Speakers



Benefits

- Allows BGP to carry a Autonomous System Number (ASN) encoded as a 4-byte entity
  - Includes the following enhancement to ensure a smooth migration from a 2-byte to 4-byte ASN environment
    - Advertisement via standard based BGP capability code
    - Two new “optional transitive” attributes: **AS4_AGGREGATOR** and **AS4_PATH**
    - A newly reserved **AS TRANS#**: 23456 for interoperability between 4 bytes ASN capable and non-capable BGP speakers
  - To further reduce operation change requirements when an operator migrating from a 2 bytes to a 4 bytes ASN environment, the implementation provides a default “**asplain**” and an optional “asdot” AS output format

Considerations

- The initial support for 4-byte ASN in Release 12.4(24)T supports all existing BGP features (including IPv4, IPv6, VPNv4, and VPNv6 address and sub address families) with the exception of Cisco IOS NetFlow

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200 Series Routers

Additional Information:

Border Gateway Protocol Home Page
http://www.cisco.com/en/US/products/ps6636/products_ios_protocol_option_home.html

Cisco IOS BGP 4-Byte ASN Support
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/data_sheet_C78-521821.html

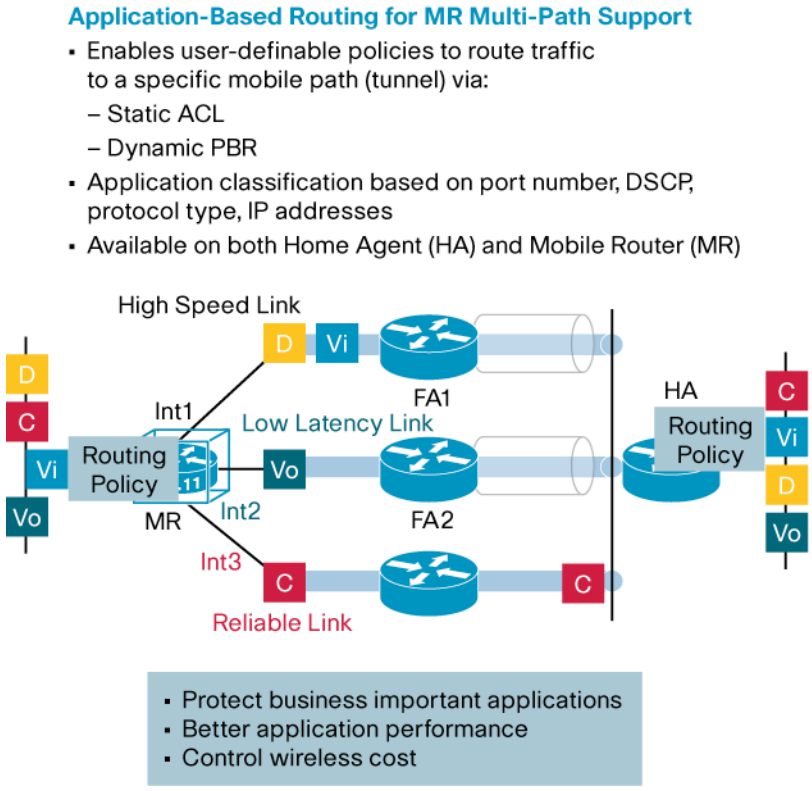
Product Management Contact: Ted Qian (tqian@cisco.com)

2.1.2) Mobile IP—Policy and Application-Based Routing for Mobile Router Multi-Path Support
Cisco Mobile Routers (MRs) running Cisco Mobile Network technology, offer seamless network connectivity for devices connecting to it. Network connectivity remains uninterrupted even when the mobile router roams among various wireless and wired networks.

Prior to the introduction MR Multi-Path support in Cisco IOS Software Release 12.4(9)T, a Cisco MR could only support seamless mobility to the Home Agent (HA) via a single mobile tunnel at a time. The Multi-Path Support for Mobile Router feature allows a MR and a HA to establish multiple Mobile IP tunnels over all available roaming interfaces. When the Multi-Path feature is enabled, the MR registers through all of its available roaming interfaces to the HA. Each registration is independent of the other registrations taking place on other roaming interfaces. Once registered through the roaming interfaces, the MR will have multiple routes or multiple paths back to the HA (assuming the Mobile IP Reverse Tunnel feature is configured). The mobile traffic from or to the mobile network is then load-balanced among the multiple routes based on the CEF load balancing algorithms, either per packet or per destination (default). In addition, this feature supports unequal load balancing. The Multi-Path feature enables users to utilize all the possible bandwidth available from all the enabled links.

New in Cisco IOS Software Release 12.4(24)T is Application-Based Routing for Mobile Router Multi-Path Support. This feature extends existing MR Multi-Path routing support to enable static Access Control Lists (ACLs) and dynamic Policy-Based Routing (PBR) route-map commands to define unique traffic types and route these traffic classes over specified interfaces or paths. This feature enables you to bi-directionally define how specific traffic types should be routed across the multiple tunnels established between the MR and HA. The same ACL and PBR policies are used on both the MR and HA.

Figure 6. Application-Based Routing for Mobile Router (MR) Multi-Path Support



Benefits

- **Better Investment Protection:** Enables the customer to optimize performance, scalability, and availability of applications traversing the multi-path mobile network via application routing policies

Hardware

Routers	• Cisco 1700, 1800, 2800, 3200, 3270, 3600, 3700, 3800, 7200, and 7301 Series Routers

Product Management Contact: Kevin Delgadillo (delgadil@cisco.com)

2.1.3) Multi-VRF Selection Using Policy-Based Routing (PBR)

Multi-VRF Selection using Policy Based Routing is an extension of VRF Selection based on Source IP Address. This functionality takes advantage of the existing Route-map (which is capable of supporting multiple selection criteria) and uses Policy Based Routing (PBR) as a way to classify packets and set the relevant routing/forwarding decision. Classification criteria include source and/or destination IP addresses, protocol number, source and/or destination port number, IP precedence value, DSCP value, TCP flags, packet length and ICMP type.

Note: This feature only supports VRF-Lite. Only IP routing protocols are supported with this feature. Multiprotocol Label Switching (MPLS) VPN is not supported.

Benefits

- Enables flexible VRF selection policies to optimize VRF-enabled network architectures.

Hardware

Routers	• Cisco 7200 and 7301 Series Routers

Product Management Contact: Kevin Delgadillo (delgadil@cisco.com)

2.2) IP Services

2.2.1) Secure Neighbor Discovery (SeND)

Secure Neighbor Discovery (SeND) protocol is designed to counter the threats of Neighbor Discovery Protocol (NDP), as detailed in RFC3756. SeND comes as an addendum on top of ND. It defines a set of new ND options, and two new ND messages (Certification Path Solicitation & Answer). It also defines a new auto-configuration mechanism, to be used in conjunction with the new ND options, to establish address ownership.

There are essentially two security features introduced by SeND to mitigate address spoofing and rogue routers, two of the biggest threats related to NDP. The first feature enables nodes to establish address ownership using IPv6 Cryptographically Generated addresses (CGA), as specified in RFC3972. The second feature provides router authorization through X.509 certificates, and is specified in RFC3971.

Deployment-wise, CGA is a very light-weight mechanism, as it does not involve cryptographic key distribution (other than providing the public key in one of the new NDP option), nor any identity of any sort or certificates.

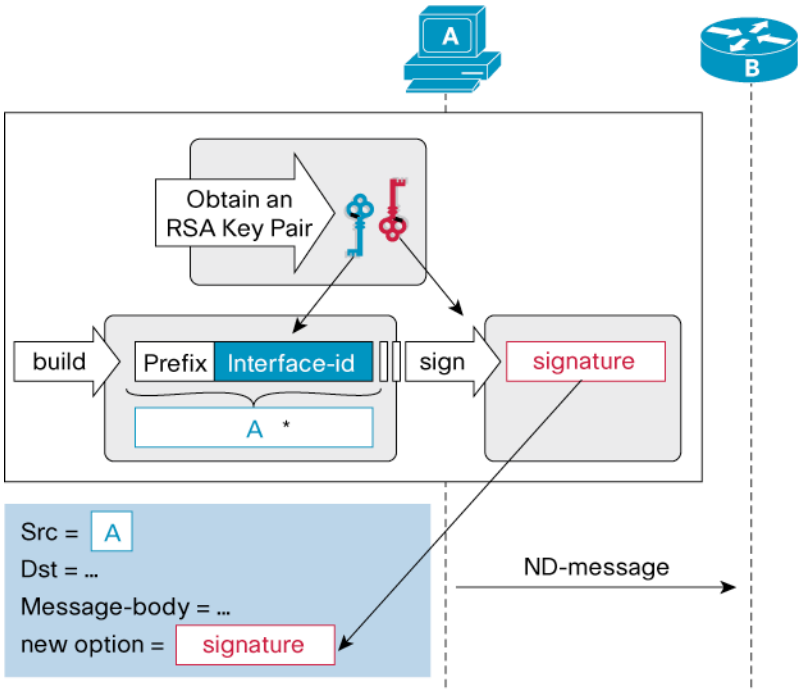
Router authorization is more challenging, since router must have an “identify”, certified through a certificate signed by a Certificate Authority, and that Certificate Authority must be known by all nodes. RFC3971 also specifies two important additional elements. Certificates can contain the list of prefixes that the router owns, so that any node could verify prefixes announced by the router prior to performing stateless auto-configuration. And last but not least, a node running SeND is expected to be able to arbitrage between concurrent claims coming from a mixture of peers speaking SeND and nodes speaking ND, in favor of the former.

The Cisco implementation, which is fully compliant with SFC3971 and 3972, supports:

- Cryptographically Generated addresses (CGA)
- Router authorization through X.509 certificates
- Prefixes embedded in certificates, as specified in RFC 3779
- Transitioning situation, where it is capable of giving preference to SeND peers over ND peers

In addition, the IOS-PKI and the IOS-CS (Certificate Server) has been upgraded to allow building certificate requests with embedded IPv6 prefixes, read and store these prefixes, and validate a certificate chain with embedded IPv6 prefixes. This is useful to install on a Cisco SeND router, a fully complied X.509 certificate with embedded prefixes, and enable Router Authorization.

Figure 7. Generation of a SeND Packet (simplified version)



Benefits

- Router interface addresses are generated in a way that the ownership can be verified by a third party
- Received address ownership is dynamically verified; Only validated neighbors are inserted into the Neighbor Discovery cache
- Router Advertisement content is dynamically verified, so no one can pretend to be a valid router on a link without a valid matching X.509 certificate

Hardware

Routers	• Cisco 800, 1800, 3800, 7200, 7301 Series Routers

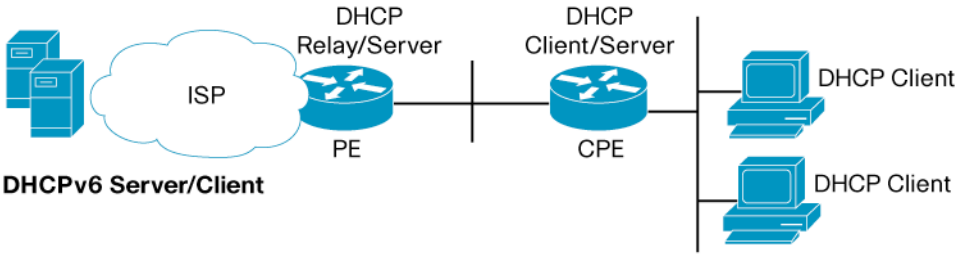
Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

2.2.2) DHCPv6 Individual Address Assignment

At the heart of the IP address distribution architecture for IPv4, DHCP has been selected by the IPv6 community to fulfill similar functions. While stateless address auto-configuration is mandated by IPv6 specifications, there is a business demand to have DHCP offer stateful address and prefix delegation in an easily deployable fashion (VoIPv6 for instance).

The new feature of allocating individual addresses is now supported for Client, Server and Relay functions.

Figure 8. DHCPv6 Individual Address Assignment Topology



DHCPv6 Client, Server, and Relay Functions

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

Client Function

The DHCPv6 client function can be enabled on individual IPv6-enabled interfaces and benefits from the new following features:

- Support for multiple IPv6 addresses (IA_NA options) on an interface
- Rapid Commit: The Rapid Commit option is supported
- The DHCPv6 Client works in an IPv6 VRF environment

Server Selection

A DHCPv6 client builds a list of potential servers by sending a solicit message and collecting advertise message replies from servers. These messages are ranked based on preference value, and servers may add a preference option to their advertise messages explicitly stating their preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.

Server Function

The DHCPv6 server function can be enabled on individual IPv6-enabled interfaces.

The DHCPv6 server is providing the following features:

- RFC3041 Compliance: IPv6 addresses will be allocated in a non-sequential fashion
- Allocating multiple IPv6 addresses to a client. (ie: if multiple address pools apply, then one address will be allocated from each address pool)
- Rapid Commit: The Rapid Commit option is supported
- The DHCPv6 server works in an IPv6 VRF environment
- The DHCPv6 server writes current allocated addresses to a TFTP server and can read currently allocated addresses back from the TFTP server upon startup
- Configuration and support of Vendor-Specific Options

DHCP Relay Agent

A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. DHCP relay agent operation is transparent to the client. A client locates a DHCP server using a reserved, link-scoped multicast address. Therefore, it is a requirement for direct communication between the client and the server that the client and the server be attached to the same link. However, in some situations in which ease of management, economy, or scalability is a

concern, it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link.

Benefits of using DHCPv6 individual Address assignment:

Flexibility, Scalability, and Customization: DHCPv6 in terms of individual address assignment now offers similar functionality as DHCPv4, which includes easy configuration of address pool and scalability.

Hardware

Routers	• Cisco 800, 1800, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/ipv6

Product Management Contact: Patrick Wetterwald, pwetterw@cisco.com

2.3) Embedded Management and Instrumentation

2.3.1) Web Services Management Agent (WSMA)
Web Services Management Agent (WSMA) allows customers, partners and developers to provision, configure, manage and adapt Cisco IOS devices using industry standard Web Services protocols. Combined with Extensible Markup Language (XML), Web Services provides secure, reliable and robust access to IOS using a familiar set of protocols already in use by the majority of customers and partners. WSMA leverages existing investments in IOS CLI as well as existing Web Services expertise and tools.

External management systems can be built to perform the following functions with a WSMA agent inside IOS:

- Retrieve configuration information in tagged and well-formed XML
- Change the running configuration using CLI or XML
- Test a candidate configuration before applying it to the running configuration
- Bulk transfer multiple CLI/Exec commands in a single Simple Object Access Protocol (SOAP) envelope
- Allow atomic rollback if a transaction fails
- Receive full audit trails of configuration changes and operation returns codes
- Control whether the WSMA agent listens for inbound sessions (listener mode) or establishes an outbound session to the external NS system (initiator mode)
- Perform “show” commands and receive the output in tagged XML format
- Copy images, apply updates and archive configurations
- Retrieve directory listings
- Run Exec commands
- Receive configuration change notifications including before and after audit trails of the configuration change
- Group Web Services using profiles which allow different transports and protocols to be assigned to different groups and services.

WSMA supports two important modes of communication; listener and initiator modes:

- **Initiator Mode**: The WSMA agent can establish an outbound session to the external NMS system to avoid opening up inbound connections to the router or switch. For customers wanting a highly secure environment which traverses firewall and resolves NAT issues, initiator mode is a significant capability
- **Listener Mode**: The WSMA listens for inbound Web Service session requests in a traditional Web Services client/server architecture

WSMA allows several highly secure methods of authentication currently used by customers; SSH and HTTPs. Future versions of WSMA support TLS as well.

Benefits

- **Increased Provisioning/Configuration Speed:** Making configuration changes through WSMA, configurations can be applied many times faster than using off-box expect scripts or manual configuration using SSH/Telnet. In addition, multiple CLI commands can be operated as an atomic operation.
- **Reduced Development Effort**: WSMA frees up web services developers to use their existing tools and expertise to rapidly build management applications. Based on industry standard web services protocols (SOAP 1.1, SOAP 1.2, etc) and transports (SSH, TLS and HTTPs) developers can rapidly build applications which are reusable and flexible.
- **Improved Automation**: In addition to return codes and audit trails, WSMA provides atomic rollback in case of failure. Should the worst occur, WSMA will return the configuration to a working state.
- **Improved Accuracy**: WSMA brings the benefits of XML and web services; accuracy and consistency. Using WSMA to provision, configure, manage and adapt a Cisco device, customers get a robust, self-describing system with the accuracy of XML access.

Hardware

Routers	• Cisco 800, 1800, 3800, 3800, 7200, 7301 Series Routers

Product Management Contact: Steve Giles, stgiles@cisco.com

2.3.2) Smart Call Home Support for the Cisco 7200 Series Router

Smart Call Home is a powerful component of Cisco SMARTnet Service that offers proactive diagnostics, real-time alerts, and personalized web-based reports on select Cisco devices.

Cisco Smart Call Home offers:

- Visibility into your network through diagnostic reports
- Real-time trouble shooting and alerts
- Automatic generation of Cisco service requests to Cisco technical engineers
- Secure, reliable data transport
- Personalized Web-based portal to review Call Home messages, detailed diagnostics, recommendations, and inventory

Cisco IOS Software Release 12.4(24)T adds Smart Call Home support for the Cisco 7200 Series Router.

Additional Information: http://www.cisco.com/go/smartcall

Product Management Contact: Tim Johnson (tijohnso@cisco.com)

2.4) Voice

2.4.1) Cisco Unified Communications Manager Express 7.1
Cisco Unified Communications Manager Express is the Cisco router based call processing solution that provides a smart, simple and robust Unified Communications solution for small and medium businesses and enterprise branch offices. Cisco IOS Software 12.4(24)T contains several new features for customers using Communications Unified Communications Manager Express.

Single Number Reach (SNR)

The Single Number Reach feature allows users to consolidate all their incoming calls into a single business phone number which reaches both their Cisco IP Phone and their cell phone. This feature enables users to answer incoming calls on their desktop IP phone or at a remote destination, such as a mobile phone.

The Single Number Reach feature includes:

1. Option to dynamically change alternate phone number from phone Telephony User Interface (TUI)
2. Allows calls to be switched between IP phone and alternate phone with the touch of a button
3. Users can toggle SNR functionality on/off from the phone

Whisper Intercom

The Whisper Intercom feature allows a receptionist to perform a whisper page to the manager phone to provide one-way voice from the calling to the called party, regardless of whether the called party is busy or idle. In case the manager is already on a call, the audio from the receptionist will not be heard on the manager's other call.

The Whisper Intercom feature includes:

1. The phone receiving a whisper page displays the extension and name of the party initiating the whisper page and Cisco Unified CME plays a zip zip tone before the called party hears the caller's voice
2. If the called party wants to speak to the caller, the called party selects the intercom button on their phone.
3. The lamp for intercom buttons is colored amber to indicate one-way audio for whisper intercom and green to indicate two-way audio for standard intercom.

SIP Line Side Enhancements

SIP Line side enhancements in Cisco Unified Communications Manager Express for Cisco SIP endpoints builds on an already robust feature set for SIP endpoints.

SIP Line Side Enhancement includes:

1. Shared line support across up to 16 Cisco SIP phones
2. Ability to barge into calls for Cisco SIP phones with shared lines
3. Calls put on hold on Cisco SIP phones with shared lines can be resumed by other shared line members

4. Privacy for SIP phones enables phone users to block other users from seeing call information or barging into a call on a SIP shared-line directory number. Users can toggle privacy on/off dynamically for shared lines.
5. Call Park and Pickup between SCCP and SIP endpoints. Both SCCP and SIP endpoints can park and retrieve calls that are parked.
6. Call Park slots can now be reserved for specific departments

Busy Lamp Field (BLF) Monitoring of Devices

Support device-based BLF monitoring, allowing a watcher to monitor the status of a phone, not only a line on the phone.

Busy Lamp Field (BLF) Monitoring of DnD, Call Park, Paging and Conferencing Directory Numbers

Provide BLF indicators for directory numbers that become DND-enabled, or are configured as call-park slots, paging numbers, or conference numbers.

SIP Trunk Video Support for SCCP Endpoints

Supports video calls between SCCP endpoints across different Cisco Unified CME routers connected through a SIP trunk. Support H.264 codec for video calls.

DSCP Enhancements

Supports Differentiated Services Code Point (DSCP) packet marking for Cisco Unified IP phones.

Multilevel Precedence and Preemption (MLPP)

MLPP service allows validated users to place priority calls, and if necessary, to preempt lower-priority calls. This capability assures high-ranking personnel can communicate with critical organizations and personnel during network stress situations, such as a national emergency or degraded network situation.

Benefits

- **Improves end user experience and productivity:** Cisco SIP IP Phone users now have access to more robust IP Telephony features available on Cisco Unified Communications Manager Express. Users have presence information for other users and can reach them seamlessly. They are also able to join calls with the touch of a button and can enable privacy to when needed.
- **Enhanced mobility:** Allows IP Phone users to provide a single number to other parties and receive calls on their desk or cell phone. This allows users to be connected while away from the office and reduces missed calls and sales opportunities.
- **Support for Public Safety and Department of Defense (DOD) initiatives:** Assure that critical calls from high ranking personnel and emergency calls are always serviced.

Hardware

Routers	• Cisco UC500, 1800, 2800, 3800 Series Routers

Additional Information: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html

Product Management Contact: Tony Huynh, tonhuynh@cisco.com

3) Release 12.4(22)T Highlights

Table 2. Release 12.4(20)T Feature Highlights

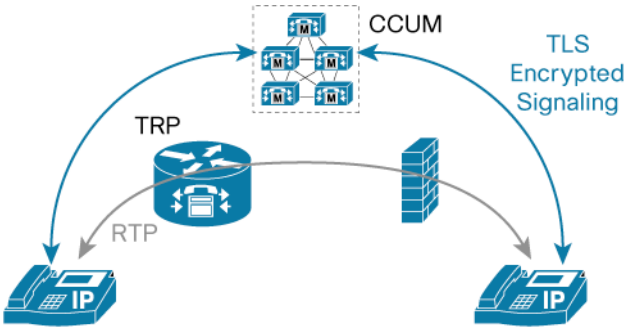
3.1) Cisco IOS Security	3.2) Embedded Management	3.3) Voice	3.4) Hardware
3.1.1) IOS Firewall Support for Trusted Relay Point (TRP) 3.1.2) Access Control List (ACL) Syslog Correlation 3.1.3) Per (DMVPN) Tunnel Quality of Service (QoS) 3.1.4) Certificate IP Address Extension Support 3.1.5) Time-based Anti-replay on VPN Services Adapter (VSA) 3.1.6) Group Encrypted Transport VPN (GET VPN) Enhancements 3.1.7) IOS SSL VPN Internationalization 3.1.8) IOS Support for Lawful Intercept	3.2.1) Cisco IOS Embedded Event Manager 3.2.2) Flexible NetFlow—NetFlow v5 Export format 3.2.3) Flexible NetFlow—TopTalkers CLI support 3.2.4) Flexible NetFlow—Multicast statistics for IPv4 support	3.3.1) Cisco VG202 and Cisco VG204 Analog Phone Gateways 3.3.2) Session Initiation Protocol (SIP) Enhancements	3.4.1) Cisco 880 3G and Cisco 880 SRST Router Series 3.4.2) Cisco IAD2435-8FXS Integrated Access Device 3.4.3) Intrusion Prevention System Enhanced Network Module

3.1) Cisco IOS Security

3.1.1) IOS Firewall Support for Trusted Relay Point

Cisco IOS firewall enhances security for Unified Communications (UC) by supporting Trusted Relay Point (TRP). This solution provides a trusted anchor within the network for seamless UC related services including media recording, QoS enforcement, and intelligent firewall traversal.

Figure 9. IOS Firewall Trusted Relay Point Use Case Scenario



Trusted Relay Point is a multi-functional architecture covering Quality of Service (QoS), Optimized Edge Routing (OER), and virtual network traversal. It eliminates the deep packet inspection and overhead associated with firewalling by signaling the firewall to permit traffic.

Benefits of UC-Trusted Firewall Control

- Provides authentication required to open port requests on the firewall
- Supports asymmetric signaling/media paths control, cases where signaling and media may not traverse the same paths in the network (such as internal “firewalling”) and might ordinarily be blocked
- Provides encrypted signaling between voice entities, cases where the firewall has the group key to look at the signaling and allow pinholes for media
- Ports for media and signaling remain open for session length only, providing more secure sessions

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.2) Access Control List (ACL) Syslog Correlation

Cisco IOS ACL Syslog Correlation feature provides a correlation mechanism for ACLs that can be used by Network Management System (NMS) tools to correlate the triggered syslog with the specific Access Control Entry (ACE) within the ACL that triggered the syslog. The ACL Syslog Correlation feature utilizes a 'tag' which is appended to the ACE generated syslog. The 'tag' can either be a user-configured alpha-numeric cookie or an IOS generated 32-bit hash. If the user does not configure the cookie, IOS will create the hash for ACEs configured with the 'log' keyword.

Figure 10. Define a tag to be used for ACE generated syslogs

```
! Define an ACE cookie to monitor access to "red-server" and "blue-server"
ip access-list extended access-control
 permit ip any host 10.10.10.100 log red-server
 permit ip any host 10.10.10.200 log blue-server
 permit ip any any
```

Figure 11. Configured tags are appended to ACE generated syslogs

```
Sep  3 16:31:18.958: %SEC-6-IPACCESSLOGDP: list access-control permitted icmp
192.168.1.100 -> 10.10.10.100 (0/0), 11 packets  [red-server]

Sep  3 16:32:18.953: %SEC-6-IPACCESSLOGDP: list access-control permitted icmp
192.168.1.100 -> 10.10.10.200 (0/0), 3 packets  [blue-server]
```

Benefits

- Provides a consistent monitoring solution for IOS ACLs, allowing network management tools to easily correlate the triggered syslog with the specific Access Control Entry (ACE) within the ACL that triggered the syslog
- Reduces complexity of managing and monitoring ACL rules for access and control by simplifying the correlation of ACE rules with their corresponding syslog events
- Assists network administrators in troubleshooting issues that occur as a result of ACE rules and allows them to monitor ACE rules' effectiveness

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, and 7200 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.3) Per Dynamic Multipoint VPN (DMVPN) Tunnel Quality of Service (QoS)

This feature enables the DMVPN hub to dynamically allocate a QoS service policy for each spoke. The DMVPN hub can have multiple QoS policies for all the remote spokes. If QoS is configured, each spoke requests a QoS policy from the hub during Next Hop Resolution Protocol (NHRP) registration. This QoS service policy is applied on the hub in the outbound direction. A typical QoS policy provides multiple classes of service, including a priority queue for voice, and traffic shaping for the total bandwidth of all classes.

Table 3. Detailed Capabilities of DMVPN Per Tunnel QoS Functionality

Feature	Benefit
Dynamic QoS policy allocation for spokes during the NHRP registration with hub	Simplifies QoS configuration on the hub router for dynamically addressed spokes
Cisco Modular QoS CLI (MQC) support configuration in every spoke policy	Allows prioritization to VoIP/delay sensitive data traffic
Protect critical control traffic before and after encryption	Enhances network stability
Dynamic QoS on the hub ensures optimal traffic flow when a spoke connects to the hub	Simplifies QoS enablement in VPN networks
Protect the crypto engine by supporting full tunnel queuing hierarchy in hierarchical queuing format; QoS queuing and shaping happens before encryption	Avoids anti-replay error reporting with IPSec
Shaping and queuing happens at the physical interface	Centralizes QoS policy in the router and simplifies configuration
Protection for critical control traffic before and after encryption	Enhances network stability
Dynamic QoS allocation on the hub router protects the spoke from traffic bursts	Protects small spokes from becoming overwhelmed from large hub sites

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, and 7200 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.4) Certificate IP Address Extension Support

This feature enables support for RFC3779, X.509 Extensions for IP addresses. One of the first protocols to use this feature will be the SEcure Neighbor Discovery Protocol (SEND). IPv6 hosts run Neighbor Discovery Protocol (NDP) to discover other devices on a link. If this link is not secured, NDP is vulnerable to various attacks such as neighbor solicitation/advertisement spoofing and duplicate address detection DoS attacks. SEND is designed to counter the threats to NDP and can use X.509 IP extensions to provide a stronger control on prefix advertisements.

Note that with SEND, RFC3779 (X.509 Extensions for IP addresses) is an optional feature. While SEND will provide its full capabilities with this version of PKI, it could still be deployed with older PKI versions that don't support IP extensions.

Benefits

- Generates certificates with IP extensions
- Counters threats to NDP
- Allows for stronger control on prefix advertisements

Hardware

Routers	• Cisco 87x, 88x, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.5) Time-Based Anti-Replay on The VPN Services Adapter (VSA)
This feature enables Time-Based Anti-Replay (TBAR) support on the VPN Services Adapter (VSA) of the 7200 NPE-G2 platform. TBAR is used in the Group Encrypted Transport VPN (GETVPN) solution to detect replay attacks since standard sequence-based anti-replay attack detection is not supported. This feature prevents 'man in the middle' attacks.

The Cisco GETVPN solution allows organizations to have branch-to-branch secure connectivity without having to incur the cost of establishing and maintaining full-mesh connections.

Benefits

- Supports anti-replay in the Cisco GET VPN solution
- Allows protection against 'man in the middle' attacks, bolstering overall GET VPN security

Hardware

Routers	• Cisco 7200 with Network Processing Engine (NPE) G2

Additional Information: http://www.cisco.com/go/vsa

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.6) Group Encrypted Transport VPN (GET VPN) Enhancements
Several new GET VPN feature enhancements are introduced in Release 12.4(22)T:

- **Passive Security Association (SA)**

  This feature enables a new mode of IPSec Security Association (SA) with GET VPN. In this mode, the SA will accept unencrypted traffic and encrypted traffic on the inbound, while it will always encrypt traffic on the outbound. Passive SA mode is configured on the Group Member (GM), and is persistent over router restarts: this allows the Group Member to modify the SAs downloaded from the Key Server (KS). Passive SA can be used similar to the SA receive-only to enable transitions in large scale deployment.

- **Fail-Close**

  This feature enables GET VPN traffic forwarding to follow the "fail-close" model, wherein an unregistered Group Member (GM) stops forwarding data packets rather than send them out unencrypted.

  The fail-close command sets up an implicit "permit ip any any" at the end of the crypto map during the pre-registration phase. Post successful GDOI registration, the "permit ip any any" is removed from the crypto map.

  You can specify exceptions that need to be forwarded in the clear, through a deny entry in the ACL. This is useful to allow routing packets and management packets from a particular host to get through. However, note that the deny ACL in the GDOI crypto map still takes precedence. After the registration is successful, the deny entry in the ACL goes away while the deny entry in the GDOI crypto map is persistent.

  Once the GM is successfully registered to all its groups, the policies downloaded from the KS take over, governing the GMs behavior and the fail-close ACL and implicit "permit ip any any" are taken out. GMs keep the policies downloaded from the KS even if the re-registration fails and IPSec SA has expired.

  When fail-close is activated, unencrypted packets are prevented prior to and during registration. Once the GM is successfully registered to all its groups however, the policies

downloaded from the KS take over, governing the GMs behavior and the fail-close ACL and implicit “permit ip any any” are dropped. GMs keep the policies downloaded from the KS even if the re-registration fails and IPSec SA has expired.

Note: GET VPN supported fail-close previously, using an interface ACL. With the above feature, interface ACL may not be required. Fail-close with interface ACL might still be useful to customers looking to enforce a policy that certain packets must always be encrypted, regardless of the downloaded key server policy.

- **Change Key Server Role**

  This feature allows you to switch the primary Key Server (KS)by forcing an election. Issuing the new **clear crypto gdoi ks coop role** command on the primary Key Server makes it relinquish the primary role and initiate an election. If the priorities have changed, a new primary will be declared elected. Note: This command does not clear any policies—it merely facilitates switching the primary KS.

- **Co-operative Key Server: Sharing Keys**

  This feature optimizes the number of rekeys that are sent out in the event of a network split, thereby allowing the network to stabilize rapidly. When there is a network split, a secondary KS takes the partition that cannot reach the primary; with this new feature, the new primary reuses the existing policies where possible. At split, the rekey is sent only if there are keys that are due to expire within the lifetime threshold (150 seconds). Unless this threshold is met, the current keys and policies are retained on the KS separated from the primary. This new ability to share the keys created by another KS reduces the number of policies to manage, thereby improving the cooperation between the KS’es.

- **Re-key From Secondary on Merge**

  This feature distributes rekeying when a partitioned network merges back. When the merge occurs, the newly-demoted secondary KS takes responsibility to send out rekeys to the group members in its database. The primary KS is freed from having to send out all rekeys, and is able to focus on sending rekeys to only the members in its own database.

Benefits

- Enables controlled deployments in phases
- Provides ability to eliminate flow of unencrypted data packets
- Allows primary key server to be changed midstream ie: for scheduled maintenance
- Optimizes cooperative key server communications during split and merge, providing better stability

Hardware

Routers	• **Group Member (GM):** Cisco 870, 88, 1800, 2800, 3800 and 7200 Series and Cisco 7301 • **Key Server (KS):** Cisco 1840, 2800, 3800 and 7200 Series and Cisco 7301

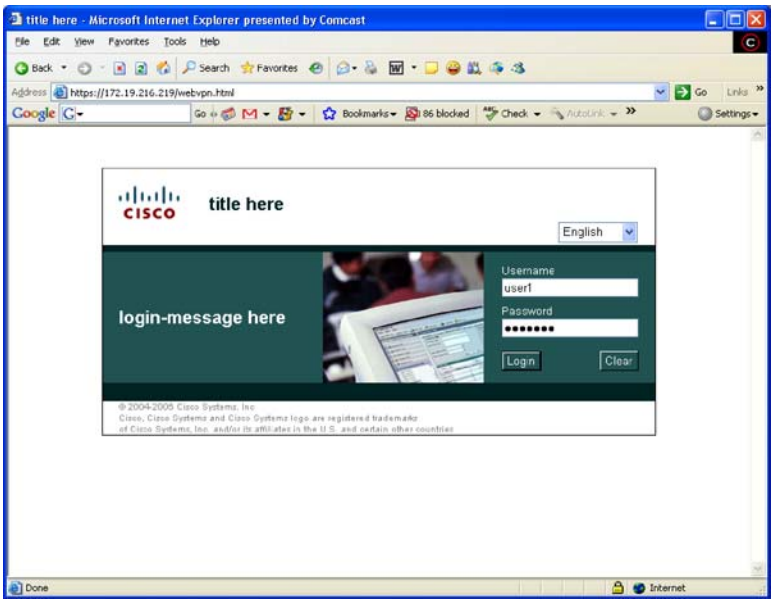
Additional Information: http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.7) IOS SSL VPN Internationalization

Cisco IOS SSL VPN Internationalization lays the framework to support multiple languages in the login and portal pages. Users will be able to select their language preference for their session from a drop down menu at the time of login.

Figure 12. IOS SSL VPN Internationalization Support



Benefits

- Allows content to be presented in the local language.

Hardware

Routers	• Cisco 87x, 88x, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

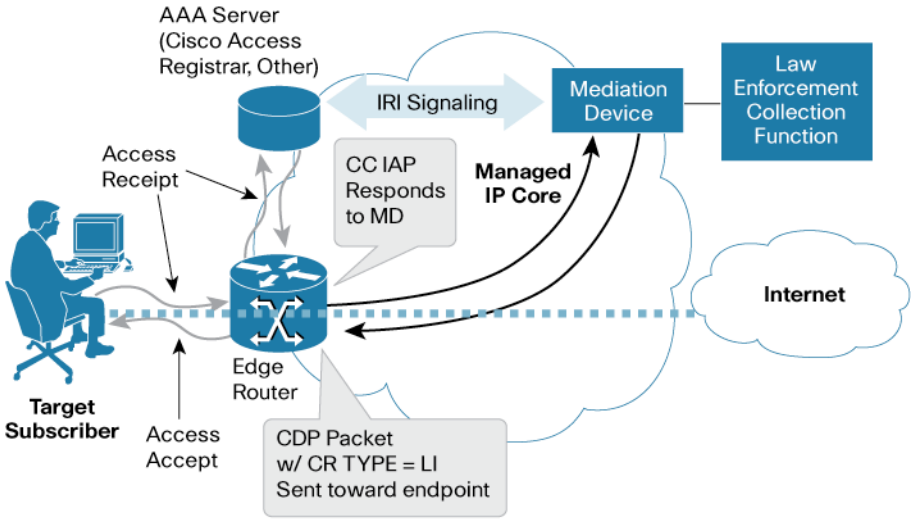
Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.8) IOS Support for Lawful Intercept

Cisco IOS provides a cost effective, yet powerful Communications Assistance for Law Enforcement Act (CALEA) compliant solution with the ability to monitor digital communications. The Cisco Service Independent Intercept (SII), Control Point Discovery (CPD) and Packet Cable 2.0 support Dynamic Discovery of Intercept Access Point (IAP). Cisco Lawful Intercept provides an out-of-band control mechanism when using a third-party mediation device to request intercepts on the network elements within the organizations trust boundaries. When performing captures for Lawful Intercept, this activity is transparent to everything else going on in the network, providing access only to authorized personnel.

Figure 13. IOS Control Point Discovery (CPD) Lawful Intercept - Use Case Scenario



1. The Cisco IOS Router will act as a platform for lawful intercept, offering a complete end-to-end solution for the network with all communication sessions and intercept details preserved.
2. The Cisco Lawful Intercept solution offers scalable packet captures and an effective, powerful solution for organizations looking to comply with CALEA requirements.

Benefits

- Cost effective way to leverage existing infrastructure to meet LI regulatory obligations
- Provides easy, proactive compliance and offers quick deployment

Hardware

Routers	• Cisco 7200 Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

3.2) Embedded Management

3.2.1) Cisco IOS Embedded Event Manager Version 3.0

The Cisco IOS Embedded Event Manager (EEM) is a unique subsystem within Cisco IOS Software. EEM is a powerful and flexible tool to automate tasks and customize the behavior of Cisco IOS and the operation of the device. Customers can use EEM to create and run programs or scripts directly on a router or switch. The scripts are referred to as EEM Policies and can be programmed using a simple CLI-based interface or using a scripting language called Tool Command Language (Tcl). EEM allows customers to harness the significant intelligence within Cisco IOS Software to respond to real-time events, automate tasks, create customer commands and take local automated action based on conditions detected by the Cisco IOS Software itself.

The latest version of the EEM subsystem within Cisco IOS Software is EEM Version 3.0.

Applications

The applications are endless and only limited by your imagination.

Suppose, for example, you would like to automatically configure a switch interface depending on the device that is connected to a port or interface, an IP phone. A script can be devised that is triggered on the interface up condition and determines the details of the connected device. Upon

discovery and verification of a newly connected IP phone, the port can be automatically configured according to prescribed parameters.

Another example might be to react to an abnormal condition, such as the detection of a high error rate on an interface, by forcing transit traffic over a more stable and error-free path. EEM can watch for the increased error rate and trigger a policy into action. The policy could notify network operations personnel and take immediate action to reroute traffic.

A third example might be to collect detailed data upon detection of a specific failure condition in order to gather information that can allow the root cause of the problem to be determined faster, leading to a lower mean time to repair and higher availability. EEM could detect a specific Syslog message and trigger a script to collect detailed data using a series of show commands. After automatically collecting the data, it can be saved to flash memory or sent to an external management system or via email to a network operator.

The control is in the network administrator's hands. You control what events to detect and what actions to take. EEM is optional—it is up to the network administrator if and when it should be used and only takes the actions you program it to take.

Features and Benefits

Cisco IOS Embedded Event Manager provides a level of embedded systems management not previously seen in Cisco IOS Software. Over twenty event detectors provide an extensive set of conditions that can be monitored and defined as event triggers. The system is extensible with new capabilities and further subsystem integration is planned. The feature is mostly product independent and available across a wide range of Cisco products. Each new version of the EEM feature introduces new event detectors or new capabilities. Consult the Cisco documentation for detailed information.

EEM Version 3.0 Enhancements

The latest version of the EEM subsystem is EEM v3.0. This version ushers in a significant number of enhancements over previous versions. This development enhances the performance, increases feature integration, adds new capabilities, and extends the flexibility, so EEM can be used in new and exciting ways.

With EEM v3.0 comes:

- Four new Event Detectors
  - Routing Event Detector

    Monitors the events relative to the Routing Information Base (RIB). Events are raised for conditions such as when a particular route is added or removed or when a route is modified.
  - Flexible NetFlow Event Detector

    Detects events related to Flexible NetFlow

    Provides a powerful set of triggers to detect and react to real-time network activity

    Triggers policies based on the detection of flows that match particular criteria such as when a new flow is seen with a particular destination IP address and port number; or detect conditions like when the rate of new flow entries exceeds some threshold you define.
  - IP SLA Event Detector

Provides event triggers based on IP SLA operation results

Integrates IP SLA directly with the EEM subsystem

Provides an event-driven mechanism to take immediate action when an IP SLA operation fails. For example, take local action to direct traffic out another interface, when an IP SLA icmp-echo operation, that pings a headquarters server over the current interface every 3 seconds, fails three times in a row.

- Enhanced CLI Event Detector

  Offers enhancements to make creation of your own custom CLI commands easier and more powerful

  Provides new event triggers when special characters like “Tab”, “?”, and the “Enter” key are seen. Provides a way for you to offer ‘help’ for your new commands and make them like Cisco-developed commands.

- High performance “Turbo” Tcl policies
  - Provides an order-of-magnitude increase in event handling
  - Up to 150 events per second depending on the product
- SNMP Library Tcl Extensions
  - Provides actions for Get, Set, and Notify for local and remote SNMP devices
  - Offers more power to communicate with neighbor devices or to interrogate local MIB variables from within your policies
- Enhanced Interactive Applets
  - Increases the power of the EEM Applet (CLI-based) policies
  - Do more without resorting to Tcl-based policies
  - Includes support for variables and logical functions and if-then-else constructs
- CLI Library Support for XML Programmable Interface
  - Provides a set of Tcl library functions to facilitate the parsing of output from the Cisco IOS CLI “format” extension in the form of: show <show-command> | format {spec-file}
  - Makes extracting data from the Cisco IOS CLI within EEM policies easier
- Support authenticating SMTP email servers
  - More practical support for email actions
- Class Based Scheduling
  - Power users have the ability to schedule policy execution according to specific requirements
- Digital Signature Support
  - Infrastructure is included to verify policies that are digitally signed by Cisco
- Additional Support for IPv6
  - The SNMP proxy feature introduced in EEM 2.4 has been enhanced to support IPv6
  - SMTP actions have been enhanced to support IPv6

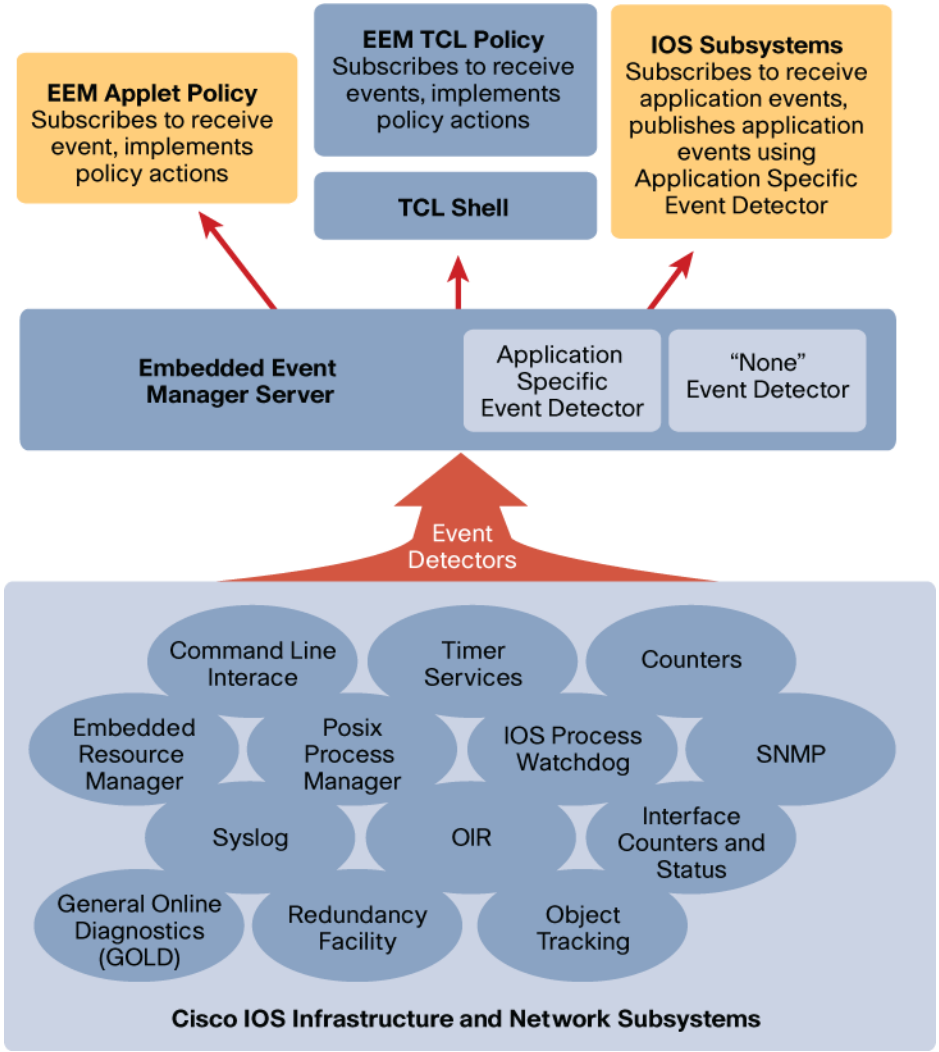
Table 4. EEM Version 3.0 Features and Benefits

Feature	Benefit
Extensible and powerful subsystem architecture	
Architecture	The EEM subsystem is designed with modularity in mind. It consists of Event Detectors, an Event Manager Server, and action routines called Policies
CLI interface	An interface to the Cisco IOS CLI to allow automated commands and access to any information that can be displayed. Includes support for XML Programmable Interface from within EEM policies.
Policy scheduler	EEM policies are scheduled one at a time or concurrently according to the number of threads configured. An enhanced class-based scheduling option for fine control over policy execution.
Built–in actions	Policies can invoke a number of built-in actions for easy automation
Extensive set of Event Detectors (ED)	
Application	Custom application events, action script interaction
Enhanced Cisco IOS CLI ED	CLI command match and run with even more capabilities for creating your own commands
Counter	Custom counter events
GOLD	Generic Online Diagnostics (GOLD) event detection
Interface	Interface counters and events
IP SLA	Tighter integration with the SLA monitoring and measurement subsystem. Easy event triggers and automation when conditions are not satisfactory.
Memory Threshold (Deprecated)	Detect memory resource related events
NetFlow	Event triggers based on traffic flow. Many uses from capacity planning to DoS alert and automated actions.
None (by run command)	Allows execution of an EEM policy by direct command, event manager run
Object Tracking	Integration with Enhanced Object Tracking (EOT)
OIR	Card Online Insertion & Removal detection
Remote Procedure Call	Allows for authorized programs outside of the device to invoke specific device-resident, embedded policies by sending a SOAP request over an SSHv2 connection.
Resource Threshold	Integration with Embedded Resource Manager, supersedes Memory Threshold ED.
RF	Cisco IOS infrastructure Redundancy Facility (RF) events
Routing	Event triggers based on routing changes
SNMP	Detect MIB Variable match and thresholds
SNMP Proxy	Creates events when a specified SNMP trap or inform is received at the device. This allows for policies to be triggered by events from other devices.
Syslog	Regular expression pattern match on emitted Syslog messages
Timer	Custom timed events
IOS Watchdog Monitor	Cisco IOS scheduler, watchdog events
WDSysMon	Cisco IOS Software Modularity: System monitor event
Secure system operation	
EEM scripts run within system constraints	Protects system from harm. ie: A looping script will not stop Cisco IOS
User scripts run in Safe-Tcl mode	Certain programmable options are disabled for protection
Controlled environment	Only a network administrator with privileged access can define and set up EEM scripts. No one else can install software to compromise the system.
Support for TACACS+/RADIUS	EEM scripts can be associated with a configured User ID. All CLI commands issued by the scripts are authorized before they are executed.
EEM is optional	If you don’t want to use this powerful capability, you don’t have to enable it.
Online scripting community	
Cisco Beyond—Product Extension Community	A place for customers to share and download scripts. Don’t reinvent the wheel. Build and extend the work of others. Learn by example. Go to: http://www.cisco.com/go/ciscobeyond

Product Architecture

The Cisco IOS Embedded Event Manager is a primarily product independent software feature consisting of a series of Event Detectors, an Embedded Event Manager Server, and interfaces to allow action routines called Policies to be invoked. There are also internal application programming interfaces for other Cisco IOS subsystems to take advantage of the EEM subsystem. The diagram in Figure 10 illustrates the EEM components.

Figure 14. EEM Architecture



Notice there are two types of EEM Policies:

- Applet Policies—Easy-to-use interface, defined using the configuration CLI
- Tcl Policies—More flexible and extensive capabilities, defined using the Tcl programming language

Once one or more policies are defined, the Event Detector software will watch for the conditions that match those defined by the policy. When a condition occurs, the event is passed to the Event Manager Server. The server then invokes any policy that has registered for that particular event. The actions defined within the policy are then carried out.

Each type of event has specific options, parameters and detailed information that is available to the policy when it is invoked. All of these details are described in the Cisco IOS documentation.

Feature Specifications

Please use the Cisco IOS Feature Navigator application on Cisco.com to check the latest information on software and product availability. Go to: http://cisco.com/go/fn. The following table includes EEM feature availability information.

Table 5. EEM Feature Specifications

Product compatibility	EEM is available for the Catalyst 6500 Series Switches, Cisco Integrated Services Routers, Cisco 7200 Series Routers, Cisco 7300 Series Routers, Cisco 7600 Series Routers, Cisco 10000 Series Routers; EEM is also available for the Catalyst 4500 Series Switches and the Catalyst 3700 Series Switches and the ASR-1000 Series Routers. Please refer to the Cisco IOS Feature Navigator for the latest device support information.
Software compatibility	EEM is available in Cisco IOS Software Releases 12.2SX, 12.2SR, 12.2SB, 12.4, and 12.4T, 12.2SG, 12.2SE, Cisco IOS XE and future versions. EEM function is also included in Cisco IOS XR and Cisco NX OS.
Software Packaging	Some Cisco products require an enhanced feature set license to acquire support for EEM. Please refer to the Cisco IOS Feature Navigator for the latest packaging information.

System Requirements

The EEM software subsystem will consume CPU and memory resources in its operation. Tcl-based policies reside on flash disk and will take up space. Customers should examine the operation in their environment to ensure resources exist for their specific scenarios. Some basic guidelines are included in Table 5.

Table 6. EEM System Requirements

Disk Space	Tcl-based policies are files stored on flash disk. The amount space required depends on the size and number of policies and any programmed storage requirements
Hardware	CPU utilization requirements are solution dependent
Memory	Each Tcl-based policy will use approximately 500KB when initialized. Beyond that utilization is specific to the policy's operational requirements
Software	A Tcl interpreter is included within the Cisco IOS Software. The current version is Tcl 8.3.4.

For More Information

For more information about the Cisco IOS Embedded Event Manager, visit http://cisco.com/go/eem or contact your local account representative or send email to askabouteem@cisco.com.

Product Management Contact: Rick Williams, rwill@cisco.com

3.2.2) Flexible NetFlow—NetFlow v5 Export Format

Flexible NetFlow exporter introduces the support of NetFlow v5 export format. NetFlow v5 export format must be used in conjunction with the v5 tupple in Flexible NetFlow (FNF) for one pre-defined flow record named original-NetFlow.

When transitioning from traditional NetFlow to Flexible NetFlow, the user will be able to create a Flow Monitor with the original-NetFlow record and export it using NetFlow v5 to the existing NetFlow v5 collector. In addition, the user will be able to create a second Flow Monitor to take advantage of other innovative FNF capabilities, such as Flow record customization and NetFlow v9 export.

Benefits

- Enable smooth migration from traditional NetFlow to Flexible NetFlow.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7300 Series Routers

Additional Information:

- http://www.cisco.com/go/netflow
- http://www.cisco.com/go/fnf

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

3.2.3) Flexible NetFlow—TopTalkers CLI Support

Understanding who is using the network and for how long, what protocols and applications are being utilized and where the network data is flowing is a necessity for today's IP network managers. NetFlow data can be used for a variety of purposes, including network management and planning, user and security monitoring, protocol and application monitoring, Enterprise accounting, and departmental charge backs, Internet Service Provider (ISP) billing, data warehousing, and data mining for marketing purposes.

Flexible NetFlow CLI is used extensively for troubleshooting and understanding network behavior. Flexible NetFlow CLI has been enhanced to provide advanced search capabilities. The new CLI provides a generic set of tools to display any kind of Flow Monitor (IPv4, IPv6, Layer2, etc.) in a more efficient way. Flexible NetFlow CLI allows filtering, aggregating and sorting the content of a Flow Monitor:

- **Flow Filtering**: The user will be able to filter on any field available in the Flow Record used by the Flow Monitor being examined. The filtering can be an exact match or a match on a range or a regular expression.
- **Flow Aggregation**: The user will be able to display the Flows that are formed by aggregating any subset of the key fields available in the Flow Record used by the Flow Monitor being examined.
- **Flow Sorting**: the user will be able to control the sorting of Flows using the fields that are available in the FNF Cache to be shown. This could be the primary or secondary (post aggregation step) cache.

Benefits

- **Security**: Able to view the list of top talkers to see if traffic patterns consistent with a Denial of Service (DoS) attack are present in the network.
- **Load balancing**: Able to identify the most heavily used parts of the system and move network traffic over to less-used parts of the system
- **Traffic analysis**: Consulting the data retrieved Top talker CLI
- Talkers feature can assist in general traffic study and planning for the network.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7300 Series Routers

Additional Information:

- http://www.cisco.com/go/netflow
- http://www.cisco.com/go/fnf

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

3.2.4) Flexible NetFlow—Multicast Statistics for IPv4 Support

The Flexible NetFlow IPv4 Multicast support feature allows users to capture multicast-specific data (both packets and bytes) for multicast flows. For example, you can capture the packet replication factor for a specific IPv4 flow, as well as for each outgoing stream.

Flexible NetFlow IPv4 Multicast Support feature can identify and count multicast IPv4 packets on the ingress side or the egress side (or both sides) of a router. Multicast ingress accounting provides information about the source and the number of times the traffic was replicated. With multicast ingress accounting, the destination interface field will be set to null, and the IP next hop field is set to zero for multicast flows. Multicast egress accounting creates a unique flow record for each outgoing interface.

Flexible NetFlow IPv4 Multicast Support feature lets you enable NetFlow statistics to account for all packets that fail the Reverse Path Forwarding (RPF) check, that are dropped in the core of the service provider network. Accounting for RPF-failed packets provides more accurate traffic statistics and patterns.

Flexible NetFlow IPv4 Multicast requires NetFlow v9 export format to export Multicast statistics.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7300 Series Routers

Additional Information:

- http://www.cisco.com/go/netflow
- http://www.cisco.com/go/fnf

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

3.3) Voice

3.3.1) Cisco VG202 and Cisco VG204 Analog Phone Gateways

The Cisco VG202 and Cisco VG204 Analog Phone Gateways are Cisco IOS Software-based analog voice gateways, which extend the Cisco VG224 offering. The Cisco VG202 and Cisco VG204 offer 2 FXS ports and 4 FXS ports per unit, respectively. Integrating into the Cisco Unified Communications solution for Enterprise branch offices and SMBs just like the Cisco VG224, these analog voice gateways enable analog phones, fax machines and modems to connect to an IP infrastructure. They will be supported by the Cisco Unified Communications Manager releases 6.1(3) and 7.0(1) or later. The Cisco VG202 and Cisco VG204 offer, in a desktop form-factor with fanless design, the entire set of rich Cisco IOS Software based voice and security features offered by the VG224. They also offer proven DSP technology that is consistent across the VG224 and the Cisco Integrated Services Router Voice Gateways.

Additional Information:
http://www.cisco.com/en/US/products/hw/gatecont/ps2250/ps5627/index.html

Product Management Contact: Jay Chokshi, jayesh@cisco.com

3.3.2) Session Initiation Protocol (SIP) Enhancements

Cisco is consistently leading the development of Session Initiation Protocol (SIP). This is part of IOS that runs on all routers in the Integrated Services Router (ISR) portfolio. This is also a key development for the unified communications solution for service providers, Enterprises, SMBs and small branch offices that provide voice, data, voicemail, Automated-Attendant, video, and security capabilities.

In this current release, core components include the following:

- RSVP Preconditions (RFC3312) for TDM Gateway and Cisco Unified Communications Manager Express. It extends negotiation of RSVP CAC/QoS across CUCM clusters*, Gateways, CUCME and CUBE
- Audio RSVP enhancements to support RE-INVITE or 302-Response based supplementary services on gateways
- RSVP support on the SIP trunk of SCCP-CUCME
- SIP SRTP Fallback to Non-secure RTP and SRTP over sip: scheme for CUBE:

This feature extends the existing SRTP fallback on the SIP-TDM gateway to interoperate with the SRTP fallback method of CUCM on SIP trunk. It adds the CUCM interoperable SRTP fallback support to SIP-SIP and SIP-H323 call-flow of CUBE. This is supported on CUBE for the following call flows—EO-EO, DO-DO, FS-EO, EO-FS, SS-DO:

- SIP Diversion Header Enhancements
- SIP History INFO (RFC 4244): Many services that SIP is anticipated to support, require the ability to determine why and how the call arrived at a specific application. SIP History-Info header provides a standard mechanism for capturing the request history information to enable a wide variety of services for networks and end-users. The History-Info header provides a building block for development of new services.
- SIP Multicast Music on Hold: When the IP-Phone puts a call on hold, the CUCM will ask the MOH server to stream the RTP packets on a pre-configured multicast address. The CM will also send mid-call Invite with Send-Only attribute and multicast address to the IOS SIP gateway to listen on that multicast address.

*Need the correct version of CUCM

Additional Information:
http://www.cisco.com/en/US/products/ps6790/Products_Sub_Category_Home.html

Product Management Contact: David Sauerhaft, dsauerha@cisco.com

3.4) Hardware

3.4.1) Cisco 880 3G and Cisco 880 SRST Router Series

Cisco Systems is pleased to announce the orderability of the Cisco 880 3G and Cisco 880 SRST Router Series. The Cisco 880 Series is part of the Cisco 800 fixed-configuration router family and offers Internet access, security, voice, and wireless services over broadband speeds in a single, secure device that is simple to use and manage, for small businesses and small remote offices.

The Cisco 880 Series Integrated Services Routers are fixed-configuration routers that provide collaborative business solutions for secure data communication to small businesses and Enterprise teleworkers. The Cisco 880 Series offers concurrent broadband services over 3G, Metro Ethernet, and multiple types of DSL for business continuity. Wireless 802.11n and 3G offer LAN and WAN mobility.

Figure 15. Cisco 880 3G and Cisco 880 SRST Router Series

The 880G Series with the 3G Wireless option offers a cost-effective, rapidly deployable, reliable and secure backup solution. In addition to 3G Wireless WAN, the Cisco 880G Series offers additional WAN options like xDSL and Fast Ethernet (FE) WAN interface, a 4-port 10/100 FE managed switch with VLAN support and the latest 802.11n Wireless LAN capability. The 880G Series supports the latest 3G standards (HSPA and EVDO Rev A) and are backward compatible with UMTS/EDGE/GPRS and EVDO Rev0/1xRTT respectively. The 880G series has 2 variants:

- GSM/UMTS models are based on 3GPP and support HSPA, UMTS, EDGE and GPRS
- CDMA models are based on 3GPP2 and support EVDO RevA/Rev0 and 1xRTT

The Cisco 880 SRST Series is ideal for small remote sites and teleworkers who need to be connected to a larger Enterprise. These routers help extend corporate networks to secure remote sites while giving users access to the same applications found in a corporate office. The Cisco 880 SRST Series routers offers WAN options like xDSL and Fast Ethernet (FE) WAN interface, a 4-port 10/100 FE managed switch with power over Ethernet, and the latest 802.11n Wireless LAN capabilities. Additionally, the Cisco 880 SRST Series offers 4 FXS ports, FXO or BRI for PSTN connectivity, and a 4 SRST user license.

Table 7. Cisco 880 3G and Cisco 880 SRST Router Series Part Numbers

Part Number	Product Name
Ethernet and 3G	**Configurable 3G Bundles**
CISCO881G-K9	Cisco 881 Ethernet Security Router with 3G
CISCO881GW-GN-A-K9	Cisco 881 Ethernet Security Router with 3G, 802.11n FCC Compliant
CISCO881GW-GN-E-K9	Cisco 881 Ethernet Security Router with 3G, 802.11n ETSI Compliant
G.SHDSL and 3G	**Configurable 3G Bundles**
CISCO888G-K9	Cisco 888 G.SHDSL Router with 3G

Part Number	Product Name
CISCO888GW-G-AN-K9	Cisco 888 G.SHDSL Wireless Router with 3G; 802.11n FCC Compliant
CISCO888GW-G-EN-K9	Cisco 888 G.SHDSL Wireless Router with 3G; 802.11n ETSI Compliant
SRST	
C881SRST-K9	Cisco 881 SRST Ethernet Security Router with FXS, FXO
C881SRSTW-GN-A-K9	Cisco 881 SRST Ethernet Security Router with FXS, FXO; 802.11n FCC Compliant
C881SRSTW-GN-E-K9	Cisco 881 SRST Ethernet Security Router with FXS, FXO; 802.11n ETSI Compliant
C888SRST-K9	Cisco 888 SRST G.SHDSL Router with FXS, BRI
C888SRSTW-GN-A-K9	Cisco 888 SRST G.SHDSL Router with FXS, BRI; 802.11n FCC Compliant
C888SRSTW-GN-E-K9	Cisco 888 SRST G.SHDSL Router with FXS, BRI; 802.11n ETSI Compliant

Additional Information:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542.html

Product Contact: Contact your Cisco representative or visit http://www.cisco.com/go/isr.

3.4.2) Cisco IAD2435-8FXS Integrated Access Device
The Cisco IAD2435-8FXS Integrated Access Device provides small and medium-sized businesses with a cost effective platform for managed data, voice, and security services.

The Cisco IAD2435-8FXS Series offers unparalleled value to both Small and Medium-sized Businesses (SMBs) and service providers delivering managed services to these customers. As an addition to the Cisco IAD2430 Series Integrated Access Device Family, IAD2435-8FXS comes loaded with integrated features and services and is designed with the scalability required for delivering managed solutions for broadband data, packet voice, unified communications and security —all in one router platform.

Cisco IAD2435-8FXS Integrated Access Device is a fixed configuration platform and comes with the following hardware and support for industry standard voice protocols like SIP, MGCP and H.323:

- 1 T1/E1 WAN Port
- 8FXS Voice Ports
- 2 10/100Mbps Ethernet Ports
- 1 Console/Aux Port

Product Contact: Contact your Cisco representative or visit http://www.cisco.com/go/iad.

3.4.3) Intrusion Prevention System Enhanced Network Module
Intrusion Prevention System Enhanced Network Module is an integrated IPS module on the Cisco 2811, 2821, 2851 and 3800 Series Routers. It provides an advanced and accelerated threat control to protect the SMB and branch offices and extend the security perimeter out to the entire corporate network. The IPS NME has the following features:

- Supports inline and promiscuous modes upon configuration
- Runs same software (CIPS 6.1) and features as Cisco IPS 4200
- Has dedicated CPU and DRAM to offload host CPU

- Runs up to 75 Mbps
- Can be managed by Cisco IPS Device Manager (IDM), Cisco Configuration Professional (CCP), Cisco Security Manager (CSM), IPS Manager Express (IME) and CS-MARS

Figure 16. Intrusion Protection System Enhanced Network Module

Additional Information: http://www.cisco.com/go/ipsnme

Product Management Contact: ask-ips-pm@cisco.com

4) Release 12.4(20)T Highlights

Table 8. Release 12.4(20)T Feature Highlights

4.1) Cisco IOS Security	4.2) Cisco IOS Infrastructure	4.3) MPLS	4.4) Quality of Service
4.1.1) Group Encrypted Transport VPN (GET VPN) Support for the Cisco VPN Services Adapter (VSA) for Cisco 7200 NPE-G2 Series Routers 4.1.2) Cisco IOS Content Filtering 4.1.3) VRF-Aware Cisco IOS Intrusion Prevention System (IPS) 4.1.4) User-based Cisco IOS Firewall 4.1.5) Application Inspection and Control for Simple Mail Transfer Protocol (SMTP) 4.1.6) Cisco IOS Firewall Support for Skinny Local Traffic 4.1.7) Cisco IOS Firewall Session Initiation Protocol (SIP) Application Layer Gateway (ALG) Enhancements 4.1.8) Cisco IOS Firewall H.323 Version 3 (v3) and Version 4 (v4) Support 4.1.9) Instant Messaging Blocking Support in Cisco IOS Firewall for "I Seek You" (ICQ) and Windows Messenger 4.1.10) Object Groups for Access Control Lists (ACLs) 4.1.11) Cisco IOS SSL VPN Access Control Enhancements 4.1.12) Cisco IOS SSL VPN AnyConnect Client Support 4.1.13) Cisco IOS SSL VPN Back End HTTP Proxy 4.1.14) Cisco IOS SSL VPN Full-Tunnel Performance Enhancements 4.1.15) Cisco IOS SSL VPN URL Split Rewrite Support 4.1.16) Next Hop Resolution Protocol (NHRP) MIB for Dynamic Multipoint VPN (DMVPN) 4.1.17) IPv6 Over Dynamic Multipoint VPN (DMVPN) Support 4.1.18) Group Encrypted Transport (GET) VPN Support for VRF-Lite 4.1.19) Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients 4.1.20) IPSec Usability Enhancements 4.1.21) Secure Shell Protocol Version 2 (SSHv2) Feature Enhancements 4.1.22) Command Line Interface (CLI) for Displaying Certificates 4.1.23) CLI to Control Certification Revocation List (CRL) Cache 4.1.24) Secure Device Provisioning (SDP) Connect Template	4.2.1) Cisco Express Forwarding Scalability and Selective Rewrite (CSSR) 4.2.2) Network Time Protocol (NTP) Version 4	4.3.1) Cisco IOS MPLS Label Distribution Protocol (LDP) Enhancements 4.3.2) Cisco IOS MPLS Traffic Engineering and Resource Reservation Protocol (TE/RSVP)	4.4.1) Cisco IOS QoS: Hierarchical Queuing Framework (HQF) 4.4.2) Resource Reservation Protocol (RSVP) Penultimate Hop Overwrite

4.5) IP Version 6	4.6) Embedded Management	4.7) Hardware	4.8) Voice
4.5.1) IPv6 VPN Provider Edge Router (6VPE) over MPLS 4.5.2) IPv6 Access Control List (ACL) enhancements for IPv6 IPSec Authentication Header (AH) 4.5.3) Mobile Network v6—Basic NEMO Support	4.6.1) Cisco IOS Service Diagnostics 4.6.2) Embedded Event Manager Version 2.4 4.6.3) Cisco IOS Embedded Packet Capture 4.6.4) Flexible NetFlow (FNF) Exporter—Outgoing Features Support 4.6.5) Flexible NetFlow for IPv6 4.6.6) Deprecating NetFlow for IPv6 Record	4.7.1) Cisco 1861 Integrated Services Router 4.7.2) Intrusion Prevention System (IPS) Advanced Integration Module 4.7.3) Cisco 860 and 880 Series Routers 4.7.4) Cisco Business-Class IAD880 Series Integrated Access Devices	4.8.1) Communications Manager Express (CME) 7.0 Voice Features 4.8.2) Survivable Remote Site Telephony 7.0 Voice Features 4.8.3) Cisco Unified Border Element (CUBE) 1.2 4.8.4) Voice Quality Improvements on Cisco VoIP Gateways

4.1) Cisco IOS Security

4.1.1) Group Encrypted Transport VPN (GET VPN) Support for the Cisco VPN Services Adapter (VSA) for Cisco 7200 NPE-G2 Series Routers

Cisco IOS Release 12.4(20)T adds GET VPN support for the Cisco VSA, the latest high-performance encryption and key-generation services module for IPSec VPN applications on Cisco 7200 NPE-G2 Series Routers.

GET VPN offers a new standards-based IP Security (IPSec) security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPSec tunnel relationship. GET VPN simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity.

Benefits

The VSA offers increased IPSec performance over the Cisco VPN Acceleration Module 2+ (VAM2+) module.

Hardware

Routers	• Cisco 7200 NPE-G2 Series Routers

Additional Information:

http://www.cisco.com/go/vsa

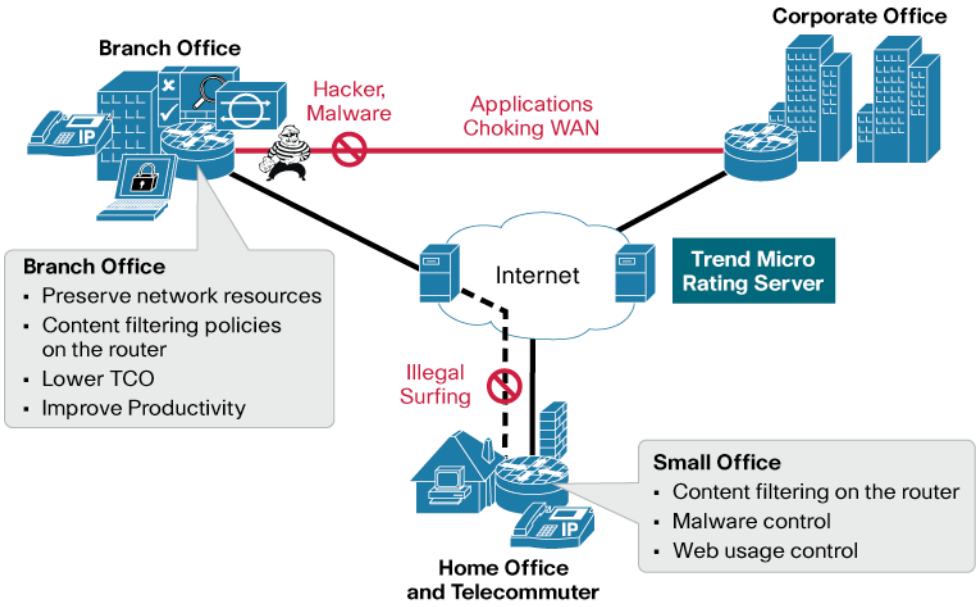
http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.2) Cisco IOS Content Filtering

Cisco IOS Content Filtering offers category-based productivity and security ratings. Content-aware security ratings protect against malware, malicious code, phishing attacks, and spyware. URL and keyword blocking help to ensure that employees are productive when accessing the Internet. This is a subscription-based hosted solution that leverages Trend Micro’s global TrendLabs™ threat database, and is closely integrated with Cisco IOS Software. It is supported on routers running the Advanced Security image. Feature licenses can be purchased directly from the Cisco.com ordering tool or through your Cisco partner/account team.

Figure 17. IOS Content Filtering Use Case Scenario



Benefits

- Secures Internet access to branch, without the need for additional devices
- Controls spyware and malware at the remote site; conserves WAN bandwidth
- Improves employee productivity and protects network resources by enabling content filtering

Hardware

Routers	• Cisco 800, 1800, 2800, and 3800 Series Routers

Additional Information: http://www.cisco.com/go/ioscontentfiltering

Product Management Contact: ask-stg-ios-pm@cisco.com

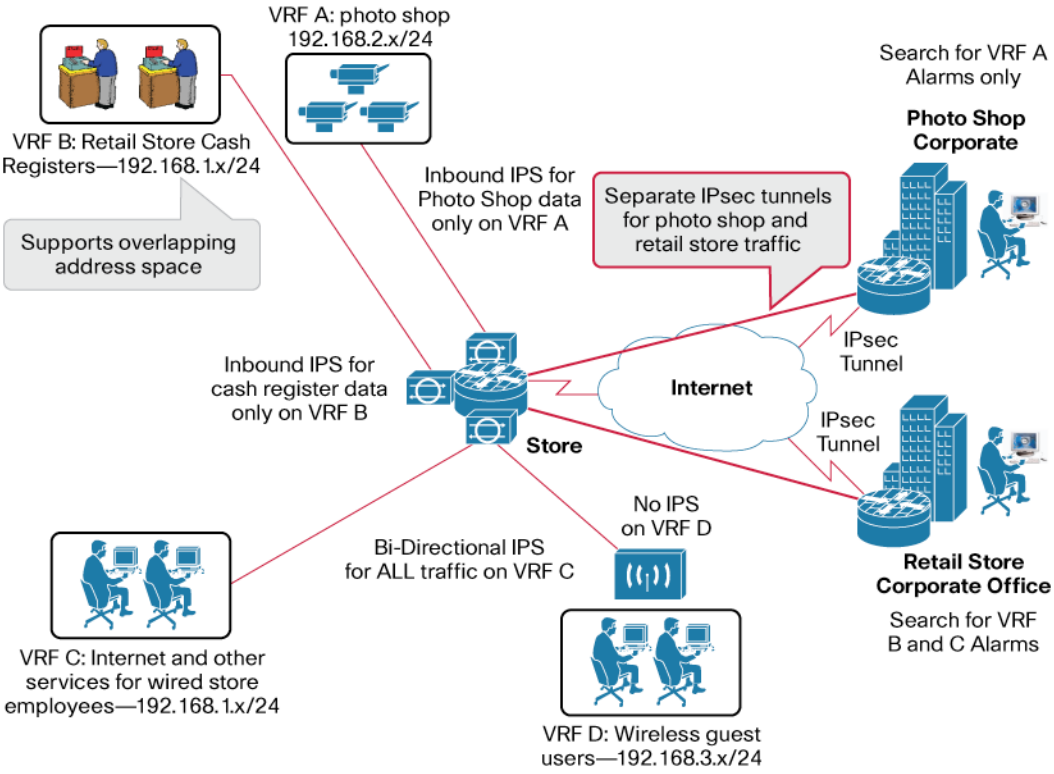
4.1.3) VRF-Aware Cisco IOS Intrusion Prevention System (IPS)

VRF-Aware Cisco IOS IPS allows Enterprises or service providers to put different groups of users or network segments into separate Virtual Routing and Forwarding (VRF) groups and to configure IPS on only certain VRFs or to configure IPS differently on each VRF. Divisions or functional groups separated by VRF segments may have different threat protection needs. Examples include:

- Vendor-provided applications vs. native applications
- Administrative users vs. regular employees vs. contractors/guests
- Vendor (photo shop, deli, pharmacy, etc.) network vs. point-of-sale network
- Students vs. faculty members vs. school administration

VRF-aware Cisco IOS IPS will also enable network security operators to distinguish between the IPS event alarms generated within each user group or network segment based on their VRF ID.

Figure 18. Typical Use Case for VRF Aware Cisco IOS IPS



Benefits

- Allows the configuration of IPS on only certain virtual network segments (VRFs) or in a different way on each VRF
- Distinguishes between IPS alarms/events generated within each group (VRF segment) based on VRF ID
- Supports IPS on VRF interfaces in addition to physical interfaces with or without overlapping IP addresses

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, and 7200 Series Routers

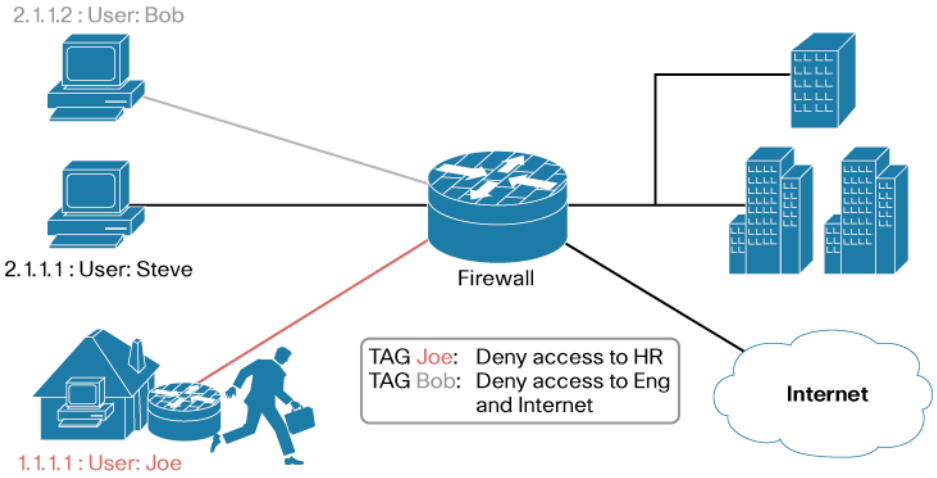
Additional Information: http://www.cisco.com/go/iosips

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.4) User-based Cisco IOS Firewall

Cisco IOS Firewall offers the ability to deploy secure access policies at all network interfaces: Internet perimeter, remote-site connectivity, business-partner access, and telecommuter connections. User-based Cisco IOS Firewall dynamically binds unique zone-based firewall policies to a group where members, regardless of IP address entry point, are authorized using authentication proxy or Network Admission Control (NAC).

Figure 19. User based Cisco IOS Firewall Example



Benefits

- Facilitates the support of Enterprise mobile workers where user access is dynamic, while maintaining source IP address and user group associations
- Secures granular access to the branch, without the need for additional devices
- Enforces non-intrusive, per-user security policies

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200 Series, 7301 Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.5) Application Inspection and Control for Simple Mail Transfer Protocol (SMTP)
Cisco IOS Firewall Application Inspection and Control (AIC) has expanded the SMTP capability to support a more detailed inspection, providing more control over how SMTP inspection is performed.

Benefits

- Inspects SMTP at a more granular level
- Scans actual e-mail data like attachment types and encoding types
- Detects a limited number of attack signatures
- Ability to use signatures in SYSLOG message alerts to warn of a possible attack, such as the detection of illegal SMTP commands in a packet

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.6) Cisco IOS Firewall Support for Skinny Local Traffic

Cisco IOS Firewall enhances Skinny Local Traffic support. This feature offers inspection for locally generated and locally terminated SKINNY protocol data in two main deployment scenarios:

1. Cisco Call Manager Express (CME) is enabled on the Cisco IOS Firewall and manages the VoIP phones using SCCP over intranet or Internet.
2. Analog and VoIP phones are connected and managed by the Cisco IOS Firewall-enabled CME router.

Benefits

- Improves user groups SCCP locally generated traffic support
- Provides inspection of CME using SCCP over the intranet/Internet

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.7) Cisco IOS Firewall Session Initiation Protocol (SIP) Application Layer Gateway (ALG) Enhancements

Cisco IOS Firewall SIP ALG and protocol inspection feature prevents unauthorized calls, call hijacking, SIP protocol exploits, and related DoS attacks. It supports both pass-through and local traffic.

Benefits

- Removes malformed packets from reaching Cisco Unified Communications Manager at the head office

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.8) Cisco IOS Firewall H.323 Version 3 (v3) and Version 4 (v4) Support

Cisco IOS Firewall adds support for H.323 v3 and v4 to maintain high availability of mission-critical IP telephony calls while upholding high level call experience.

Benefits

- Includes H.323 v3 and v4 Annex E, Annex G, and Annex D support
- Supports H.323 v3 and v4 fax and call transfer capabilities

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.9) Instant Messaging Blocking Support in Cisco IOS Firewall for “I Seek You” (ICQ) and Windows Messenger

Cisco IOS Firewall Application Inspection and Control (AIC) adds comprehensive management and control of Instant Messaging (IM) applications such as ICQ and Windows Messenger.

Benefits

- Detects, blocks or throttles ICQ and Windows Messenger services
- Enforces associated policy of “I Seek You” (ICQ) Instant Messenger Version 2001b and above as well as Windows Instant Messenger Version 5.1
- Provides granular control when managing things such as file transfers and attachments, application sharing, games, video/audio conferencing, and pop-ups
- Offers the ability to send syslog information of the event

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.10) Object Groups for Access Control Lists (ACL)

ACL Object Groups allow network administrators to classify users, devices, and protocols into groups allowing them to apply policies based on group classification. IP hosts and networks, protocols and ports are defined in object groups. Once configured, object groups can then be used in the place of IP addresses, protocols or ports within Access Control Lists (ACLs).

The two steps required to configure object groups for ACLs is shown below:

Step 1. Define the Object Group:

```
! Define network type object-groups to group IP hosts and networks
object-group network Engineering
  10.240.12.0 255.255.255.0
  10.245.10.0 255255.255.0
object-group network Web-Servers
  10.1.1.0 255.255.255.0
   host 10.10.10.100
object-group network Mail-Servers
  10.32.1.0 255.255.255.0


! Define a service type object group to group you protocols and ports
object-group service Web-ports
```

```
  tcp www
  tcp 8080
object-group service Mail-ports
  tcp smtp
  tcp pop3
  tcp 587
  tcp 143
```

Step 2. Use Object Groups in ACL Configurations:

```
ip access-list extended access-policy
  10 permit object-group Web-ports object-group Engineering object-group
Web-Servers
  20 permit object-group Mail-ports object-group Engineering object-group
Mail-Servers
```

Benefits

- Provides a simple and intuitive mechanism for configuring and managing large ACLs, especially ones that frequently change
- Reduces ACL configuration size and make ACLs more readable and easier to manage

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.11) Cisco IOS SSL VPN Access Control Enhancements

Depending on the network security design, the need to repeatedly provide user credentials to gain secure access may be redundant. This is especially true for cellular providers that authenticate users as they join the network. Using Cisco IOS SSL VPN Access Control Enhancements, login credentials can be embedded in the URL used by the client machine to connect to the SSL VPN gateway. Users would not be challenged for credentials but would instead immediately start their secure SSL VPN session.

Benefits

- Simplifies the user login procedures
- Reduces intrusive and repetitive login prompts

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.12) Cisco IOS SSL VPN AnyConnect Client Support

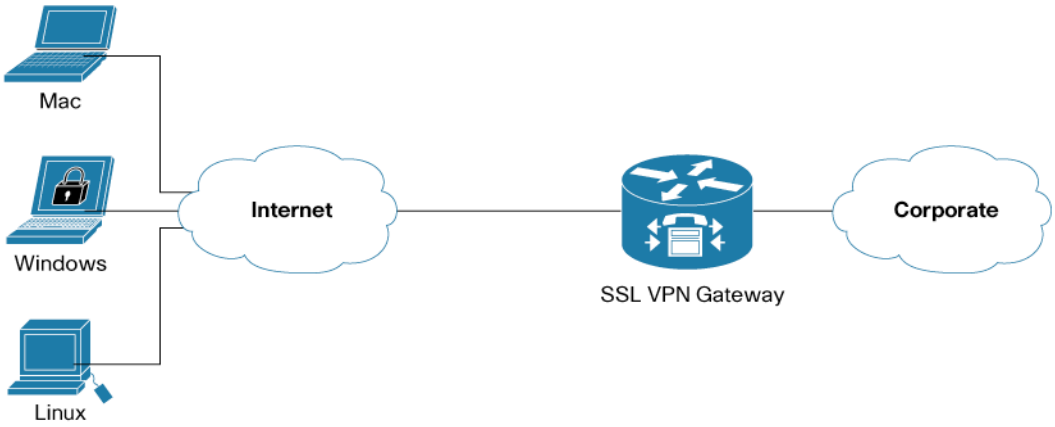
AnyConnect is the Cisco next generation SSL VPN client. It replaces the current Cisco SSL VPN Client (SVC), and requires no pre-installation or pre-configuration on the client machine.

The Cisco IOS SSL VPN AnyConnect Client is pushed from the secure gateway to the client machine when needed. Traffic is encrypted and authenticated using a Layer 2 tunneling functionality that is similar to traditional IPSec, and is agnostic to traffic type. Performance is greatly improved because there is no need to apply URL mangling on the secure traffic as is required with clientless connections.

AnyConnect provides added functionality beyond the current SVC client with support for multiple operating systems including Windows Vista, Apple Mac OS X, and Linux. Administrators can now support a mixed operating system network environment.

Once pushed down to the user, the Cisco AnyConnect client can be configured to stay installed so that subsequent connections do not require repeated downloads and installations. Standalone mode allows users to initiate new SSL VPN tunnel sessions without the need of a web browser, simplifying the login procedure.

Figure 20. Cisco IOS SSL VPN AnyConnect Client Support



Benefits

- Avoids pre-configuration and pre-installation requirements
- Improves performance over clientless only traffic
- Offers support for multiple operating systems
- Reduces bandwidth requirements in Standalone mode

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.13) Cisco IOS SSL VPN Back End HTTP Proxy

In the past, all clientless mode user requests were sent to internal servers directly. This meant that the internal servers had to be directly addressable by the SSL VPN gateway for connectivity to

succeed. This feature enhancement adds HTTP proxy client functionality to the Cisco IOS SSL VPN gateway so requests can now be passed through to an internal proxy server in the protected network.

Benefits

- Provides increased flexibility and control in supporting more diverse internal network architectures

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.14) Cisco IOS SSL VPN Full-Tunnel Performance Enhancements

Cisco Express Forwarding (CEF) Scalability and Selective Rewrite (CSSR) technology for IP has been added to full-tunnel mode as well as clientless SSL VPN deployments. Combining CSSR with SSL VPN full-tunnel traffic provides greater throughput and reduces router CPU utilization.

Note: CSSR, supported in Cisco IOS Release 12.4(20)T onward, is a scalable, distributed, Layer 3 switching technology designed to meet the future performance requirements of Enterprise networks. Refer to the Cisco IOS Infrastructure section for more information on CSSR support.

Benefits

- Increases scalability and performance

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

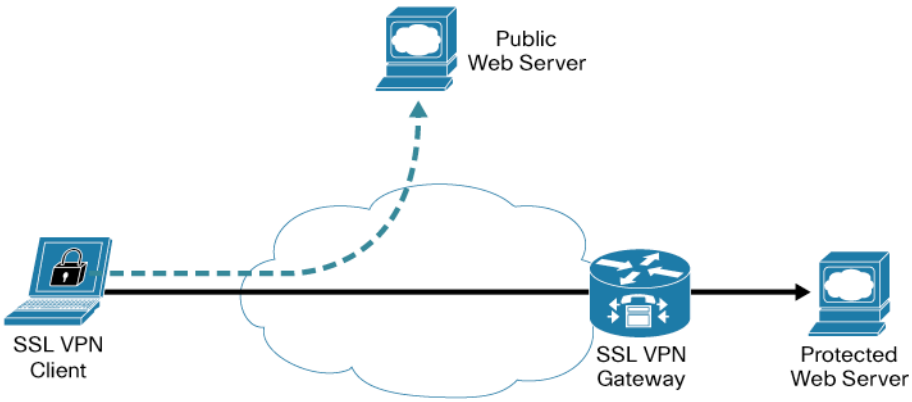
Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.15) Cisco IOS SSL VPN URL Split Rewrite Support

In SSL VPN clientless operation, the SSL VPN gateway acts as a proxy between client and server, inspecting all web-based traffic and rewriting URLs in the content. This process is very CPU intensive and time consuming, affecting performance and scalability.

Conceptually similar to split tunneling in IPSec, the URL Split Rewrite for Cisco IOS SSL VPN feature enables the administrator to select which URLs are processed through the SSL VPN gateway, and which URLs the client can reach directly. Internal web-based connections to protected resources are still processed normally through the SSL VPN gateway, while external traffic can be allowed a direct connection.

Figure 21. Cisco IOS SSL VPN URL Split Rewrite Support



Benefits

- Provides flexibility to selectively define what traffic needs SSL VPN protection
- Improves scalability and performance by not having to process all of a remote users traffic

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.16) Next Hop Resolution Protocol (NHRP) MIB for Dynamic Multipoint VPN (DMVPN)
To manage DMVPN deployments most effectively, administrators are not only interested in knowing about individual IPSec and tunnel protected Multipoint GRE (mGRE) tunnels, but also the control plane (ie: NHRP) statistics associated with corresponding tunnels.

The NHRP MIB for DMVPN feature addresses this by providing information on NHRP usage, routes, sessions, NHRP supported hub maximum throughput, and memory in a DMVPN network.

Benefits

- Improves manageability of DMVPN networks.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/dmvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.17) IPv6 Over Dynamic Multipoint VPN (DMVPN) Support
DMVPN has added support for IPv6 in combined IPv4 and IPv6 network environments. Where secure connectivity is required, DMVPN can now be used to connect IPv4 and IPv6 networks.

Benefits

- Supports standards-based IPv6
- Supports IPSec native mode

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/dmvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.18) Group Encrypted Transport (GET) VPN Support for VRF-Lite

GET VPN support for VRF-Lite allows Enterprises or service providers to support multiple VPN Routing and Forwarding (VRF) instances on Customer Edge (CE) devices. VRF-Lite extends limited Provider Edge (PE) functionality to a CE device, giving it the ability to maintain separate VRF tables and extending the privacy and security of a VPN to the branch office. This also allows the capability of sharing the same CE device for various internal departments while maintaining separate VRF tables for each department.

The GET VPN key server is not VRF aware. As a result, there can be 2 possible scenarios (cases) for deployment depending on whether single or multiple MPLS VPNs (PE VRFs) are used on the PE router for each GETVPN group:

- **Case 1:** PE uses a single MPLS VPN (PE VRF) for all group member VRFs (CE VRFs). For this, group members can use the same certificate for authentication, for all the crypto maps applied on VRF interfaces. No overlapping addresses can be supported in the group member VRFs because the PE has all the group member addresses in a single VRF. However, traffic excluded from any of the encryption policies are subject to be routed across group member VRFs.
- **Case 2:** To use overlapping addresses between group member VRFs, the PE router should use a unique MPLS VPN (PE VRFs) for each group member VRFs. In addition, a separate key server must be dedicated to each VRF because the key server is not VRF-aware. Group members should also use a separate certificate to authenticate each crypto map.

Benefits

- Allows customers to share the same CE router for various internal departments while maintaining separate VRF tables for each department

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

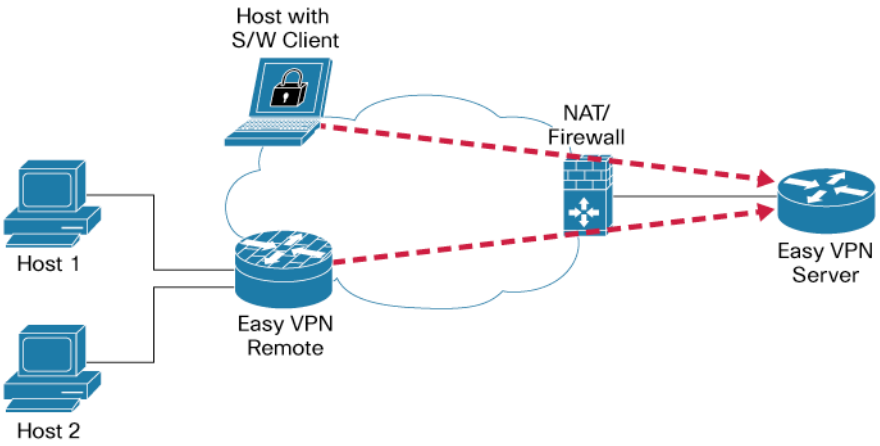
Additional Information: http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.19) Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients

There are many situations where customers require a VPN client to operate in an environment where standard ESP (Protocol 50) or UDP 500 (IKE) can either not work, or not function transparently without modifications to existing firewall rules. With Cisco Tunnel Control Protocol (cTCP), users can establish VPN tunnels from the client to an Easy VPN Server through a third-party Network Address Translation (NAT) device or firewall.

Figure 22. Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients



Benefits

- Requires no modification of firewall rules
- Creates fewer limitations from where clients can connect
- Offers transparent interoperability with third party firewalls

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/easyvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.20) IPSec Usability Enhancements

A variety of IPSec usability enhancements are being introduced in Release 12.4(20)T:

Intelligent Defaults

Support for eight Internet Key Exchange (IKE) default policies and IPSec transform set policies. By default, the IKE option is turned on. The default IPSec transform set will be used only if no other transform set is configured for a crypto map.

To display the default IKE policy, the following CLI command has been created:

```
show crypto isakmp default policy
```

If the default policies are turned off, then show crypto isakmp default policy will not display the default policies. If the user configures the isakmp policy then the default policy will not be used during negotiation. This command is not available in the K8 images.

To display the default IPSec transform set policy, the following CLI command has been created:

```
show crypto ipsec default  transform-set
```

The default transform-sets is not available in the K8 images.

IPSec Show Command Enhancements

Using IOS `show` commands to display MIB agent maintained data helps monitor CPE devices. The following show commands are some examples (MIB table information is for a specific VRF if the VRF-name is provided; otherwise, the information for all vrfs is displayed):

```
show crypto mib isakmp flowmib failure { vrf <vrf-name> }
show crypto mib isakmp flowmib global  { vrf <vrf-name> }
show crypto mib isakmp flowmib history  { vrf <vrf-name>}
```

Show Tech Support IPSEC

Often to resolve technical issues, multiple `show` commands need to be executed and the output needs to be collected. To simplify this process, the show `tech-support IPSEC  [vrf <vrf>] [peer-ip <address>]` has been created to collect the same output in one show command.

Benefits

- Improves administration
- Simplifies configuration with default policies
- Improves problem reporting

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/ipsec

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.21) Secure Shell Protocol Version 2 (SSHv2) Feature Enhancements

A number of SSHv2 enhancements have been added including additional debugging functionality, VRF-aware SSH support, SSH keyboard mode, and Diffie-Hellman group exchange key support for mods 2048 and 4096.

Benefits

- Simplifies debugging
- Supports larger Diffie-Hellman key sizes
- Provides VRF-aware SSH client-side functionality

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6665/products_ios_protocol_option_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.22) Command Line Interface (CLI) for Displaying Certificates
Cisco IOS CLI introduces a new command to allow administrators to easily display all certificates in the Cisco IOS Certificate Server database.

Benefits

- Improves manageability by allowing all certificates in the Cisco IOS Certificate Store (CS) database to be displayed

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.23) CLI to Control Certification Revocation List (CRL) Cache
When processing X.509 certificates, the Certificate Revocation List (CRL) is consulted. To improve performance of certificate validation, IOS keeps a cache of the downloaded CRL in volatile storage on the router. Instead of using a fixed amount of volatile memory, administrators can reduce the cache size for low memory conditions or increase it for better performance when dealing with a large number of CRLs.

Benefits

- Helps to optimize router memory allocation

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.24) Secure Device Provisioning (SDP) Connect Template
SDP Connect Template increases the usability and range of applications for configuring the device for Internet connectivity. This eases the deployment process for routers, particularly routers that do not already have Internet connectivity.

Benefits

- Eases deployment burden on administrators
- Reduces deployment costs

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

4.2) Cisco IOS Infrastructure

4.2.1) Cisco Express Forwarding Scalability and Selective Rewrite (CSSR)
Cisco Express Forwarding (CEF) technology for IP is a scalable, distributed, layer 3 switching solution designed to meet the performance requirements of the Internet and Enterprise networks. The CEF infrastructure has been adapted and rewritten as Cisco Express Forwarding Scalability and Selective Rewrite (CSSR) in order to meet the requirements and scalability of Internet traffic evolution as well as support new platforms and features developed by Cisco.

This infrastructure is also supported in Cisco IOS Software Releases 12.2SB, 12.2SE, 12.2SG, 12.2SR, and 12.2SX.

Benefits

CSSR delivers the following benefits:

- Enhances scalability to sustain the Internet growth, support larger numbers of:
  - IPv4/IPv6 prefixes and adjacencies
  - Load balanced paths
  - VPNs (VPN routing/forwarding instances)
- Simplifies fast switching path decisions for both IPv4 and IPv6 traffic
- Offers improved manageability:
  - CEF logging for both IPv4 and IPv6
  - Unicast Reverse Path Forwarding Strict and Loose mode for both IPv4 and IPv6
  - CEF MIB support
  - uRPF MIB support
  - CLI display enhancements

Considerations

CSSR infrastructure enhancements in Release 12.4(20)T might result in changed performance characteristics in your networks. Please test your configurations prior to upgrading to this software release.

Hardware

Routers	• Cisco 1800, 2800, 3800, and 7200 Series Routers

Product Management Contact: Patrick Grossetete, pgrosset@cisco.com

4.2.2) Network Time Protocol (NTP) Version 4
NTP Version 4 is a protocol designed to time-synchronize a network of machines. It is widely used in the Internet to synchronize hosts and routers clocks as a large number of manufacturers include NTP software for their systems.

As the Internet evolves from thousands to millions of devices, improvements to NTP are required to better scale, enhance security, and comply with next generation of Internet Protocol Version 6 (IPv6).

The NTP Version 4 IETF draft is a significant revision to the NTP Version 3 standard, with a number of NTP v4 implementations in production today. The Cisco implementation prior to Release 12.4(20)T was based on NTP Version 3, an Internet draft standard formalized in RFC 1305.

Benefits

- Provides NTPv4 client and server functionality
- Allows NTPv4 configuration in IPv4 environments, including backward compatibility with NTPv3
- Enables NTP configuration in IPv6 environments
- Enables NTP configuration in VRF environment for both IPv4 and IPv6

Hardware

Routers	• Cisco 1800, 2800, 3800, and 7200 Series Routers

Additional Information:

http://www.ietf.org/html.charters/ntp-charter.html

Public NTP server information: http://support.ntp.org/bin/view/Servers/WebHome

Product Management Contact: Patrick Grossetete, pgrosset@cisco.com

4.3) MPLS

4.3.1) Cisco IOS MPLS Label Distribution Protocol (LDP) Enhancements
Cisco IOS MPLS LDP offers standards-based feature capabilities for MPLS label information signaling between MPLS-enabled routers. In addition to RFC3036-compliant MPLS signaling, Cisco MPLS LDP also offers a number of value-added feature capabilities, which enable improved configuration and usability. MPLS LDP feature capabilities are focused on MPLS LDP CLI configuration enhancements, enhanced security, and coexistence support with Cisco High Availability (HA) feature set, including Nonstop Forwarding (NSF) with Stateful Switchover (SSO).

The following LDP features and enhancements are introduced in Cisco IOS Release 12.4(20)T:

MPLS LDP—Message Digest 5 (MD5) Global Configuration

The MPLS LDP MD5 Global Configuration feature provides enhancements to the use of MD5 passwords for LDP session authentication. This feature allows the user to enable LDP MD5 globally (ie: in global router configuration context) instead of on a per-LDP peer basis. Using this feature allows setup of password requirements for a specific LDP neighbor, or a set of LDP neighbors (ie:LDP peer group) to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages.

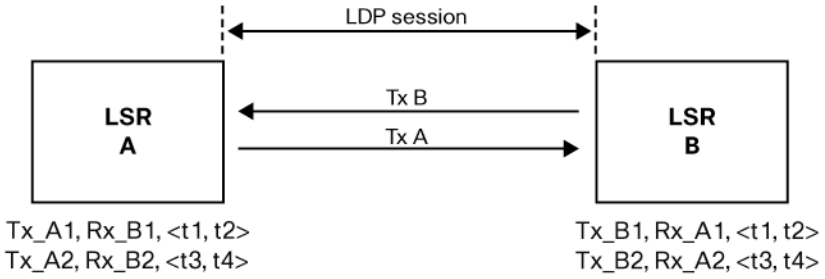
MPLS LDP—Lossless MD5 LDP Session Authentication

The MPLS LDP MD5 Global Configuration feature provides a configuration enhancement for enabling MD5-based session authentication of LDP sessions. This prevents unauthorized LDP peer applications from establishing LDP sessions with the local LDP process and also helps to block spoofed TCP messages.

The feature allows configuration of LDP MD5 support globally (ie: for all LDP-enabled interfaces on a MPLS-enabled router) instead of on a per-LDP peer basis. In addition, MD5 session authentication can be enabled for a selective set of LDP sessions via access-control lists.

Additional LDP feature enhancements are also introduced to provide the ability to dynamically change the configuration of MD5 keys for LDP session authentication. Via a configurable MD5 keychain, multiple MD5 authentication keys with specific activation intervals can be configured for a given LDP session. These new LDP enhancements complement existing MD5 LDP session authentication capabilities, which prior to Release 12.4(20)T only enabled configuration of one single MD5 key per LDP session.

Figure 23. MPLS LDP MD5 Global Configuration feature overview



Tx_A1, Tx_A2 : MD5 keys used by A for athenticating TCP segments sent to B
Tx_B1, Tx_B2 : MD5 keys used by B for athenticating TCP segments sent to A
Rx_A1, Rx_A2 : MD5 keys used by B for athenticating TCP segments received from A
Rx_B1, Rx_B2 : MD5 keys used by A for athenticating TCP segments received from B
<t1, t2> : Time window within a set of MD5 keys is valid

Benefits

Key benefits of the new MPLS LDP feature enhancements include the following:

- **MPLS LDP—MD5 Global Configuration:** Enhanced configuration capabilities for enabling MD5-based LDP session authentication, including MD5 authentication configuration for specific LDP peer groups and ability to update existing MD5 keys without impacting current state of LDP sessions.
- **MPLS LDP—Lossless MD5 LDP Session Authentication:** No need anymore to tear down LDP session to activate new MD5 key for LDP session authentication. Configurable key chain enables flexible scheduling of multiple MD5 keys to be used for LDP session authentication.

Hardware

Routers	• Cisco 2800, 3800, and 7200 Series Routers

Product Management Contact: Harmen van der Linde (havander@cisco.com)

4.3.2) Cisco IOS MPLS Traffic Engineering and Resource Reservation Protocol (TE/RSVP)
Cisco IOS MPLS TE offers standards-based feature capabilities for MPLS traffic management, including explicit path configuration and protection, via signaling of TE/RSVP tunnels. In addition to RFC-compliant RSVP/TE signaling procedures, Cisco MPLS TE also offers a number of value-added feature capabilities, which enable improved configuration and usability of MPLS TE functionality, such as coexistence support with the Cisco High Availability (HA) feature set.

Starting with Cisco IOS Release 12.4(20)T, a full set of MPLS TE/RSVP capabilities will also be available including the following features:

Basic MPLS TE/RSVP:

The following capabilities are now supported as part of the base MPLS TE/RSVP feature set:

- MPLS Traffic Engineering (TE)
- MPLS TE—OSPF Flooding Support
- MPLS TE—IS-IS Flooding Support
- MPLS TE—Support for LSP Attributes
- MPLS TE—Autoroute Announce
- MPLS TE—Verbatim Path Support
- MPLS TE—Configurable Path Calculation Metric for Tunnels
- MPLS TE—Hello State Timer
- MPLS TE—RSVP Refresh Reduction

Advanced MPLS TE/RSVP Signaling:

The following features enable advanced MPLS TE/RSVP signaling and support selective, flexible, and automated setup of traffic engineered paths in a MPLS network:

- MPLS TE—Explicit IP Address Exclusion
- MPLS TE—Link Affinity Attributes
- MPLS TE—Autotunnel Primary and Backup
- MPLS TE—Automesh (OSPF only)
- MPLS TE—Shared Risk Link Group (SRLG)

Explicit Traffic Mapping onto TE/RSVP Tunnels:

The following feature items enable explicit configuration of policies for mapping ingress traffic onto specific MPLS TE/RSVP tunnels:

- MPLS TE—Static Route Mapping into TE Tunnels
- MPLS TE—Policy-based Routing
- MPLS TE—Forwarding Adjacency

Inter-Domain MPLS TE/RSVP Support:

The following MPLS TE/RSVP feature items enable signaling of traffic engineered paths across multiple IGP and AS domains in a MPLS network:

- MPLS TE—Inter-Area Support
- MPLS TE—Inter-AS Support

MPLS TE/RSVP for Providing Network Protection (FRR):

The following MPLS TE/RSVP feature items enable support for Fast Re-Route (FRR) link and node protection in a MPLS network:

- MPLS TE—Fast ReRoute Link and Node Protection (RSVP Hellos)
- MPLS TE—Fast ReRoute (FRR) Bandwidth Protection
- MPLS TE—Fast Tunnel Interface Down
- MPLS TE—Node Protection Desired Bit
- MPLS TE—Path Protection
- MPLS TE—RSVP Graceful Restart

MPLS TE/RSVP for Providing Bandwidth (BW) Optimization:

The following MPLS TE/RSVP feature capabilities facilitate automated bandwidth optimization capabilities for TE tunnels:

- MPLS TE—Auto Bandwidth

MPLS TE/RSVP Management:

The following embedded management capabilities are available for support of MPLS TE/RSVP resource monitoring and TE tunnel connectivity validation and trouble shooting:

- MPLS EM—TE MIB based on IETF Draft Version 05
- MPLS OAM—LSP Ping/Trace for RSVP IPv4 FECs—RFC4379 (available since Release 12.4(6)T)

Benefits

Key benefits of the new MPLS TE/RSVP feature capabilities in Release 12.4(20)T:

- **Sub-second Traffic Protection:** Via Fast Re-Route (FRR), MPLS TE/RSVP offers fast recovery of link and node failures in a MPLS network and this way minimizing potential traffic loss as result of network failures.
- **Bandwidth protection and network capacity engineering:** Via RSVP bandwidth allocation and signaling, MPLS TE enables optimized traffic bandwidth allocation and distribution in a MPLS network.
- **Tight QoS traffic control:** Via explicit routing and QoS mapping procedures (ie: mapping of QoS traffic onto specific traffic engineered tunnels) MPLS TE offers the ability to control the flow of QoS-market traffic across a MPLS network.
- **Deterministic traffic flow control:** MPLS TE/RSVP enables setup of explicitly routed traffic paths across a MPLS network, which can facilitate temporary reroute of traffic during network maintenance activities.

Hardware

Routers	• Cisco 2800, 3800, and 7200 Series Routers

Product Management Contact: Harmen van der Linde (havander@cisco.com)

4.4) Quality of Service

4.4.1) Cisco IOS QoS: Hierarchical Queuing Framework (HQF)

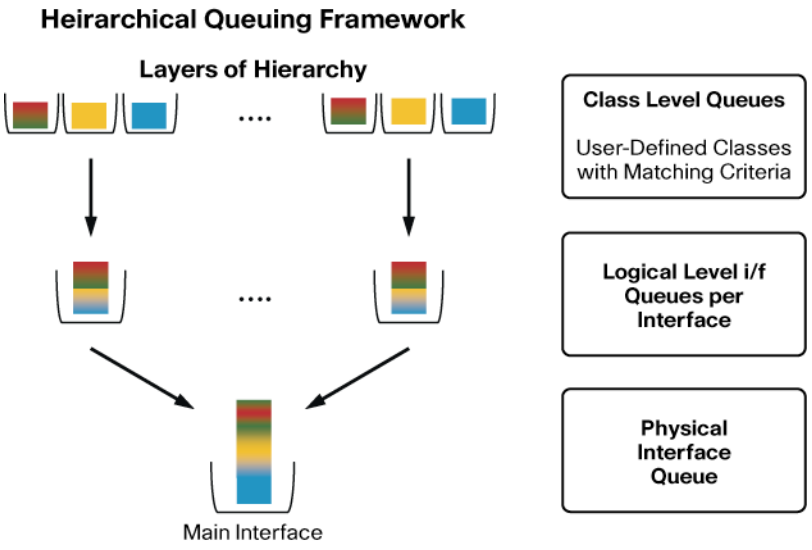
Cisco IOS Software today offers an extensive set of QoS features for queuing and shaping which network managers use for optimizing network bandwidth utilization. However, as more services are being deployed on the network, the general network implementation architecture becomes extremely complex, creating the need for more structured QoS queuing and shaping capabilities.

Cisco IOS Release 12.4(20)T introduces Hierarchical Queuing Framework (HQF), which enables customers to manage their QoS at multiple levels (physical interface level, logical interface level, and class level) of scheduling for applying QoS queuing and shaping. This provides the most comprehensive, granular, and flexible QoS network operating system architecture available in the industry today.

Benefits of HQF

- Extensive abstraction layer for consistent queue definitions within QoS
- Faster deployment of QoS queuing & shaping in large-scale networks
- Consistent queuing behavior applied with common Cisco Command Level Interface (CLI) commands across HQF supported Cisco IOS Software releases

Figure 24. HQF Layers of Hierarchy



Hardware

Platforms Supported	• Cisco 1801, 1802, 1803, 1805, 1811, 1812, 1841, 1861, 2821, 2851, 2811, 2801, 3250, 3220, 3270, 3825, 3845, AS5300XM, AS5400XM, IAD2430, IAD2431, IAD2432, VG224, 7204VXR, 7206VXR (NPE-400, NPE-G1, NPE-G2), 7201, and 7301 Series

Product Management Contact: Michael Lin, (mhelin@cisco.com)

4.4.2) Resource Reservation Protocol (RSVP) Penultimate Hop Overwrite

The RSVP Penultimate Hop Overwrite feature allows you to configure an RSVP enabled router on a per interface basis to populate an address other than the interface address in the previous hop address field of the Previous Hop (PHOP) object when forwarding a PATH message onto that interface. You can configure the actual address for the router to use, or which interface, including a loopback, from which to borrow the address.

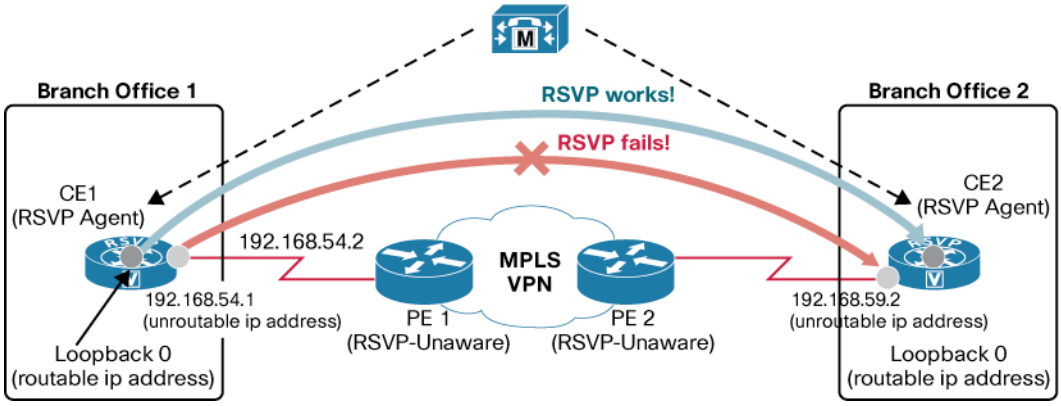
RSVP Penultimate Hop Overwrite Operation

Figure 12 below shows a sample network in which the following scenario occurs (no RSVP reservation is established):

An RSVP PATH message contains PHOP object that is rewritten at every RSVP hop. The object's purpose is to enable an RSVP router (R1) sending a PATH message to convey to the next RSVP router (R2) downstream that the previous RSVP hop is R1. R2 uses this information to forward the corresponding RESV message upstream hop-by-hop towards the sender.

The behavior in Cisco IOS Software prior to Release 12.4(20)T was that an RSVP router always set the PHOP address to be the IP address of the egress interface onto which the router transmits the PATH message. There are situations, however, where even though some IP addresses of R1 are reachable, the IP address of its egress interface is not reachable from a remote RSVP router (R2). This results in the corresponding RESV message generated by R2 never reaching R1, and the reservation never being established.

Figure 25. RSVP Penultimate Hop Overwrite Use Case



In the illustration shown in Figure 12 above, when a call is made from Branch Office 1 to Branch Office 2, the RSVP agent on customer edge router 1 (CE1) tries to set up a RSVP session with customer edge router 2 (CE2) and sends a PATH message. CE1 records its outgoing interface IP address (192.168.54.1), which is an un-routable IP address, in the PHOP object of the PATH message. This PATH message is tunneled across the service provider network and processed by CE2. CE2 records this IP address in the PHOP object of the received PATH message in the Path State Block (PSB).

CE2 has a receiver proxy configured for the destination address of the session. As a result, when CE2 replies back with a RESV message, CE2 tries to send the RESV message to the IP address that CE2 had recorded in its PSB. Because this IP address (192.168.54.1) is un-routable from CE2, the RESV message will fail.

Benefits

Flexibility and Customization: The user has the flexibility to specify RSVP PHOP IP address (example: loopback 0), which enables the deployment of RSVP over L3VPN RSVP-unaware core network even if the L3VPN network provider makes the CE-PE IP addresses un-routable (ie: using unnumbered IP addresses).

Hardware

Routers	• Cisco 1800, 2800, 3800, and 7200 Series Router

Additional Information: http://www.cisco.com/go/rsvp

Product Management Contact: Bertrand Duvivier, bduvivie@cisco.com

4.5) IP Version 6

4.5.1) IPv6 VPN Provider Edge Router (6VPE) over MPLS
6VPE, the Cisco implementation of IPv6 VPN provider edge router over MPLS, enables IPv6 locations in a VPN to communicate with each other over an MPLS IPv4 core network infrastructure levering MPLS Label Switched Paths (LSPs).

The 6VPE feature relies on multiprotocol Border Gateway Protocol (BGP) extensions in the IPv4 network configuration on the Provider Edge (PE) router to exchange IPv6 VPN reachability information, in addition to an MPLS label for each IPv6 address prefix to be advertised.

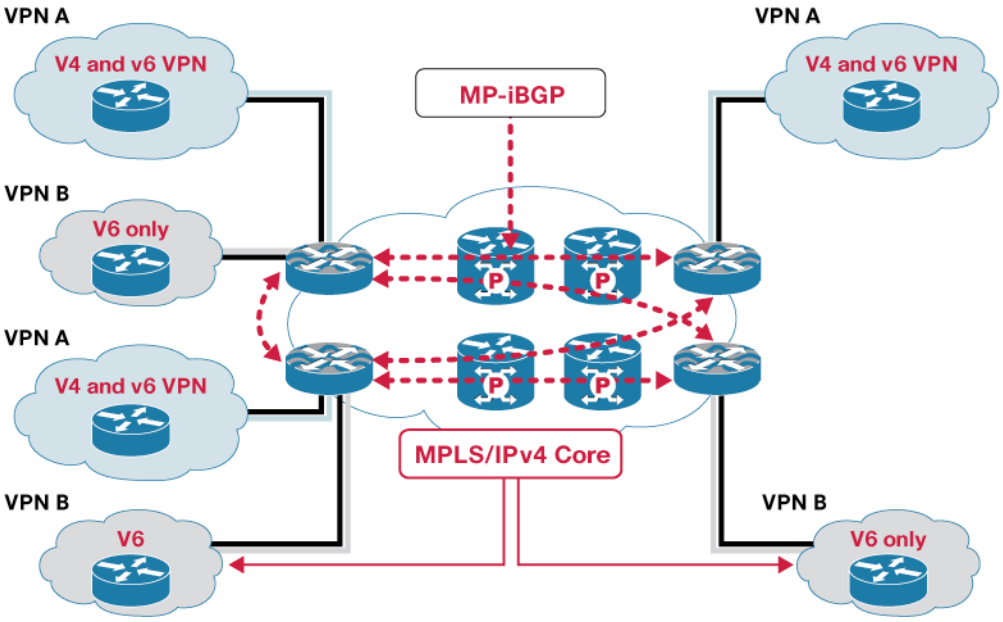
Edge routers are configured to be dual stack running both IPv4 and IPv6, and IPv4 VPN and IPv6 VPN can co-exist with similar coverage and policies.

The Cisco 6VPE implementation also provides IPv6 VRF-Lite support, enabling low-end Customer Edge (CE) routers without MPLS support to be supported.

6VPE was originally proposed at the IETF and published as RFC 4659.

6VPE is also supported in Cisco IOS Software Release 12.2SR for Cisco 7200 and 7600 Series Routers, and Cisco IOS-XR 3.5.2 for the Cisco 12000 Series Router.

Figure 26. 6VPE over MPLS Deployment



Benefits

6VPE allows IPv6 VPN to be deployed over existing MPLS Multiservice infrastructure with marginal operational impact, cost, and risk.

Key benefits include:

- IPv4 or MPLS Core Infrastructure is IPv6-unaware
- Cisco routers configured as PEs are updated to support Dual Stack/6VPE
- Cisco routers can be configured with IPv6 VRF-Lite
- IPv6 VPN reachability exchanged among 6VPEs via iBGP (MP-BGP)
- IPv6 VPN can co-exist with IPv4 VPN—same coverage and policies

Hardware

Routers	• Cisco 1800, 2800, 3800, and 7200 Series Routers

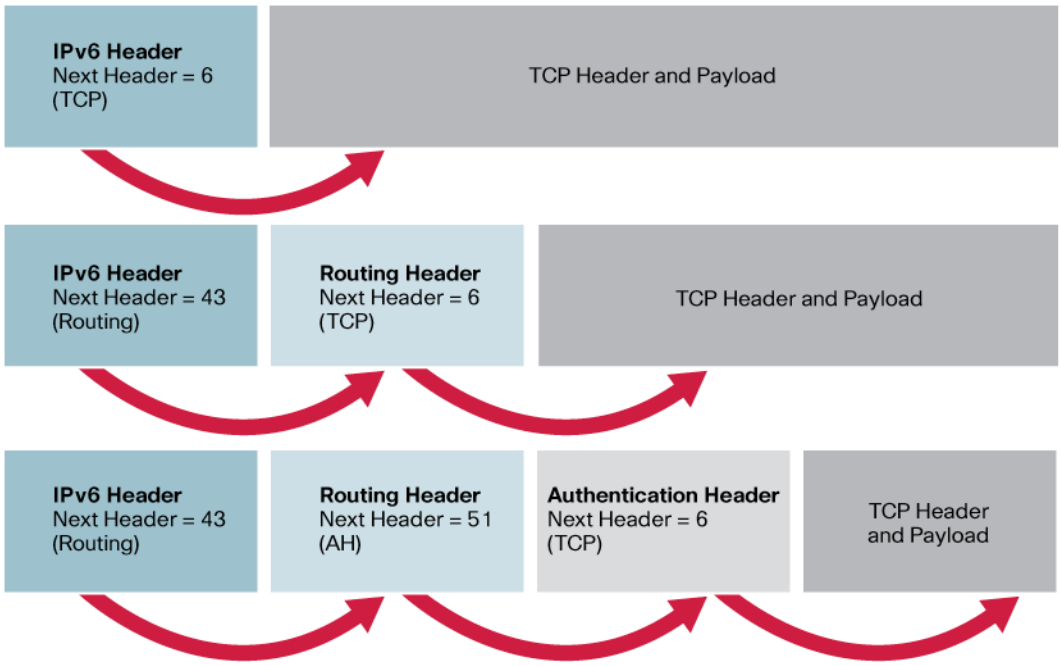
Additional Information: http://www.cisco.com/ipv6

Product Management Contact: Patrick Grossetete, pgrosset@cisco.com

4.5.2) IPv6 Access Control List (ACL) enhancements for IPv6 IPSec Authentication Header (AH) IPv6 Extended Access Control List (ACL) support, first introduced in Cisco IOS Software Release 12.2(2)T, included the ability to parse IPv6 extension headers to examine upper layer information. One exception was the ability to parse beyond the IPSec Authentication Header (AH). Some recent 3rd party operating system releases enable IPv6 traffic authentication between hosts in a managed domain through the use of the IPv6 IPSec AH extension header.

Cisco IOS Release 12.4(20)T introduces the capability to parse beyond the IPSec AH and process upper layer information (TCP, UDP, etc.), which offers greater flexibility in packet matching for ACLs and Quality of Service (QoS).

Figure 27. Parsing IPv6 Option Headers



Benefits

The IPv6 ACL enhancement for IPv6 IPSec Authentication Header allows network managers to keep control of key networking features when IPv6 Hosts generate traffic using IPv6 IPSec AH:

- IPv6 packet filtering continues to permit or deny IPv6 packets with IPSec AH
- IPv6 QoS marking or re-marking can be applied to packets with IPSec AH

Hardware

Routers	• Cisco 1800, 2800, 3800, and 7200 Series Routers

Additional Information:

http://www.cisco.com/ipv6

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d_ps6553_Products_White_Paper.html

Product Management Contact: Patrick Grossetete, pgrosset@cisco.com

4.5.3) Mobile Network v6—Basic NEMO Support
Cisco Mobile Network v6—Basic NEMO Support enables IPv6 networks, such as networks in a vehicle, to stay connected when moving from one location to another.

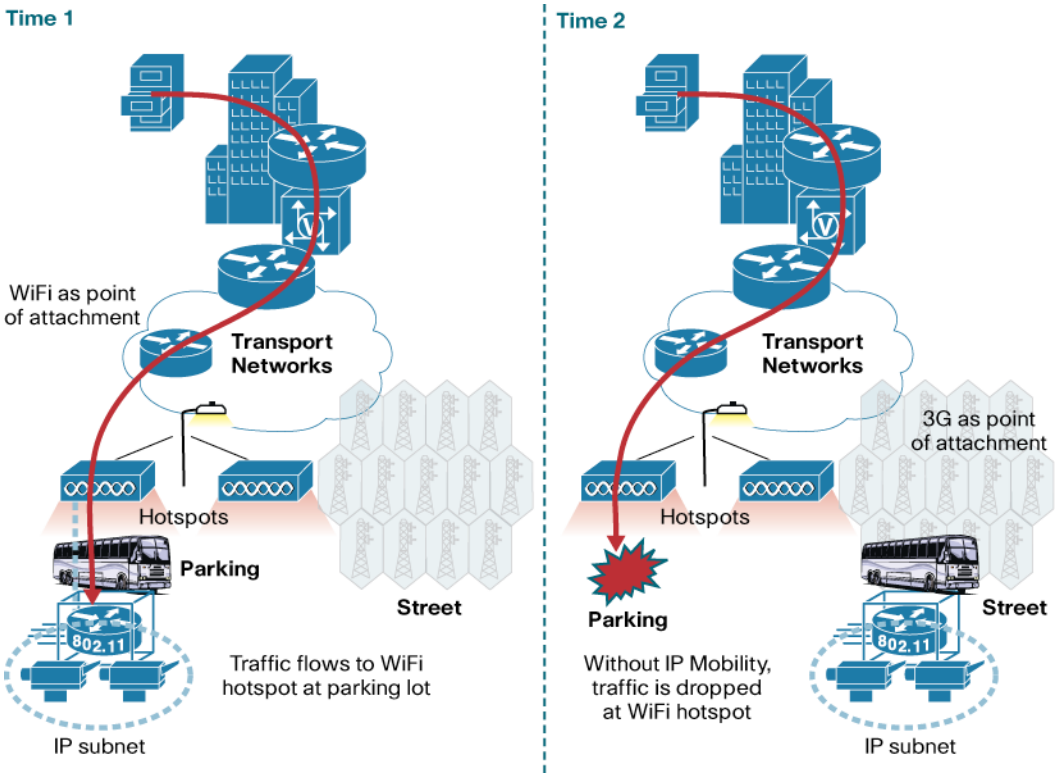
The Cisco Mobile Networks v6—Basic NEMO is based on IETF standard—RFC 3776 Network Mobility (NEMO) Basic Support Protocol. It is part of the Cisco IP Mobility technology offering, which includes Cisco Mobile IPv4, Cisco Mobile IPv6, and Cisco Mobile Network v4: http://www.cisco.com/en/US/products/ps6591/products_ios_protocol_group_home.html

Today, an increasing number of business operations occur outside of offices and often involve movement from one geographic location to another. IT departments look for ways to extend

existing office applications and introduce new applications to where the operations take place. Through these practices, organizations expect their business operations to become more streamlined, and mobile workers are able to perform their job functions remotely in an efficient and effective manner.

However, simply extending IP networks is not sufficient to support mobile operations. When an IP network moves from one location to another, its network point of attachment is often changed. Without proper provisioning, the IP network can become unreachable. As a result, application traffic to IP devices on that IP network is dropped. The diagram below illustrates this point.

Figure 28. Traffic is dropped when IP networks are moved from one location to another

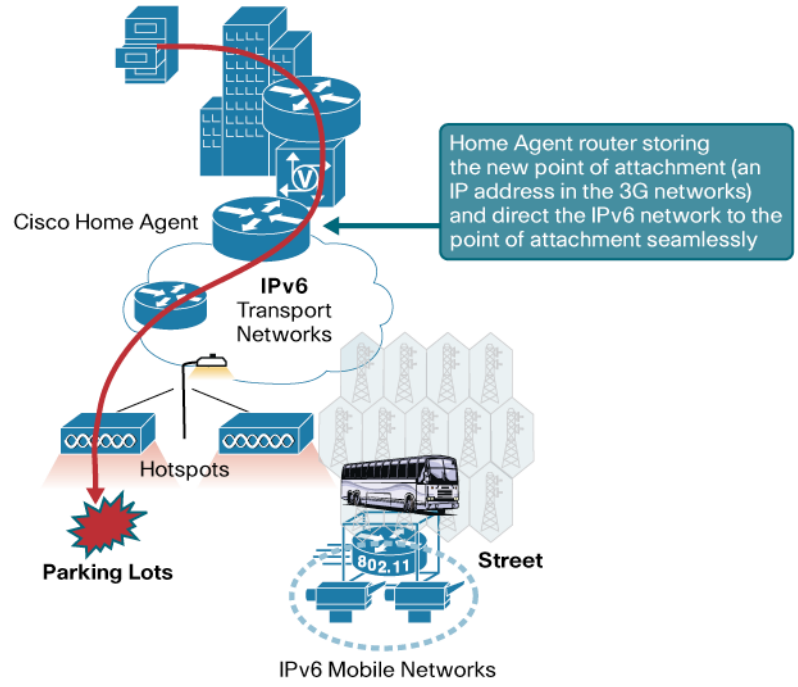


The bus shown in Figure 15 above has an IP network associated with a router. The router provides backhaul connectivity to the data center and there are multiple IP devices, such as video surveillance camera, connected to the IP network on the router. At time 1, the bus is in a parking lot and its network point of attachment is through a WiFi network in the parking lot. At time 2, when the bus leaves the parking lot and drives onto the street, it losses its WiFi connection and is now using a 3G wireless connection as the network point of attachment. When this happens without IP mobility technology, the traffic destined to the IP network is dropped (since the rest of the network has routing tables that point the IP network toward the WiFi network).

The Cisco Mobile Network (for both IPv4 and IPv6) resolves this issue by automatically routing the traffic for the IP network to the new point of attachment. When the router moves to its new point of attachment, it registers with a Mobile IP Home Agent to inform its new point of attachment. The rest of the network continues forwarding the traffic to the Home Agent, and the Home Agent forwards the traffic to the IP network via the new point of attachment. This results in no routing convergence, eliminating disruptions in network connectivity.

With Mobile Networks v6—Basic NEMO support, both mobile networks and transport networks can also be IPv6 networks, allowing the extension of the number of mobile nodes to large scale in situations where an IPv6 addressing scheme is available.

Figure 29. Mobile Network v6—Basic NEMO Support for Home Agent



With IP Mobility, traffic is redirected to the new point of attachment automatically without causing routing churn

Benefits

- Application sessions are not interrupted during movement (underlying IP address remains constant)
- Supports large number of mobile devices through IPv6 mobile network infrastructures
- Eases mobile networking deployment without impacting routing operations
- Improves operation efficiency and worker productivity

Hardware

Routers	• Cisco 1800, 2800, 3200,3800, and 7200 Series Routers

Additional Information:

http://www.cisco.com/en/US/products/ps6551/products_ios_technology_home.html

Product Management Contact: Richard Shao, rshao@cisco.com

4.6) Embedded Management

4.6.1) Cisco IOS Service Diagnostics

Cisco IOS Service Diagnostics is an embedded feature that enables customers, partners and Cisco TAC engineers the ability to diagnose software and network neighborhood issues on Cisco platforms, minimizing troubleshooting time. It can be used to run diagnostic audits on the network and monitor device health and state.

Cisco IOS Service Diagnostics provides a simple interface for deploying and receiving diagnostic information from scenario-specific troubleshooting scripts. It automates the Cisco comprehensive troubleshooting expertise in the BGP, OSPF, QoS, and resource diagnostics areas, with the goal of reducing the configuration burden of defining TCL scripts and/or EEM policies.

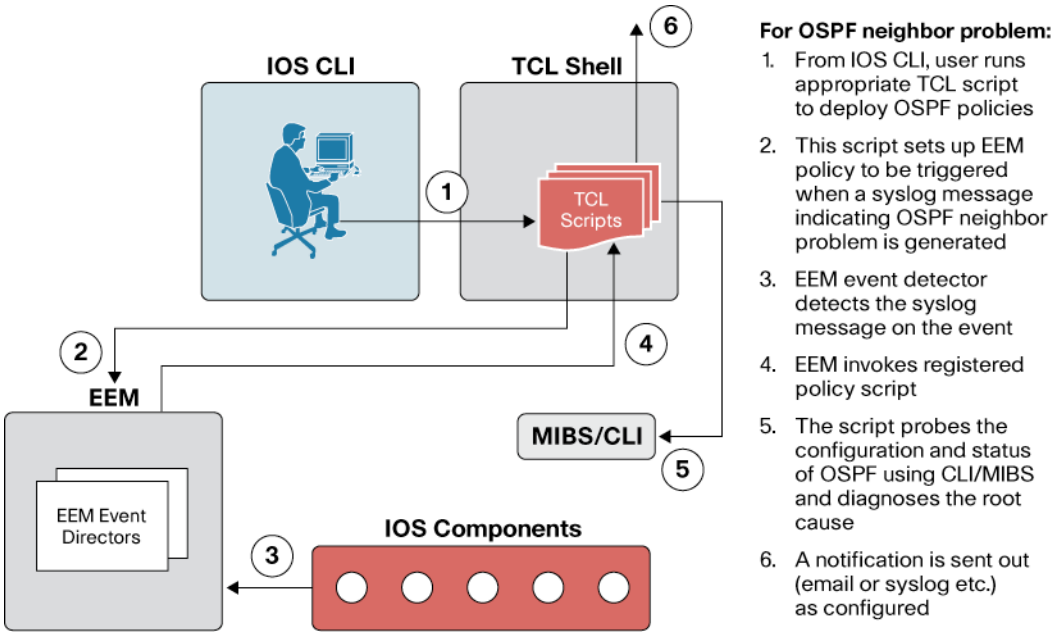
The benefits of Cisco IOS Service Diagnostics feature include but are not limited to:

- Cost savings (Reduced MTTR)
- Increased network uptime
- Automatically identify the most common root causes for the most common failure scenarios related to BGP, OSPF, QoS
- Send automatic alerts on resource monitoring when configured thresholds are crossed
- Automatically collect additional context information that is relevant to diagnosing a problem (accelerates problem resolution)
- Provide an infrastructure to customize and add additional diagnostics
- Enhance programmable platform capabilities of Cisco IOS Software

Cisco IOS Service Diagnostics also includes a new feature called **Embedded Menu Manager** (EMM). EMM provides a programmable framework which allows Cisco IOS to present a custom, character-based menu wizard user interface to guide users through complex configuration tasks.

EMM also allows the extension of the Cisco IOS user interface though the use of Menu Definition Files (MDF).

Figure 30. Example of OSPF Diagnosis Workflow



Benefits

- XML MDF file very flexible and file based
  - Definitions can be centrally stored on network servers
  - Menu elements can be made more dynamic with Tcl
- Built-in customizable context-sensitive help
- Wizard mode steps users through menu application
- Built-in input validation
- Ability to record and play back menu sessions

Additional Information:

http://www.cisco.com/en/US/products/ps9424/products_ios_protocol_group_home.html

http://cisco.com/go/ciscobeyond

Product Management Contact: Madhu Vulpala, mvulpala@cisco.com

4.6.2) Embedded Event Manager Version 2.4

Cisco IOS Embedded Event Manager (EEM) is a unique subsystem within Cisco IOS Software. EEM is a powerful and flexible tool to automate tasks and customize the behavior of Cisco IOS and the operation of the device. Customers can use EEM to create and run programs or scripts directly on a router or switch. The scripts are referred to as EEM Policies and can be programmed using a simple CLI-based interface or using a scripting language called Tool Command Language (Tcl).

EEM allows customers to harness the significant intelligence within Cisco IOS Software to respond to real-time events, automate tasks, create customer commands and take local automated action based on conditions detected by the Cisco IOS Software itself.

EEM provides a level of embedded systems management not previously seen in Cisco IOS Software. Over fifteen event detectors provide an extensive set of conditions that can be monitored

and defined as event triggers. The system is extensible with new capabilities and further subsystem integration is planned.

EEM Version 2.4 Feature Enhancements and Benefits

EEM Version 2.4 ushers in a significant number of enhancements over previous versions:

1. Two new event detectors:
   - **Remote Procedure Call Event Detector**: Allows for programs outside of the device to invoke specific device-resident, embedded policies by sending a SOAP request over an SSHv2 connection. The device-resident policy runs on the device and may reply with information in a subsequent SOAP response.
   - **SNMP Proxy Event Detector**: Creates events when a specified SNMP trap or inform is received at the device. This allows for policies to be triggered by events from other devices.
2. **Multiple Event Correlation:** EEM 2.4 now allows for multiple events to be considered for policy invocation. Previously, a single event specification triggered a policy. Now up to 8 events may be correlated together using logical operators allowing for more granular and very powerful policy triggers.
3. **Script Policy Refresh**: This feature allows for easy management, distribution, and update of device resident polices using a pull model.
4. Additional ease of use enhancements and extensions:
   - **Interface Counter ED**: Rate based trigger; Bytecode support; Support for parameters on the event manager run command; Clear command to kill a policy; Registration substitution enhancement; SNMP ED enhancement - delta value; Tcl package support

Table 9. EEM 2.4 Features and Benefits

Feature	Benefit
Extensible and powerful subsystem architecture	
Architecture	The EEM subsystem is designed with modularity in mind. It consists of Event Detectors, an Event Manager Server, and action routines called Policies
CLI interface	An interface to the Cisco IOS CLI to allow automated commands and access to any information that can be displayed
Policy scheduler	EEM policies are scheduled one at a time or concurrently according to the number of threads configured
Built–in actions	Policies can invoke a number of built-in actions for easy automation
Extensive set of Event Detectors (ED)	
Application	Custom application events, action script interaction
CLI	CLI command match and run
Counter	Custom counter events
GOLD	Generic Online Diagnostics (GOLD) event detection
Interface	Interface counters and events
Memory Threshold (Deprecated)	Detect memory resource related events.
None (by run command)	Allows execution of an EEM policy by direct command, event manager run.
Object Tracking	Integration with Enhanced Object Tracking (EOT).
OIR	Card Online Insertion & Removal detection.
Remote Procedure Call	Allows for authorized programs outside of the device to invoke specific device-resident, embedded policies by sending a SOAP request over an SSHv2 connection.
Resource Threshold	Integration with Embedded Resource Manager, supersedes Memory Threshold ED.

Feature	Benefit
RF	Cisco IOS infrastructure Redundancy Facility (RF) events
SNMP	Detect MIB variable match and thresholds.
SNMP Proxy	Creates events when a specified SNMP trap or inform is received at the device. This allows for policies to be triggered by events from other devices.
Syslog	Regular expression pattern match on emitted Syslog messages.
Timer	Custom timed events.
IOS Watchdog Monitor	Cisco IOS scheduler, watchdog events.
WDSysMon	Cisco IOS Software Modularity: System monitor event.
Secure system operation	
EEM scripts run within system constraints	Protects system from harm. ie: A looping script will not stop Cisco IOS.
User scripts run in Safe-Tcl mode	Certain programmable options are disabled for protection
Controlled environment	Only a network administrator with privileged access can define and set up EEM scripts. No one else can install software to compromise the system.
Support for TACACS+/RADIUS	EEM scripts can be associated with a configured User ID and be checked for permission.
EEM is optional	If you don't want to use this powerful capability, you don't have to enable it.
Online scripting community	
Cisco Beyond—Product Extension Community	A place for customers to share and download scripts. Don't reinvent the wheel. Build and extend the work of others. Learn by example. Go to: http://www.cisco.com/go/ciscobeyond .

Hardware

Routers	• Cisco Integrated Services Routers and Cisco 7200 Series Routers (refer to the Cisco IOS Feature Navigator for the latest device support information).

Additional Information: For more information about Cisco IOS EEM visit http://cisco.com/go/eem or contact your local Cisco account representative.

Product Management Contact: Rick Williams, rwill@cisco.com

4.6.3) Cisco IOS Embedded Packet Capture

Cisco IOS Embedded Packet Capture (EPC) is a powerful troubleshooting and tracing tool which allows network administrators to capture data packets flowing through, to, and from, a Cisco router. EPC be used in troubleshooting scenarios where it is helpful to see the actual data being sent through, from, or to the network device.

Suppose, for example, help desk personnel need to determine why a particular device cannot access the network or some application. It might be necessary to capture IP data packets and examine the data to determine the problem.

Another case might be when trying to determine an attack signature for a network threat or server system security breach. EPC can help capture packets flowing into the network at the origin or perimeter.

EPC is also useful whenever a network protocol analyzer might be useful in debugging a problem, but when it's not practical to install such a device.

Features and Benefits

EPC provides the following capabilities:

- Ability to capture IPv4 and IPv6 packets in the Cisco Express Forwarding path
- A flexible method for specifying the capture buffer size and type
- EXEC-level commands to start and stop the capture
- Show commands to display packet contents on the device
- Facility to export the Packet Capture in PCAP format suitable for analysis using an external tool such as Wireshark
- Extensible infrastructure for enabling packet capture points

Hardware

Routers	• Cisco Integrated Services Routers, Cisco 7200 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6555/products_ios_technology_home.html

Product Management Contact: Rick Williams, rwill@cisco.com

4.6.4) Flexible NetFlow (FNF) Exporter—Outgoing Features Support
Flexible NetFlow (FNF) Exporter is the FNF component in charge of pulling flow records out of the cache and sending those flows records to NetFlow collectors. Prior to Cisco IOS Release 12.4(20)T, NetFlow packets generated by Flexible NetFlow exporter were bypassing output features (QoS and Crypto) configured on the outgoing interface exported packets are sent through.

Flexible NetFlow Exporter can be configured to run output features, which allows NetFlow exported packets to be classified using QoS, and sent encrypted when IPSec is configured on the outgoing interface where exported packets are sent through.

Benefits

- Enables classification of NetFlow export packets using MQC
- Enables encryption of NetFlow export packets when crypto is configured on the outgoing interface

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200, and 7300 Series Routers

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

4.6.5) Flexible NetFlow for IPv6
Flexible NetFlow is the next-generation in flow technology. It allows optimization of the network infrastructure, reducing operation costs, improved capacity planning and security incident detection with increased NetFlow flexibility and scalability beyond other flow based technologies available today.

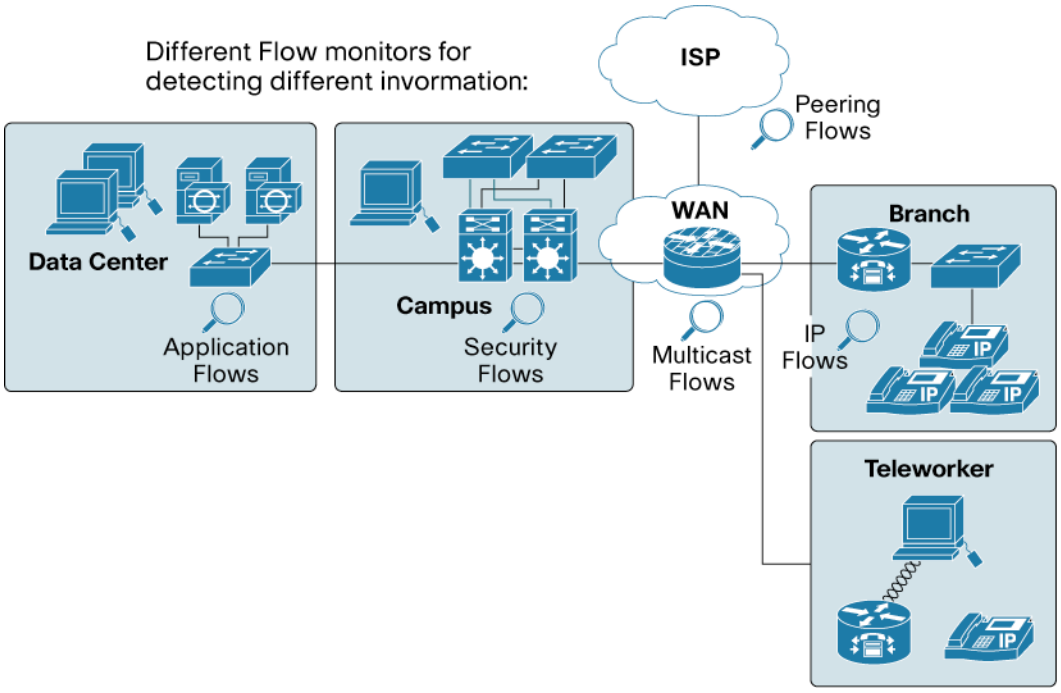
Benefits

Key Advantages of Flexible NetFlow include:

- Flexibility, scalability, and customization of flow data
- The ability to monitor a wider range of packet information
- Enhanced network anomaly and security detection
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
- Convergence of multiple accounting technologies into one accounting mechanism
- Multiple configurable flow caches

Flexible NetFlow can track multiple NetFlow applications simultaneously. For example, the user can create concurrent flow data for both security analysis and traffic analysis. Cisco IOS Flexible NetFlow provides enhanced security detection and or network troubleshooting by allowing customization of flow information. For example, the user can create a specific flow definition to focus and analyze a particular network issue or incident.

Figure 31. Flexible NetFlow Customizable Flow Monitors



Flexible NetFlow for IPv6 is a superset of NetFlow for IPv6. It will allow customers to replicate all existing features available in NetFlow for IPv6 without impact to existing collectors. This includes the collection of flows records using a pre-defined set of key fields, and the export of flow records using NetFlow v9 with pre-defined aggregations.

In addition to existing NetFlow for IPv6 features, Flexible NetFlow for IPv6 provides customers the following capabilities:

- Ingress and Egress NetFlow support
- Sampling for IPv6 Flows

- Multiple Monitor support for IPv6 Flows
- Support of IPv6 Options header
- Custom IPv6 Flow records definition

Table 10. IPv6 fields available for custom IPv6 Flow record definition

IPV6		Routing	Transport	Transport
IP (Source or Destination)	Payload Size	Destination AS	Destination Port	TCP Flag: ACK
		Peer AS	Source Port	TCP Flag: CWR
Prefix (Source or Destination)	Packet Section (Header)	Traffic Index	ICMP Code	TCP Flag: ECE
Mask (Source or Destination)	Packet Section (Payload)	Forwarding Status	ICMP Type	TCP Flag: FIN
		Is-Multicast	IGMP Type	TCP Flag: PSH
Minimum-Mask (Source or Destination)	DSCP	IGP Next Hop	TCP ACK Number	TCP Flag: RST
		BGP Next Hop	TCP Header Length	TCP Flag: SYN
Protocol	Extension	**Flow**	TCP Sequence Number	TCP Flag: URG
Traffic Class	Hop-Limit	Samples ID		
Flow Label	Length	Direction	TCP Window-Size	UDP Message Length
Option Header	Next-header	**Interface**	TCP Source Port	UDP Source Port
Header Length	Version	Input	TCP Destination Port	UDP Destination Port
Payload Lengh		Output	TCP Urgent Pointer	

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200, and 7300 Series Routers

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

4.6.6) Deprecating NetFlow for IPv6 Record

NetFlow allows you to collect traffic flow statistics on Layer 3 devices, analyze traffic patterns to detect DoS attacks, perform network capacity planning and performance management, and many other applications. NetFlow for IPv6 allows customers to collect data from IPv6 and export traffic flows using the NetFlow Version 9 export format.

From Cisco IOS Software Release 12.4(20)T onward, NetFlow for IPv6 is no longer available, and is being replaced by Flexible NetFlow for IPv6. Flexible NetFlow for IPv6 leverages the enhanced CSSF infrastructure introduced in Release 12.4(20)T, enabling greater scalability and performance.

Flexible NetFlow provides a set of features that enable customers to migrate smoothly without any modification of existing collectors. This can be achieved by using predefined records and pre-defined aggregation.

Migrating from NetFlow for IPv6 to Flexible NetFlow for IPv6

Cisco IOS does not provide automatic configuration conversion between NetFlow for IPv6 and Flexible NetFlow for IPv6. Below is a snapshot of Cisco IOS CLI configuration modifications required to migrate from NetFlow for IPv6 to Flexible NetFlow for IPv6:

Figure 32. NetFlow for IPv6 to Flexible NetFlow for IPv6 Migration Configuration Example

NetFlow for IPv6 Configuration	Flexible NetFlow for IPv6 Configuration
router(config)# ipv6 flow-export destination <*ip-address*> <*udp-port*> router(config)# ipv6 flow-export template {refresh-rate *packet-refresh-rate* | timeout <*timeout-value*>}	router(config)# flow exporter <Exporter_Name> router(config-flow-exporter)# destination <**ip-address**> router(config-flow-exporter)# transport udp <**udp-port**> router(config-flow-exporter)# template data timeout <**timeout**> router(config-flow-exporter)# end
router(config)# ipv6 flow-export version 9 [bgp-nexthop] [origin-as [bgp-nexthop] | peer-as [bgp-nexthop]] router(config)# ipv6 flow-aggregation cache {**as** | **bgp-nexthop** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}	router(config)# flow monitor <Monitor_Name> router(config-flow-monitor)# exporter <Exporter_Name> router(config-flow-monitor)# record netflow ipv6 ? **As** AS aggregation schemes **bgp-nexthop** BGP nexthop aggregation schemes **destination-prefix** Destination Prefix aggregation schemes **prefix** Source and Dest Prefixes aggregation schemes **protocol-port** Protocol and Ports aggregation scheme **source-prefix** Source AS and Prefix aggregation schemes **original-input** Traditional IPv6 input NetFlow with Ass **original-output** Traditional IPv6 output NetFlow with Ass router(config-flow-monitor)# **end**
router(config)# interface serial 0 router(config-if)# **ipv6 flow {ingress egress}**	router(config)# interface serial 0 router(config-if)# **ipv6 flow monitor <Monitor_Name> {ingress egress}**

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200 and 7300 Series Routers

Product Management Contact: Jean-Charles Griviaud, jgriviau@cisco.com

4.7) Hardware

4.7.1) Cisco 1861 Integrated Services Router

The Cisco 1861 Integrated Services Router, which is part of the Cisco 1800 Series Integrated Services Router portfolio. It is a unified communications solution for small to medium size businesses and Enterprise branch offices that provide voice, data, voicemail, automated-attendant, video, and security capabilities while integrating with existing desktop applications such as calendar, email, and Customer Relationship Management (CRM) programs.

Figure 33. Cisco 1861 Integrated Services Router

This easy-to-manage platform takes full advantage of business-class, proven unified communications technologies and supports flexible deployment models based on your needs-a wide array of IP phones, Public Switched Telephone Network (PSTN) interfaces, and Internet connectivity.

Core components include the following:

- Integrated Cisco Unified Communications Manager Express or Cisco Unified Survivable Remote Site Telephony (SRST) for call processing
- Optional Cisco Unity® Express for voice messaging and Automated Attendant
- Integrated LAN switching with Power over Ethernet (PoE)-expandable through Cisco Catalyst® Switches
- Optional support for a range of High-speed WAN Interface Cards (HWICs)
- Optional security with firewall, VPN, Secure Sockets Layer (SSL), and Intrusion Prevention System (IPS) capabilities

Additional Information:

For more information about the Cisco Integrated Services Routers, please visit http://www.cisco.com/en/US/prod/routers/networking_solutions_products_genericcontent0900aecd806cab99.html

Product Management Contact: cs-1800@cisco.com

4.7.2) Intrusion Prevention System (IPS) Advanced Integration Module
The IPS AIM provides accelerated threat control for the Cisco 1841, Cisco 2800 and the Cisco 3800 family of Integrated Service Routers.

The IPS AIM has a dedicated CPU and DRAM to offload the host CPU and up to 45Mbps on the Cisco 3845 ISR.

It enables inline IPS and runs the same software (CIPS 6.0) and enables the same features as the Cisco IPS 4200.

The IPS AIM can be managed through Cisco IPS Device Manager or Cisco Security Manager, and it is supported by CS-MARS for event monitoring and correlation.

Figure 34. Intrusion Prevention System (IPS) Advanced Integration Module

Hardware

Routers	• Cisco 1841, 2800, and 3800 Series Routers

Additional Information: http://www.cisco.com/en/US/products/ps8395/index.html

Product Management Contact: Tina Lam (tinalam@cisco.com)

4.7.3) Cisco 860 and 880 Series Routers
The Cisco 860 and 880 Series Routers are part of the Cisco 800 fixed-configuration router family and offer Internet access, security, and wireless services over broadband speeds onto a single, secure device that's simple to use and manage for small businesses.

Cisco 880 Product Overview

Cisco 880 Series Integrated Services Routers are fixed-configuration routers that provide collaborative business solutions for secure data communication to small businesses and Enterprise teleworkers. The Cisco 880 Series offers concurrent broadband services over 3G[1], Metro Ethernet, multiple types of Digital Subscriber Line (DSL) and business continuity. Wireless 802.11n and 3G supported by the Cisco 880 support LAN/WAN mobility.

The Cisco 880 Series provides the performance required for concurrent services, including firewall, intrusion prevention, content filtering, and encryption for VPNs; optional 802.11g/n for mobility; and Quality of Service (QoS) features for optimizing voice and video applications.

In addition, Cisco Configuration Professional is a Web-based configuration tool that simplifies setup and deployment. Centralized management capabilities give network managers visibility and control of the network configurations at the remote site.

Benefits

Cisco 880 Series Integrated Services Routers offer:

- High performance for broadband access in small offices and small branch and teleworker sites
- Collaborative services and data communication
- Business continuity and WAN diversity with redundant WAN links: Fast Ethernet, G.SHDSL, 3G, and ISDN
- Enhanced security:
  - Firewall with advance application and control for email, Instant Messaging (IM) and HTTP traffic
  - Site-to-site remote access and dynamic VPN services: IPSec VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES]), Dynamic Multipoint VPN [DMVPN], Group Encrypted Transport VPN with onboard acceleration, and Secure Sockets Layer (SSL) VPN
- 4-port 10/100 Fast Ethernet managed switch with VLAN support; two ports support Power over Ethernet (PoE) for powering IP phones or external access points
- Secure 802.11g/n access point option based on draft 802.11n standard with support for Autonomous or Cisco Unified WLAN architectures

[1] Availability 2Half Calendar 2008

- CON/AUX port for console or external modem
- 1 USB 1.1 port for security e-token credentials, booting from USB, loading configuration
- Easy setup, deployment, and remote management capabilities through Web-based tools and Cisco IOS Software

Figure 35. Cisco 880 Series Integrated Services Router

Table 11. Cisco 880 Series Data Models

Models	WAN Interface	LAN Interfaces	802.11g/n Option	Integrated 3G *	Integrated ISDN Dial Backup
Cisco 881	10/100-Mbps Fast Ethernet	4-port 10/100-Mbps managed switch	Yes (Cisco 881W)	Yes (Cisco 881G) *	–
Cisco 888	G.SHDSL	4-port 10/100-Mbps managed switch	Yes (Cisco 888W)	Yes (Cisco 888G)	Yes

* Available in second half of calendar year 2008

Cisco 860 Product Overview

The Cisco 860 Series Integrated Services Routers combine Internet access, security, and wireless services onto a single, secure device that is simple to use and manage for small businesses. Cisco 860 Series delivers features, including firewall, IPSec VPNs, and WLANs, at broadband speeds to small offices. Easy deployment and centralized management features enable the Cisco 860 Series to be deployed by service providers for small businesses.

Benefits

Cisco 860 Series Integrated Services Routers offer:

- Concurrent broadband services for small offices, and remote sites
- Secure connectivity with Stateful Inspection Firewall and IP Security (IPSec) VPN support for small offices
- 4-port 10/100 Fast Ethernet managed switch with VLAN support
- CON/AUX Port for console or external modem connections
- Secure 802.11g/n access point option based on draft 802.11n
- Easy setup, deployment, and remote management capabilities through Web-based tools and Cisco IOS Software
- Security features including:
  - Stateful Inspection Firewall
  - IP Security (IPSec) VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES])

Figure 36. Cisco 860 Series Integrated Services Router

Product Management Contact: Harbans Kaur, harbkaur@cisco.com

4.7.4) Cisco Business-Class IAD880 Series Integrated Access Devices

The Cisco IAD880 Series Integrated Access Devices are cost-effective, fixed configuration, customer premises equipment for service providers offering managed voice and data services. It offers a set of cost-effective platforms for providing interconnect solutions for accelerating the migration from Time-Division Multiplexing (TDM) to Voice over IP (VoIP). It provides secure concurrent services, including firewall, content filtering, VPNs, and WLANs, at broadband speeds to small offices.

The Cisco IAD880 Series includes fixed configuration platforms with voice ports, WAN uplinks, embedded encryption acceleration, voice Digital-Signal-Processor (DSP) slots on the motherboard, IPS, and IPSec features while maintaining a desktop form factor for space-saving service provider managed services deployments.

Figure 37. Cisco IAD880 Integrated Access Device

Table 5 lists the routers that currently comprise the Cisco IAD880 Series.

Table 12. Cisco IAD880 Series Models

Model	WAN Interface	LAN Interfaces	VPN	Voice	Data Backup	802.11n Wireless (b/g Compatible)
IAD881	10/100 Mbps Fast Ethernet	4-port 10/100-Mbps managed switch	Up to 20 tunnels	4 FXS or 2 BRI	-	An option on all IAD881 SKUs
IAD888	G.SHDSL (Symmetrical High-Data-Rate DSL)	4-port 10/100-Mbps managed switch	Up to 20 tunnels	4 FXS or 2 BRI	ISDN	An option on all IAD888 SKUs

Primary Features and Benefits to Service Providers

Cost Effectiveness

The Cisco IAD880 Series offers the entire gamut of industry-leading features at a very cost effective price for service providers. With flexible support for a variety of WAN interfaces and line side voice interfaces, wireless services, as well as integrated security services, the Cisco IAD880 Series is customized to the unique requirements for the small and medium-sized business. Priced with the small and medium-sized business customer in mind, the feature-rich Cisco IAD880 Series offers superior value to a service provider interested in taking advantage of the growing managed small and medium-sized business services market.

Transparent Service Migration

The Cisco IAD880 Series can help service providers transparently migrate end customers from TDM-based voice service to call agent-based packet voice services without the need for a complete equipment upgrade at the end-customer site. The provider can choose SIP, MGCP or H.323 for VoIP protocols, based on the services that need to be delivered.

Flexibility

The Cisco IAD880 Series offers both TDM and VoIP with rich VoIP signaling protocol support. Combined with the option for call agent- and BRI-based network designs, the Cisco IAD880 Series offers powerful flexibility in the design of next-generation multiservice networks.

Functional Intelligence

When used with the popular Cisco Configuration Express tool, the auto-installation technology offers true ready-to-use installation. In addition, the Cisco IAD880 Series is based on Cisco IOS Software and provides the same IP features that power more than 80 percent of the Internet infrastructure. Cisco IOS Software delivers rich data services, allowing service providers to gain additional data revenue, in addition to proven industry-tested voice features.

Operational Efficiencies

The new Cisco IAD880 Series can increase operational efficiencies by reducing or eliminating the necessity for complete hardware upgrades, warehousing, complete equipment upgrades, and highly skilled technician involvement. Service providers that deploy these devices with other Cisco equipment and Cisco IOS Software can cost-effectively extend training, administration, and maintenance activities across the entire network.

End-to-End Solution

Because the Cisco IAD880 Series is compatible with a wide range of industry-leading DSL Access Multiplexers (DSLAMs) and voice gateways and offers world-class data features of Cisco IOS Software, service providers can deploy a highly efficient and scalable end-to-end multiservice network. The Cisco IAD880 Series is an integral part of Cisco packet voice solutions.

Primary Benefits to End Users

Robust Voice Quality

The Cisco experience in providing toll-quality packet-voice service helps ensure that the Cisco IAD880 Series provides the clear, robust voice quality that users have come to expect from telephony services.

Reliability

Cisco products are known for their exceptional reliability earned through years of proven industry service. The Cisco IAD880 Series extends the same reliability standards to managed service environments to provide end users with high levels of dependability.

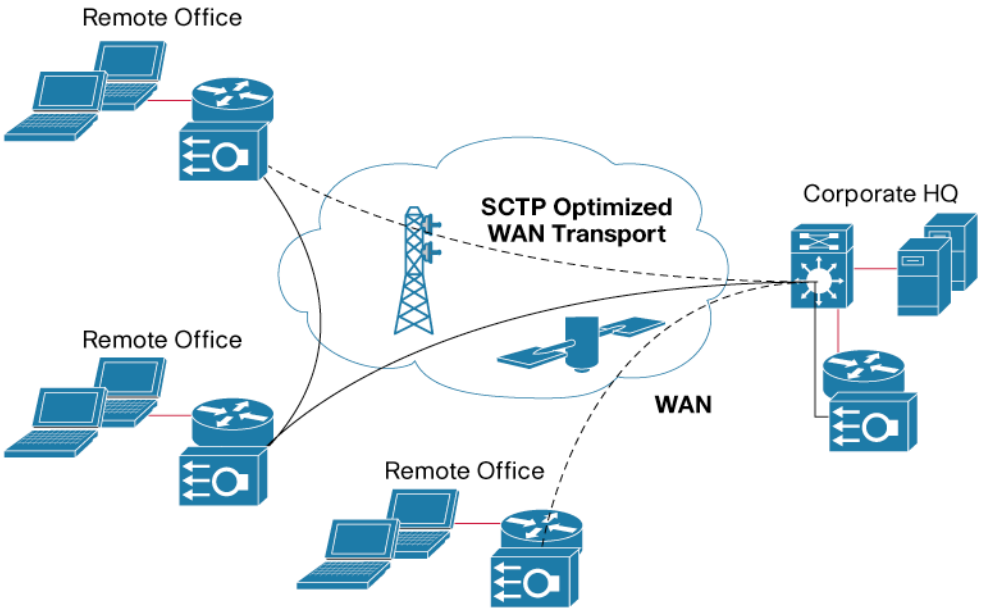
Service Flexibility

Today's rapidly changing business environment leads to constant change in network requirements of small and medium-sized businesses. The Cisco IAD880 Series allows service providers to add or remove service offerings remotely based on end-user needs.

Network Capacity Expansion (NCE) System for Cisco ISRs

Cisco Network Capacity Expansion (NCE) System is a transparent proxy that increases the amount of available bandwidth at small to midsized branch offices and remote locations. It is designed to cost-effectively accelerate data transfer over the WAN by overcoming bandwidth limitations, and mitigating effects of latency and packet loss. With NCE, multisite organizations get more data through and more value out of their existing WAN links. Unlike other bandwidth optimization or latency mitigation products, Cisco NCE is a small-footprint module that easily integrates into the modular Cisco ISRs.

Figure 38. Network Capacity Expansion (NCE) System for Cisco ISRs



Benefits

- Accelerates WAN data transfer 3-20 times
- Hardware-based Layer 4 compression
- SCTP-based TCP optimization
- Cost-effective and network transparent
- Targeted at all TCP based applications
- Based on IETF standards (SCTP, Deflate, PEP)

Hardware

Routers	• Cisco 1841, 2800, and 3800 Series Routers

Additional Information: http://www.cisco.com/en/US/products/ps9702/index.html

Product Management Contact: ask-nce-pm@cisco.com

4.8) Voice

4.8.1) Communications Manager Express (CME) 7.0 Voice Features
Cisco IOS Release 12.4(20)T contains several new features for customers using Communications Manager Express call processing:

E911 Support

E911 feature provides support for the enhanced 911 services to connect your Cisco Unified Communications Manager Express system to your local Public Safety Answering Point (PSAP).

The E911 feature includes:

1. Option to define unlimited number of Emergency Response Locations (ERL) for handling 911 calling party translation
2. Each ERL can have two (2) Emergency Location Identification Numbers (ELIN) for handling two calls at once from the ERL
3. Phones can be assigned to an ERL by use of IP address subnets or by using phone Mac address
4. On an outbound call to 911 (or any defined emergency number) the IP Phone calling party number is changed to the ELIN to allow the Public Safety Answering Point to know the location of the caller
5. Return calls from the Public Safety Answering Point to the IP Phone are routed back to the original 911 caller
6. Return calls from PSAP are routed to an operator or security personnel in case no matching E911 callback record is found
7. Ability to connect the CME system to multiple Public Safety Answering Points
8. Flexible ERL matching with the use of zones allowing for ranking of the locations and controlling the order of ERL searches
9. History of E911 calls placed can be viewed using Cisco IOS CLI Show command, or tracked via Radius or CSV Call Detail Record (CDR) collection
10. Use of CME E911 requires Primary Rate Interface (PRI) or Centralized Automated Message Accounting (CAMA) trunks

New Comma Separated Value Format and Supplementary Services Enhancements for Call Detail Records (CDR)

Cisco Unified Communications Manager Express can now generate Call Detail Records in a Comma Separated Value (CSV) format. The records in the CSV format can be either stored on the CME router flash or sent to a billing server directly using the File Transfer Protocol (FTP).

Extension Mobility

Extension Mobility in Cisco Unified CME provides the benefit of phone mobility for end users. A user login service allows phone users to temporarily access a physical phone other than their own phone and utilize their personal settings, such as directory number, speed-dial lists, and services, as if the phone is their own desk phone. The phone user can make and receive calls on that phone using the same personal directory number as is on their own desk phone.

Octo-line support

An octo-line directory number supports up to eight active calls, both incoming and outgoing, on a single phone button. Unlike a dual-line directory number, which is shared exclusively among phones (after a call is answered, that phone owns both channels of the dual-line directory number), an octo-line directory number can split its channels among other phones that share the directory number. All phones are allowed to initiate or receive calls on the idle channels of the shared octo-line directory number.

Call Barge with Privacy Release

The Barge feature enables phone users to join a call on a shared octo-line directory number by pressing the Cbarge soft key and converting the call to an ad hoc conference. This feature uses a hardware conference bridge configured in Cisco Unified CME. When the initiator barges into a call, an ad hoc conference is created between the barge initiator, the target party, and the other party connected in the call. Parties see the call information on their phone displays and, if the conference join tone is configured, hear a tone. The call information for all parties changes to barge and the participants can add more parties to the conference or drop any party. The initiator of the barge sees a new call created on their line in the connected state. The original remote-in-use call at the initiator does not change state as a result of the barge. The target party of the barge sees a new call created on their line in the remote-in-use state. The original connected call at the target party does not change state as a result of the barge.

The privacy feature enables phone users to block other users from seeing call information or barging into a call on a shared octo-line directory number. When a phone receives an incoming call on a shared octo-line, the user can make the call private by pressing the Privacy feature button, which toggles between on and off to allow the user to alter the privacy setting on their phone. The privacy state is applied to new calls and current calls owned by the phone user.

Privacy is enabled for all phones in the system by default. You can disable privacy globally and enable it for specific phones only, either individually or through an ephone template.

Add/change speed dial on phone

IP phone users can now configure their own speed-dial and fast-dial settings directly from the phone. The speed-dial and fast-dial settings can be added or modified on the phone by using a menu available with the Services feature button. Extension Mobility users can add or modify speed-dial settings in their user profile after logging in. The logout profile is not configurable from the phone.

Transfer to Voice Mail

The Transfer to Voice Mail feature allows a phone user to transfer a caller directly to a voice-mail extension. The user presses the TrnsfVM soft key to place the call on hold, enters the extension number, and then commits the transfer by pressing the TrnsfVM soft key again. The caller hears the complete voice mail greeting. This feature is supported using the TrnsfVM soft key or Feature Access Code (FAC).

Live Record Softkey with Cisco Unity Express

The Live Record feature enables IP phone users in a Cisco Unified CME system to record a phone conversation if Cisco Unity Express is the voice mail system. An audible notification, either by announcement or by periodic beep, alerts participants that the conversation is being recorded. The playing of the announcement or beep is under the control of Cisco Unity Express.

Blast/Parallel Hunt Group

Parallel hunt groups are a type of hunt groups where incoming calls simultaneously ring multiple phones. Using parallel hunt groups is also referred to as application-level forking because it enables the forking of a call to multiple destinations. In versions earlier than Cisco Unified CME 7.0, only SIP phones support parallel hunt groups. In Cisco Unified CME 7.0 and later versions, SCCP phones also support voice hunt groups.

Call Transfer Recall

The Call-Transfer Recall feature in Cisco Unified CME returns a transferred call to the phone that initiated the transfer if the destination does not answer. After a phone user completes a transfer to a directory number on a local phone, if the transfer-to party does not answer, the call is forwarded back to the transferor phone after the configured recall timer expires.

If the transfer-recall timer expires before a call is answered, the call is directed back to the transferor phone if the transfer-to directory number does not have Call Forward Busy enabled and is not a member of any hunt group.

Integration with Cisco 3200 Rugged ISR (previously the Cisco Mobile Access Router)

Cisco Unified CME on the Cisco 3200 Series can be deployed in sites requiring on demand network connectivity and voice and data communications that typically do not have PSTN connectivity. The benefits include:

- Ensures voice communications locally if the WAN link fails
- Allows greater autonomy for voice communications at remote sites
- Supports H.323 and SIP trunks
- Easily portable

SRTP media encryption for secure conversation

Cisco Unified Communications Manager Express now supports SRTP for media encryption to provide secure conversations. SRTP for secure media encryption when used with secure call control signaling using either Transport Layer Security (TLS) or IP Security (IPSec) channel provides completely secured communications.

Cisco Unified CME manages the SRTP keys to endpoints and to gateways. The Media Encryption (SRTP) on Cisco Unified CME feature supports the following features:

- Secure voice calls using SRTP for SCCP endpoints
- Secure voice calls in a mixed shared line environment that allows both RTP and SRTP capable endpoints; shared line media security depends on the endpoint configuration.
- Secure supplementary services using H.450 including:—Call forward—Call transfer—Call hold and resume—Call park and call pickup—Nonsecure software conference
  Note: SRTP conference calls over H.323 may experience a 0 to 2 second noise interval when the call is joined to the conference
- Secure calls in a non H.450 environment
- Secure Cisco Unified CME interaction with secure Cisco Unity
- Secure Cisco Unified CME interaction with Cisco Unity Express (interaction is supported and calls are downgraded to nonsecure mode)
- Secure transcoding for remote phones with DSP farm transcoding configured

Interoperability with Cisco Unified Contact Center Express 5.0

Cisco Unified CME now supports interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) 5.0 and later versions with Cisco Unified Call Center Express (Unified CCX), including enhanced call processing, device and call monitoring, unattended call transfers to multiple call center agents and basic extension mobility, and IP IVR applications.

The Unified CCX application uses the CRS platform to provide a multimedia (voice, data, and web) connection. Cisco IP IVR functionality is available with Unified CCX and includes prompt-and-collect and call treatment.

The following functions are provided in Cisco Unified CME

- Support of Unified CCX Cisco Agent Desktop for use with Cisco Unified CME
- Configuration query and update between Unified CCX and Cisco Unified CME
- SIP-based simple and supplementary call control services including:
  - Call routing between Cisco Unified CME and Unified CCX using SIP-based route point
  - First-party call control for SIP-based simple and supplementary call
  - Call monitoring and device monitoring based on SIP presence and dialog event package
- Unified CCX session management of Cisco Unified CME
- Unified CCX device and call monitoring of agent lines and call activities in Cisco Unified CME

G.722 and iLBC Codec Support

In Cisco Unified CME, support for G.722-64K and the Internet Low Bit Rate Codec (iLBC) have now been added. This enables Cisco Unified CME to support the same codecs that are used in newer Cisco Unified IP phones, mobile wireless networks, and internet telephony without transcoding. This feature provides support for the following:

- iLBC and G.722-capable SIP and SCCP IP phones in Cisco Unified CME
- iLBC-capable SCCP analog endpoints and remote phones in Cisco Unified CME
- Conferencing support for G.722 and ILBC

- Supplementary services, such as transfer, call forward, MOH, support for G.722 and iLBC, including any supplementary services that require transcoding between G.722 and any other codec
- Transcoding for G.722 and iLBC, including G.722 to G.711 and G.722 to any other codec

Hardware

Routers	• Cisco 2800 and 3800 Series Integrated Services, UC500 Series Routers

Product Management Contact: Vipul Jain (vipujain@cisco.com)

4.8.2) Survivable Remote Site Telephony 7.0 Voice Features

Cisco IOS Software Release 12.4(20)T contains new features for customers using Cisco Unified Survivable Remote Site Telephony (SRST) for backup call control with a centralized Communications Manager cluster:

Octo-line support

With the octo-line support in the Cisco Unified SRST, a single phone button can have up to 8 active calls, both incoming and outgoing during the time the connection to the centralized communications manager is out of service.

Hardware

Routers	• Cisco 2800 and 3800 Series Integrated Services Routers

Product Management Contact: Vipul Jain (vipujain@cisco.com)

4.8.3) Cisco Unified Border Element (CUBE) 1.2

Cisco Unified Border Element provides the necessary services for interconnecting Unified Communications networks securely, flexibly and reliably. Designed to meet Enterprise and service provider UC interconnection needs, including Session Border Controller (SBC) functions, Cisco Unified Border Element is an integrated Cisco IOS Software application.

Figure 39.

The new features in CUBE 1.2 enable unprecedented adaptability and interoperability with more endpoints. SIP profiles enable the integration of new types of devices and applications and allow for interoperability with third party devices that require specific SIP messages. Additional features include SIP video for Telepresence calls, Session Border Controller Enhancements for H.323 video, H.239 signaling, H235 security and universal transcoding.

Hardware

Routers	• Cisco 2800, 3800, AS5350XM and AS5400XM Series

Additional Information: http://www.cisco.com/go/cube

Product Management Contact: ask-cube-pm@cisco.com

4.8.4) Voice Quality Improvements on Cisco VoIP Gateways

The G.722-64 and iLBC codecs can now be used to enable conferencing and transcoding on Cisco IOS voice gateways in a Cisco Unified Communications Manager or in a Cisco Unified Communications Manager Express network. Digital Signal Processor (DSP) farms provide conferencing and transcoding services using DSP resources on high-density digital voice/fax network modules (PVDM2). G.722-64 brings “high definition” voice for the branch office using the same bandwidth as G.711 (64Kbps). iLBC provides high robustness to packet loss while maintaining good voice quality with efficient bandwidth usage.

A rich set of voice quality metrics such as K factor and late voice packet counts are made available in gateways for SIP and H323 signaling protocols in addition to MGCP. The metrics available via IOS CLIs, CDRs and Syslog can be used for efficient diagnostics and proactive monitoring of voice calls. Troubleshooting problems such as one way audio and echo are made easier for network administrators. Voice jitter buffer improvement applicable on the Cisco VoIP gateways results in overall improved VoIP call quality and better delay adaptation with a variety of endpoints in branch offices.

Integrated 3G-324M Gateway Support on the AS5000 Series

Cisco adds the 3G-324M standard gateway protocol to IOS to be supported on the AS5350XM and AS5400XM for video telephony services. This feature enables the IP video and voice network implementations to talk directly to the next generation 3G mobile networks.

In addition, the Cisco 3G-Gateway functionality interfaces with the Cisco Unified Customer Voice Portal (CVP) SIP Back-to-Back User Agent (B2BUA). This allows Interactive Voice Response (IVR) sessions that start as an audio call to switch to video IVR session providing an enhanced customer experience. Ultimately, these video calls are transferred to agents with video capabilities. The 3G-324M gateway functionality is supported for basic calls and also for calls which require supplementary services like hold, resume, transfer and conference. The Cisco IOS 3G-324M gateway solution supports a wide range of endpoint types including H.263+ endpoints which are commonly adopted for this type of solution. Cisco IOS Software Release 12.4(20)T further enhances the video capabilities on the Cisco Integrated Services Router (ISR) 2800 and 3800 Series by implementing H.320 ISO-13871 bonding enhancements to the existing Cisco IOS H.320 Gateway functionality.

Land Mobile Radio (LMR) Over IP - Tone Control Feature

Cisco IOS Release 12.4(20) T enhances the Land Mobile Radio (LMR) Over IP capabilities of the Cisco Integrated Services Router (ISR) 2800 and 3800 Series by providing RFC2833 based tone control feature for use with Cisco IPICS2.1.

ISDN Q.931 tunneling over SIP

This feature enables ISDN Q.931 tunneling using the RAW format over the SIP TDM gateway.

Hardware

Routers	• Cisco AS5350XM and AS5400XM Series

Product Management Contacts:

Teresa Newell, tnewell@cisco.com

Li Shen, lishen@cisco.com

5) Release 12.4(15)T Highlights

Table 13. Release 12.4(15)T Feature Highlights

5.1) Cisco IOS Security	5.2) Routing and Multicast	5.3) IP Services	5.4) High Availability	5.5) Connectivity
5.1.1) Cisco IOS Intrusion Prevention System (IPS) Support for Microsoft Vulnerabilities *	5.2.1) OSPF Mechanism to Exclude Connected Prefixes	5.3.1) Gateway Load Balancing Protocol (GLBP) Client Cache	5.4.1) Bidirectional Forward Detection (BFD) Support for Cisco Integrated Services Routers*	5.5.1) Multiple PPP-over-Ethernet (PPPoE) Clients per VC Support
5.1.2) Flexible Packet Matching (FPM) Full Packet Filtering *	5.2.2) Optimized Edge Routing (OER) Application Aware Routing *	5.3.2) Dynamic Host Configuration Protocol (DHCP) Server Multiple Subnet		5.5.2) Layer 2 Tunneling Protocol (L2TP) Forwarding of PPPoE Tags
5.1.3) Cisco IOS SSL VPN Enhancements	5.2.3) OER Link Grouping	5.3.3) Hot Standby Routing Protocol (HSRP) Bidirectional Forwarding Detection (BFD) Peering		
5.1.4) Cisco IOS Software Support for AnyConnect VPN Client	5.2.4) Bandwidth Call Admission Control (CAC) for IP Multicast	5.3.4) DHCPv6 Stateless Enhancements		
5.1.5) Reverse Route Injection Distance Metric Enhancements				

5.6) Management, Instrumentation, and User Interface	5.7) Mobility and Wireless	5.8) Voice	5.9) Hardware
5.6.1) Cisco IOS Auto-Upgrade Manager * 5.6.2) Cisco IOS Embedded Resource Manager * 5.6.3) Toolkit Command Language (TCL) Signing	5.7.1) Mobile Ad Hoc Networking (MANET) Networking Enhancements for Router Radio Links 5.7.2) Access Point Link Role Flexibility * 5.7.3) IP Pool Address Holdback Timer	5.8.1) Communications Manager Express (CME) 4.1 Voice Features 5.8.2) Survivable Remote Site Telephony 4.1 Voice Features	5.9.1) Cisco 7201 Router * 5.9.2) ATM T3/E3 for the Cisco 2800 and3800 Series Integrated Services Router 5.9.3) HWIC-2SHDSL & HWIC-4SHDSL 5.9.4) Cisco 1- and 2-Port Enhanced Capability T3/E3 Clear Channel Port Adapters and Feature Offload Support for Multichannel T3 Port Adapters 5.9.5) USB eToken 64KB Enhancement 5.9.6) Boot from USB Flash Enhancement

* Indicates Key Highlight

5.1) Cisco IOS Security

5.1.1) Cisco IOS Intrusion Prevention System (IPS) Support for Microsoft Vulnerabilities
Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. As a core facet of the self-defending network, Cisco IOS IPS enables the network to defend itself with the intelligence to accurately identify, classify, and stop or block malicious or damaging traffic in real time.

While it is common practice to defend against attacks by inspecting traffic at the data centers and corporate headquarters, distributing the defense to stop malicious traffic close to its entry point at the branch offices is also critical. Deploying inline Cisco IOS IPS at the branch enables gateways to drop offending traffic, send an alarm, block an attacker or reset a potentially malicious client-server connection as needed to stop attacking traffic at its point of origin.

Key **Benefits** of Cisco IOS IPS features include:

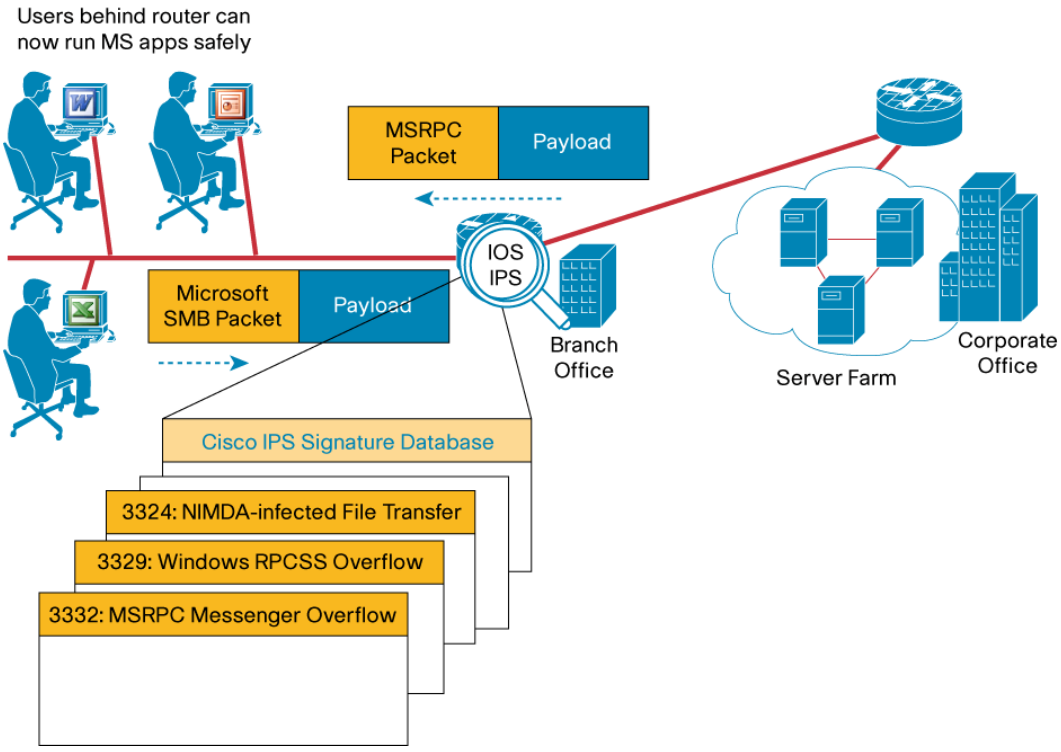
- Provides network-wide, distributed protection from many worms, viruses, and attacks exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as in small and medium-sized business networks
- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports same signature database available for Cisco Intrusion Prevention System (IPS) appliances

In Cisco IOS Software Release 12.4(15)T, Cisco IOS Intrusion Prevention System (IPS) provides support for the Cisco IPS Software Version 5.x/6.0 signature format, which is also used by the latest Cisco appliance-based IPS products. The Cisco IPS version 5.x signature format is improved to support encrypted signature parameters and other features such as signature Risk Rating. In this release, Cisco IOS IPS feature will also support signatures for many vulnerabilities found in Microsoft Server Message Block (SMB) and Microsoft Remote Procedure Call (MSRPC) protocols. Both of those protocols are widely and frequently used by most of Microsoft's computer applications and software packages.

New Cisco IOS IPS features in Cisco IOS Release 12.4(15)T provides:

- Signatures for vulnerabilities in Microsoft SMB and MSRPC protocols
- Support for encrypted signatures provided by vendors under NDA (such as Microsoft)
- Risk Rating value in IPS alarms for efficient event filtering, monitoring and correlation
- Supports Signature Event Action Processor (SEAP) for automated adjustment of signature event actions based on Risk Rating
- Support for the same signature format as the latest Cisco IPS appliance/module software version
- Individual and category based signature provisioning capabilities via Cisco IOS CLI
- XML-based IDCONF signature provisioning mechanism
- Automated signature updates (at periodic intervals) from a local TFTP or HTTP/HTTPS server

Figure 40. IPS Now Supports Microsoft SMB and MSRPC Signatures Natively



Benefits of IPS Features in Cisco IOS Software Release 12.4(15)T

- **Enhanced Microsoft Signature Support (MSRPC and SMB):**

  Cisco IOS IPS adds support for ~95 signatures for vulnerabilities in Microsoft Remote Procedure Call (MSRPC) and Microsoft Small Message Block (SMB) protocols.

- **Support for Encrypted Signatures Released Under NDA:**

  Cisco IOS IPS can now scan for encrypted signatures for certain vulnerabilities as provided by vendors under NDA (such as Microsoft) sometimes even before their public release.

- **More Accurate and Efficient Event Monitoring with Reduced False Positives:**

  Event Risk Rating value provided in IPS alarms are calculated based on signature severity, signature fidelity (high fidelity signatures have a lower rate of false positives) and a “target

value rating" defined by users. Event monitoring/correlation applications or devices such as CS-MARS may use the Risk Rating (RR) value in IPS alarms to filter out events below a certain RR threshold and/or trigger event correlation/action rules based on relative importance of IPS events indicated by their Risk Rating value.

- **Quick and Automated Adjustment of Signature Event Actions Based on Calculated Risk:**

  The Signature Event Action Processor (SEAP) feature allows overriding of default signature actions based on calculated Risk Rating value. For instance, signatures generating events with a Risk Rating value of 90 or higher (on a scale of 1 to 100) may be configured to drop offending packets and/or deny traffic from the attacker's address in addition to the default action of simply sending an alarm.

- **Common Operational Model for Cisco IPS Appliances, Modules and Cisco IOS IPS:**

  In this release, Cisco IOS IPS starts using the same signature format and deployment/update/provisioning mechanism as all other Cisco IPS devices allowing Cisco Security Manager 3.1 to apply the same policy changes (signature tunings) to all Cisco IOS routers, IPS appliances and modules in a customer network.

- **Secure and Scalable Management of Signature Policies for Any Kind of Deployment:**

  Security Device Manager 2.4 and Cisco Security Manager 3.1 provides complete IPS provisioning capabilities for a single router and multiple routers and IPS devices, respectively. Both management applications use IDCONF protocol running securely over HTTPS. Granular customization and tuning of signatures is also possible via CLI and custom CLI scripts. For large scale deployments, it is possible to distribute signature selection and action tunings applied to a single router to a large number of routers using Cisco Configuration Engine.

- **Timely Protection from the Latest Threats with Minimal User Intervention:**

  Automated and periodic signature updates from a local TFTP or HTTP(S) server.

Hardware

Routers	• Cisco 87x, 1800, 2800, 3700, 3800, 7200 Series Routers

Additional Information: http://www.cisco.com/go/iosips

Product Management Contact: Kemal Akozer (kemal@cisco.com)

5.1.2) Flexible Packet Matching (FPM) Full Packet Filtering

Flexible Packet Matching (FPM) is the next-generation Access Control List (ACL) technology that provides a flexible and rapid first line of defense against malicious traffic at the entry point into the network. It features powerful custom pattern matching deep within the packet header or payload, minimizing inadvertent blocking of legitimate business traffic.

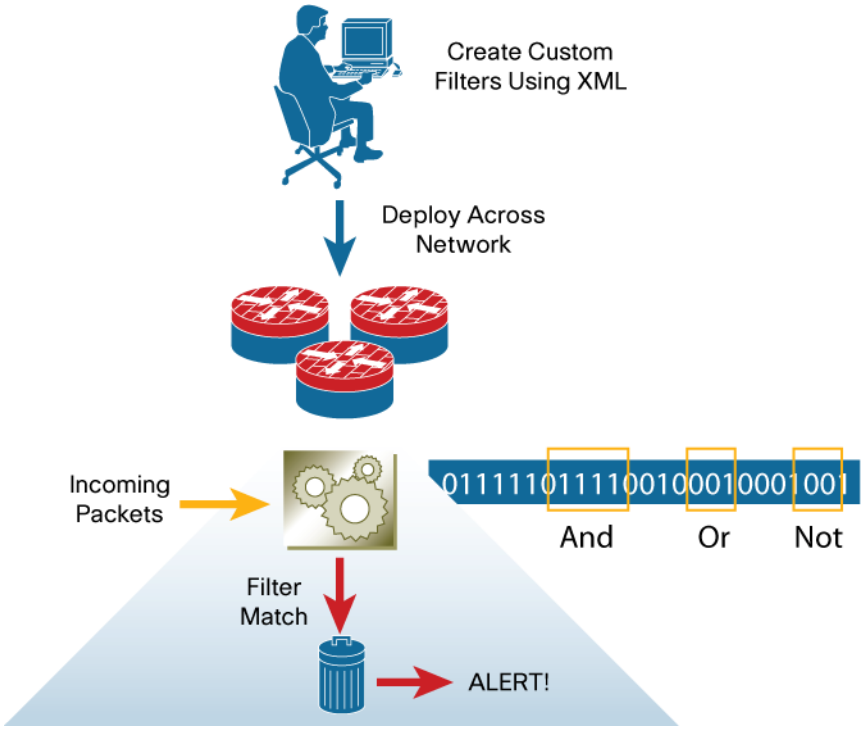
FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM further extends the network traffic class definition capability to include new CLI syntax to offset into a user-defined protocol header and, furthermore, into the data portion of the packet.

FPM provides network security administrators with powerful tools to identify miscreant traffic as it enters the network, and to immediately drop and/or keep a log for audit purposes. Administrators can specify custom match patterns at multiple offsets within the packet. FPM includes ready-made

definitions for standard protocols via Protocol Header Definition Files (PHDF), which simplify deployment. Customers can also customize and add extensions to PHDFs at device run time.

FPM was first introduced in Cisco IOS Release 12.4(4)T. In the initial release, FPM was limited to searching for patterns 32 bytes long within the first 256 bytes of a packet. Release 12.4(15)T extends the FPM matching capability by allowing network security administrators the ability to search for strings up to 256 bytes long anywhere within the entire packet. This provides greater flexibility for defining filters for miscreant traffic targeting your network.

Figure 41. Flexible Packet Matching Process



Benefits

- FPM enables users to create their own stateless packet classification criteria and to define policies with multiple actions (ie: drop, log or send ICMP unreachable) to immediately block new viruses, worms, and attacks
- FPM provides a flexible, granular Layer 2-7 matching capability providing the ability to inspect packets for characteristics regardless of the header fields involved
- FPM goes beyond static attributes allowing you to specify arbitrary bits/bytes at any offset within the entire packet (header or payload), minimizing inadvertent blocking of legitimate business traffic
- Allows network security administrators to rapidly set up custom filters using CLI or XML-based policy language
- Useful for Security Incident Response Teams for reacting to threats targeting their networks

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 and 7301 Series

Considerations

The Flexible Packet Matching feature is only available in Cisco IOS Software Release 12.4(15)T (and higher) Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

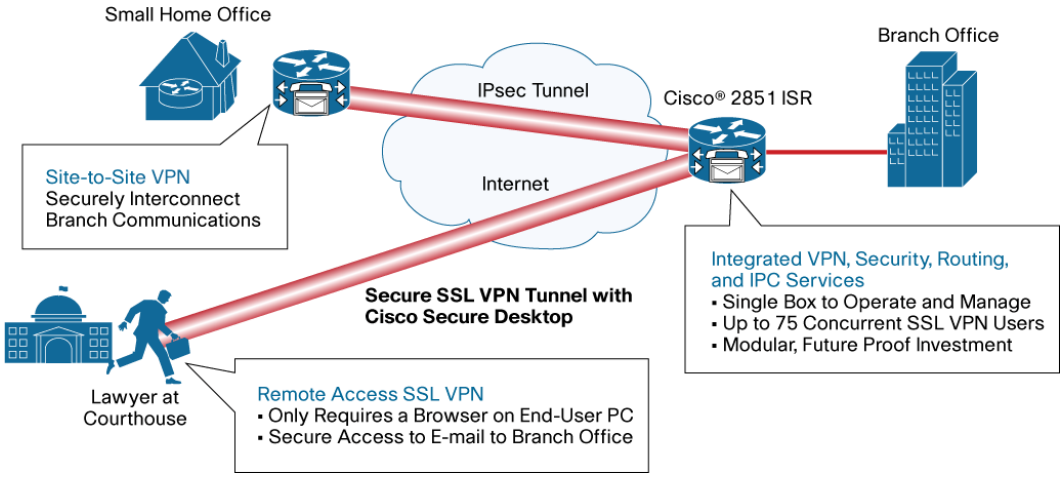
Additional Information: http://www.cisco.com/go/fpm

Product Management Contact: ask-stg-ios-pm@cisco.com

5.1.3) Cisco IOS SSL VPN Enhancements

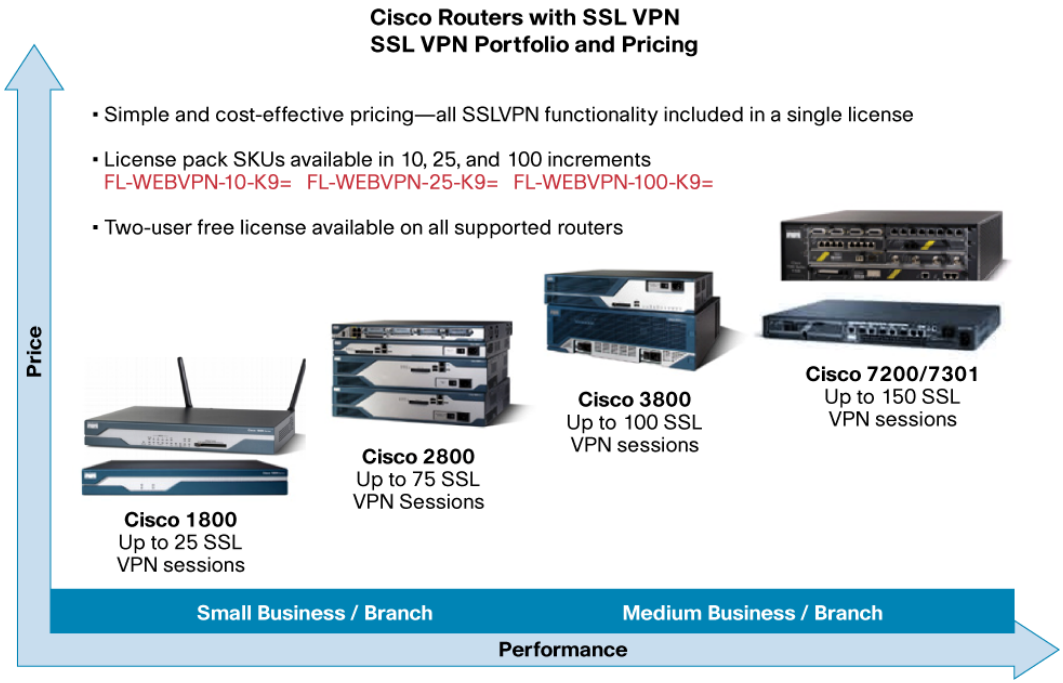
Unlike IPsec-VPN, SSL VPN in clientless mode is an application-aware technology. Using SSL VPN on the routers, companies can securely and transparently extend their companies' networks to any Internet-enabled location. SSL VPN is compelling because the security is transparent to the end user and easy for IT to administer. Using only a Web browser, companies can extend their secure Enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots-thereby enabling higher employee productivity and protecting corporate data. Cisco IOS SSL VPN supports clientless access to applications such as HTML-based intranet content, email, network file shares, and Citrix. While this allows for a great end-user experience, it must be balanced with proper access-control so end-users have access to only those resources dictated by corporate policy. Figure 29 provides a use-case scenario for customers to implement Cisco IOS SSL VPN effectively at the branch.

Figure 42. IOS SSL VPN Use Case Scenario



Cisco IOS® SSL VPN is a licensed feature supported on Cisco® 871, 1800, 2800, 3700, 3800, 7200, and 7301 routers running the Advanced Security image since Cisco IOS Software Release 12.4(6)T (and higher). You can purchase the feature license in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com ordering tool or through your Cisco partner/account team. Figure 30 provides more portfolio and license pricing details.

Figure 43. Cisco IOS SSL VPN Portfolio and Pricing



New SSL VPN features in Cisco IOS Software Release 12.4(15)T include the following:

1. SSL VPN Clientless Performance Enhancements
2. SSL VPN GUI Enhancements
3. SSL VPN User-level Bookmarking
4. Front Door-VRF Support

5.1.3.1) SSL VPN Clientless Performance Enhancements

Prior to this feature, traffic from clientless SSL VPN users was processed switched. Clientless performance enhancements bring CEF support to clientless SSL VPN traffic through this Cisco IOS SSL VPN gateway. Cisco Express Forwarding (CEF) technology for IP is a scalable, distributed, layer 3 switching solution designed to meet the future performance requirements of the Internet and Enterprise networks. Hardware acceleration is also now supported, offloading the processor from extensive cryptographic computations.

Reduction of the overall load of the processor allows for greater scalability and throughput providing for an improved user experience and user density per router. Reducing the CPU load also allows for configuration of other concurrent features on the router. CEF and hardware support are enabled by default.

Benefits

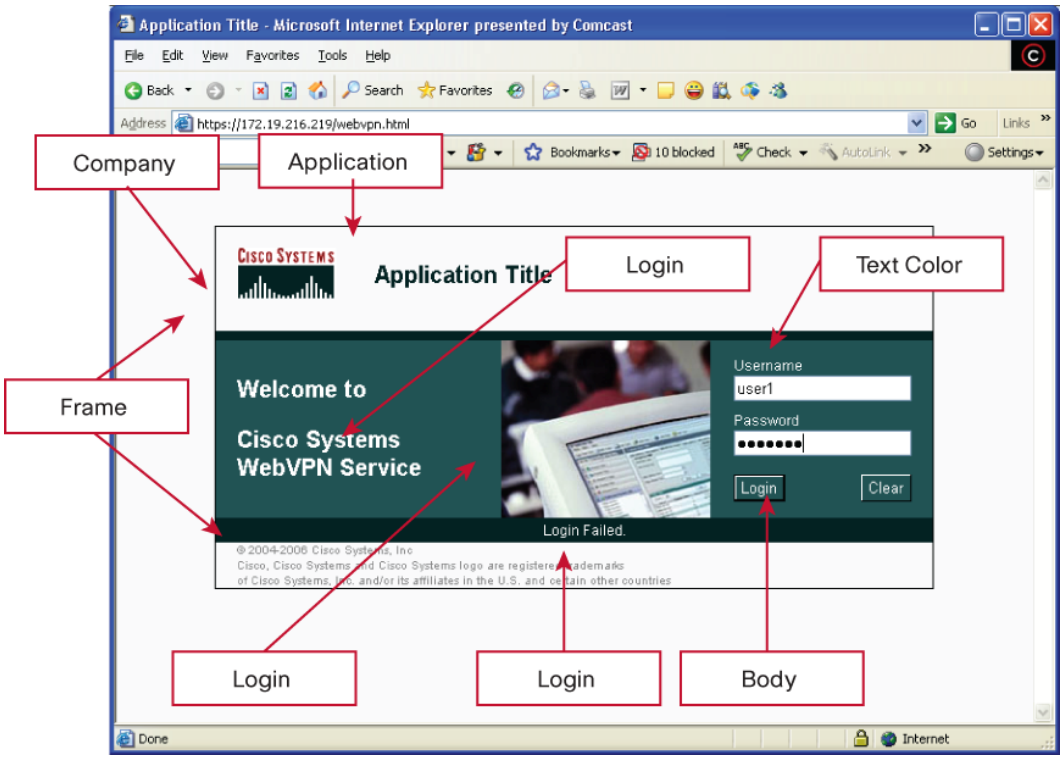
- **Increased Scalability and Performance:** Increased number of concurrent users and throughput.

5.1.3.2) SSL VPN GUI Enhancements

Ergonomic improvements of the GUI user interface of the Cisco IOS SSL VPN gateway have been added. Improved customization of the user interface provide for greater flexibility and ability to tailor the portal pages for an individualized look and feel. Features are more clearly delineated, making for a more intuitive and less cluttered interface. The portal page now spawns new pages for

mangled links or URLs, eliminating any need to navigate back to the portal page. The separate toolbar window has been replaced with an integrated floating toolbar that floats in either the upper left or right (dynamically configurable) of pages spawned from the portal page. Previous interface configurations are still available.

Figure 44. SSL VPN GUI Enhancements



User Configurable Enhancements:

- Login Banner message
- Login Picture

GUI Improvements:

- GUI layout
- Toolbar integrated directly into spawned pages:

Previous Configurable Elements:

- Login message
- Color accents
- Logo
- Secondary browser color
- Secondary text color

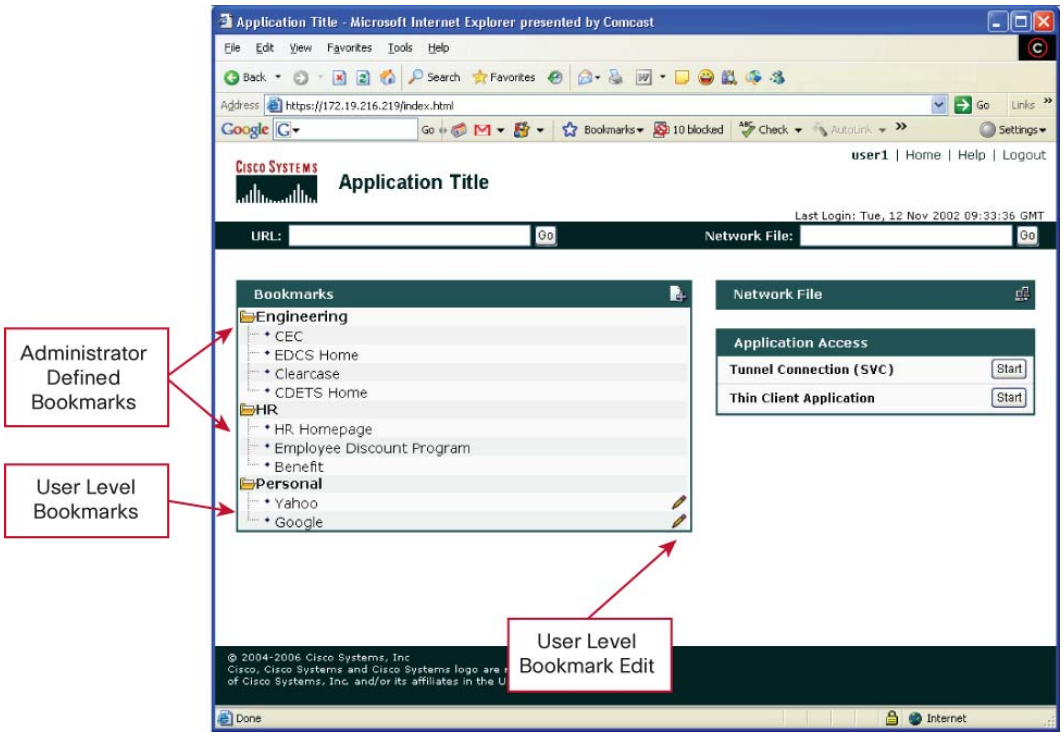
Benefits

- **Ease of use/Customization:** The improved GUI takes into account the latest Cisco IOS SSL VPN features and presents them in a layout that is more intuitive and aesthetic. Integration of the toolbar reduces clutter of the desktop by removing an extra window.

5.1.3.3) SSL VPN User-Level Bookmarking

User level bookmarking allows individual users to customize the portal page with their own bookmarks. Bookmarks are stored on the router and are linked to the individual user id's so the user's bookmarks are location/machine independent. The user profile location can be stored on any of the file systems on the router as well as externally such as a Trivial File Transfer Protocol (TFTP) server. In addition to administrator defined bookmarks, Cisco IOS SSL VPN users can create, edit, and delete their own individual bookmark list and have access to them on any computer at any location.

Figure 45. SSLVPN User-Level Bookmarking



Benefits

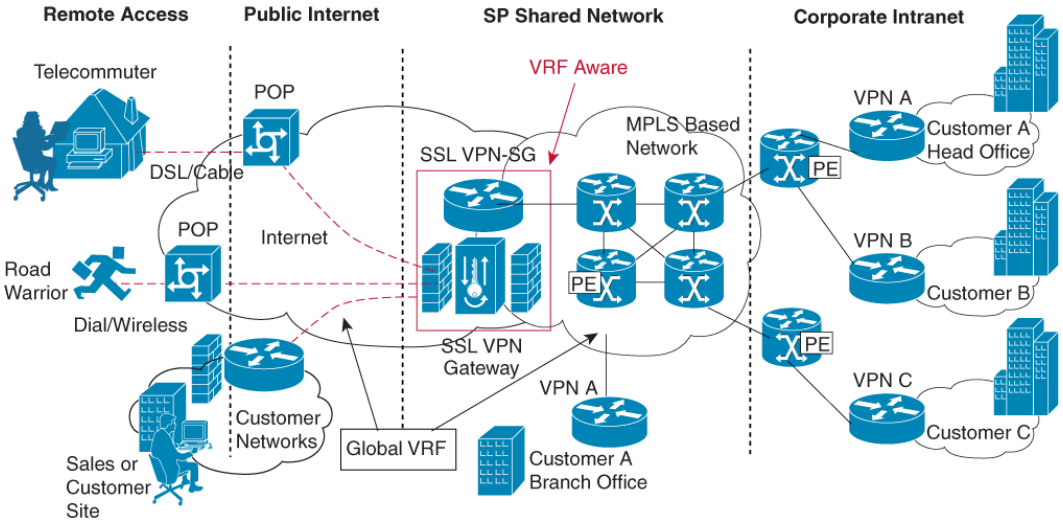
- **Increased Usability:** The user level bookmarking feature gives flexibility to users to customize the portal page to suit their individual needs. In addition to predefined links configured by the administrator, users can create a list of bookmarks that are most useful for them.

5.1.3.4) Front door-VRF (fVRF) Support

Front door-VRF (fVRF) support, coupled with the already supported internal VRF (iVRF) capability in Cisco IOS Software Release 12.4T, allows the Cisco IOS SSL VPN gateway to be fully integrated into an MPLS network. The virtual gateway can be placed into a VRF, separate from the Internet to avoid internal MPLS/IP network exposure. This reduces the vulnerability of the router by separating the Internet routes and/or the global routing table. Clients can now reach the gateway

via the fVRF which can be separate from the global VRF. The backend or iVRF functionality remains the same.

Figure 46. Front door-VRF Support



Benefits

- **Increased Security:** Cisco IOS SSL VPN virtual gateway can be placed and accessed on a separate VRF to reduce network exposure and provide support for overlapping IP addresses.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

5.1.4) Cisco IOS Software Support for AnyConnect VPN Client

The Cisco AnyConnect VPN Client is the Cisco next generation VPN client providing secure remote access through an SSL VPN tunnel. It provides similar functionality and features as traditional IPsec clients. As with clientless access, no provisioning on the client machine is required. The AnyConnect client is pushed from the Cisco IOS SSL VPN gateway to the client where it is installed and a secure tunnel is established. Initial installation requires admin rights, but upgrading an existing install does not.

AnyConnect supports 32-bit Microsoft Windows 2000, Windows XP, Windows Vista (64-bit platforms to follow as well as Windows Mobile 5), Mac, and Linux platforms.

Figure 47. Cisco IOS Software Support for AnyConnect VPN Client

Benefits

- **Increased Functionality and Flexibility:** The Cisco AnyConnect VPN Client provides a secure remote access alternative for non-Web based traffic. It compliments clientless operations, allowing for traditional IPsec like connectivity between clients and the secure Cisco IOS Software gateway.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

5.1.5) Reverse Route Injection Distance Metric Enhancements

Reverse Route Injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. The RRI Distance Metric Enhancement defines a distance metric for each static route created by RRI.

RRI is supported on both ipsec-profile and crypto map configuration (CLI) profiles:

- Configuration example on crypto map:

```
crypto map mymap 1 ipsec-isakmp
   set reverse-route distance 20
```

- Configuration example on ipsec-profiles:

```
crypto ipsec profile myprof
   set reverse-route distance 20
```

Benefits

- **Increased Flexibility:** Improves RRI flexibility when used in dynamic routing scenarios. Static routes can be tailored so dynamic routes can have priority in the routing table.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

5.2) Routing and Multicast

5.2.1) OSPF Mechanism to Exclude Connected Prefixes

By default, when an OSPF router is connected to other OSPF routers via an IP numbered link, it automatically includes prefixes of IP numbered links in its advertisements. The OSPF Mechanism to Exclude Connected Prefixes feature enhancement provides the ability to exclude directly connected prefixes from advertising throughout the network.

When this feature is configured, IP numbered link prefixes will not be advertised into the network, resulting in improved convergence times and enhanced security by excluding internal network prefixes from being exposed outside of the network.

Key Benefits:

- **Improved convergence, scalability and performance:** By excluding prefixes in OSPF advertisements, the network will converge faster, scale better. Performance of routers is improved by dealing with less number of prefixes in a network.
- **Improved security:** By not advertising connected prefixes, OSPF area border routers or autonomous system border routers will not be able to advertise these prefixes outside of the network. This improves the security of the network by not advertising connected prefixes to external entities.

Hardware

Routers	• Cisco 7200 Series Routers

Product Management Contact: Suresh Katukam (skatukam@cisco.com)

5.2.2) Optimized Edge Routing (OER) Application Aware Routing

Previously Optimized Edge Routing (OER) allowed users to optimize traffic based upon IP Prefixes, DSCP values, and Access Control Lists (ACLs). This feature allows OER the ability to optimize well known applications without having to configure ACLs to classify the traffic. Application optimization can be divided into three important tasks; application detection (learning), application performance measurement, and application route control. With this feature, you can specify an application by name for learning, performance measurement and route optimization.

Table 7 is a list of some of the applications that can be defined in OER policies for performance routing:

Table 14. Application List for OER Application Aware Routing

Application Name	Protocol	Port Number
CU-SeeMe-Server	TCP UDP	7648 7649 7648 7649 24032
DHCP-Server	UDP/TCP	67
DHCP-Client	UDP/TCP	68
DNS	UDP/TCP	53
FINGER-Server	TCP	79
GOPHER-Server	TCP/UDP	70
HTTPSSL-Server	TCP	443
HTTP	TCP/UDP	80
IMAP-Server	TCP/UDP	143 220
SIMAP-Server	TCP/UDP	585 993(preferred)
IRC-Server	TCP/UDP	194
SIRC	TCP/UDP	994
KERBEROS-Server	TCP/UDP	88 749
L2TP-Sever	UDP	1701
LDAP-Server	TCP/UDP	389
SLDAP-Server	TCP/UDP	636
MSSQL-Server	TCP	1433
NETBIOS-Server	UDP TCP	137 138 137 139
NFS-Server	TCP/UDP	2049
NNTP-Server	TCP/UDP	119
SNNTP-Server	TCP/UDP	563
NOTES-Server	TCP/UDP	1352
NTP-Server	TCP/UDP	123
PCanywhere-Server	UDP TCP	22 5632 65301 5631
POP3-Server	TCP/UDP	110
SPOP3-Server	TCP/UDP	995
PPTP-Server	TCP	1723
SMTP-Sever	TCP	25

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7200, and 7500 Series Routers

Product Management Contact: Scott Van de Houten (svandeho@cisco.com)

5.2.3) OER Link Grouping

OER automates routing in order to select the best path based upon cost minimization, load distribution policy, and overall network performance. This enables intelligent network traffic load distribution and dynamic failure detection of data-paths at the WAN edge (for multi-homing to the Internet or intranet connectivity). OER is unique in that it can make adaptive and dynamic routing

adjustments based on criteria other than static routing metrics: response time, packet loss, jitter, MOS scores, path availability, traffic load distribution, and financial cost minimization policies.

OER Link Grouping allows one or more interfaces on the border router to be assigned to a link group. By assigning interfaces to a link group, applications can be directed to only traverse interfaces within a link group. Policies are used to select an exit interface from a given link group. Fallback link groups can be used by the Policy if no interface within a link group is available or meets the policy requirements.

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7200, and 7500 Series Routers

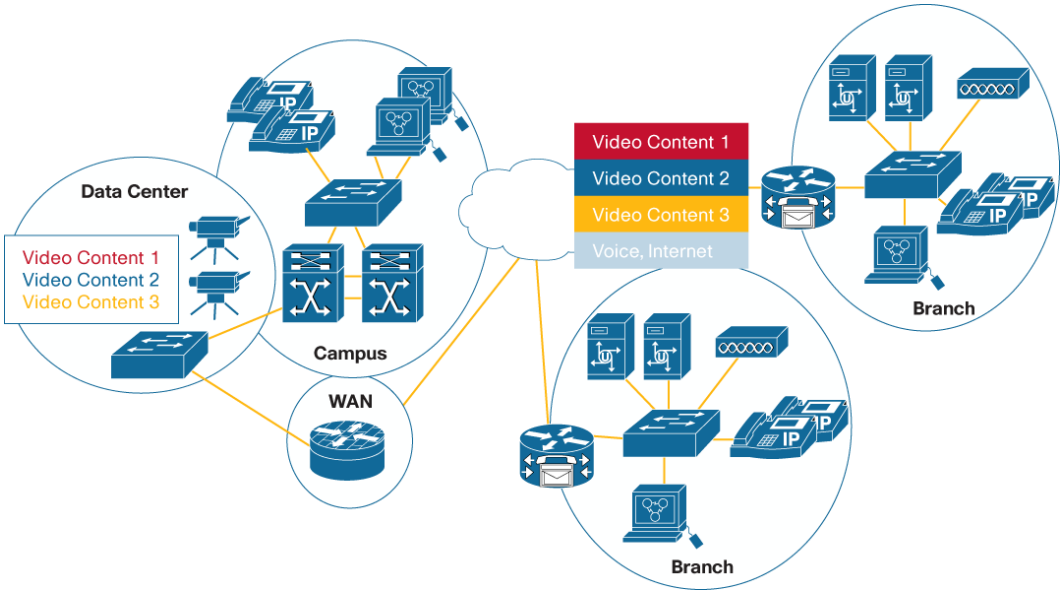
Product Management Contact: Scott Van de Houten (svandeho@cisco.com)

5.2.4) Bandwidth Call Admission Control (CAC) for IP Multicast

In multicast enabled networks, monitoring and controlling the amount of bandwidth utilized is critical for service efficiency. In corporate communications or IP video environments, it is important that the network link is not oversubscribed or video services might degrade for a set of users. Cisco understands this problem and has implemented a method to control and monitor the total bandwidth consumed at the network edge. In today's networks voice, video and data need to be allocated respective bandwidth and bandwidth based CAC allows seamless integration of video services.

The Bandwidth Based Call Admission Control (CAC) for IP Multicast feature allows the monitoring of bandwidth per set of multicast groups per interface in the network. Bandwidth based CAC has the ability to control how much bandwidth various content providers can use across a network by assigning specific multicast groups allowable bandwidth consumption.

Figure 48. Bandwidth Based Call Admission Control (CAC) for IP Multicast—Details



Benefits

- Enhances video services by monitoring video bandwidth consumption on the edge
- Provides guaranteed control of multicast based total bandwidth usage per interface

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2600XM, 2800, 3600, 3700, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/multicast

Product Management Contact: Scott Van de Houten (svandeho@cisco.com)

5.3) IP Services

5.3.1) Gateway Load Balancing Protocol (GLBP) Client Cache

Gateway Load Balancing Protocol (GLBP) protects data traffic from a failed router or circuit, while allowing packet load sharing between a group of redundant routers. GLBP differentiates itself from Virtual Router Redundancy Protocol (VRRP) in that GLBP offers the ability to concurrently use more than one gateway, significantly reducing the cost of a First Hop Routing solution.

GLBP is enhanced with the ability to display more information about individual network clients that are using GLBP as their default gateway. This makes it easier to understand:

- How well GLBP clients have been distributed among forwarders
- Which forwarder a particular client is assigned to
- How many clients are assigned to each forwarder
- Which clients are assigned to each forwarder

To achieve the above mentioned benefits, the following data is provided through a Cisco IOS CLI “show command” on the Active Virtual Gateway for the group:

- Percentage of all clients currently assigned to each forwarder
- Forwarder assigned to a specified client MAC address
- Number of clients assigned to each forwarder
- Information about each client assigned to each forwarder

Benefits

- Manageability and network troubleshooting of GLBP is greatly improved

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fb97.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

5.3.2) Dynamic Host Configuration Protocol (DHCP) Server Multiple Subnet

The Dynamic Host Configuration Protocol (DHCP) server now supports the configuration of multiple subnets under a single pool name. This enables large deployments where common DHCP parameters configuration can be grouped under a single pool, while subnet specific parameters can be set as well.

Benefits

- DHCP configuration is made easier and the number of pools to configure is kept to a minimum

Hardware

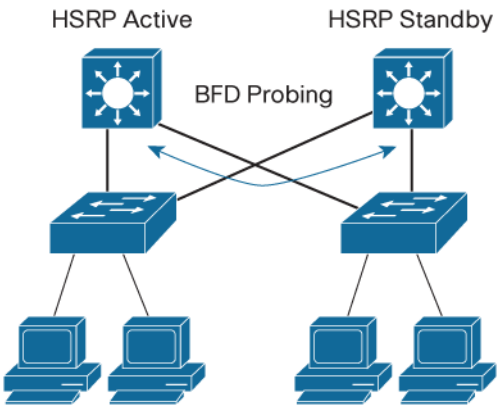
Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804419eb.html - wp1084769

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

5.3.3) Hot Standby Routing Protocol (HSRP) Bidirectional Forwarding Detection (BFD) Peering
Bidirectional Forwarding Detection (BFD) is introduced in the Hot Standby Routing Protocol (HSRP) group member health monitoring system. Previously, group member monitoring relied exclusively on HSRP multicast messages. These messages are relatively large, hence CPU consuming to produce and check. In architectures where a single interface hosts hundreds of groups there is a need for a lighter protocol. BFD addresses this issue and offers sub-second health monitoring at a relatively low CPU impact.

Figure 49. HSRP BFD Peering Topology



Benefits

- Allows for quicker and more efficient failure detection of HSRP group member

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

5.3.4) DHCPv6 Stateless Enhancements

Stateless DHCPv6 is enhanced to support new options in the Client and the Server component. Cisco IOS Release 12.4(15)T adds support for new DHCPv6 options for configuration of the DHCP Server:

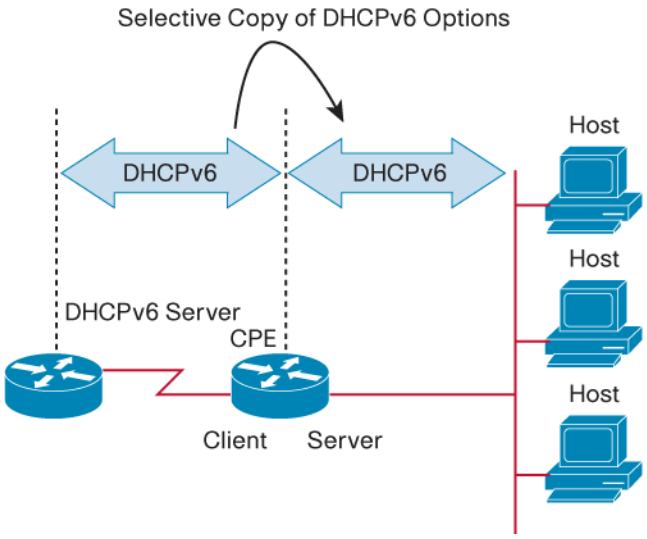
- NIS SERVERS
- NISP SERVERS
- NIS DOMAIN_NAME
- NISP DOMAIN_NAME
- SNTP SERVERS
- INFORMATION REFRESH TIME

Special attention must be paid to “INFORMATION REFRESH TIME” as it provides the end-host the capability to regularly refresh the content of stateless options that don’t carry a lease time with them.

The above mentioned options are requested by the DHCPv6 Client and INFORMATION REFRESH TIME is taken into account to refresh the content on stateless DHCP options received by the Client.

In scenarios where a router is a DHCPv6 client toward its upstream router and a DHCPv6 Server toward downstream hosts, it is now possible to import received options from the Client side to automatically populate the DHCPv6 Server configuration with those options. The choice of imported options is set on a pool basis.

Figure 50. Hierarchical Stateless DHCPv6



Benefits

- DHCPv6 Stateless parameters are regularly renewed
- DHCPv6 Server configuration on CPE is made more dynamic

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200,and 7301 Series Routers

Additional Information:
http://www/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00806f542d.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

5.4) High Availability

5.4.1) Bidirectional Forward Detection (BFD) Support for Cisco Integrated Services Routers
BFD is a detection protocol that is designed to provide fast forwarding path failure detection times for all media types.

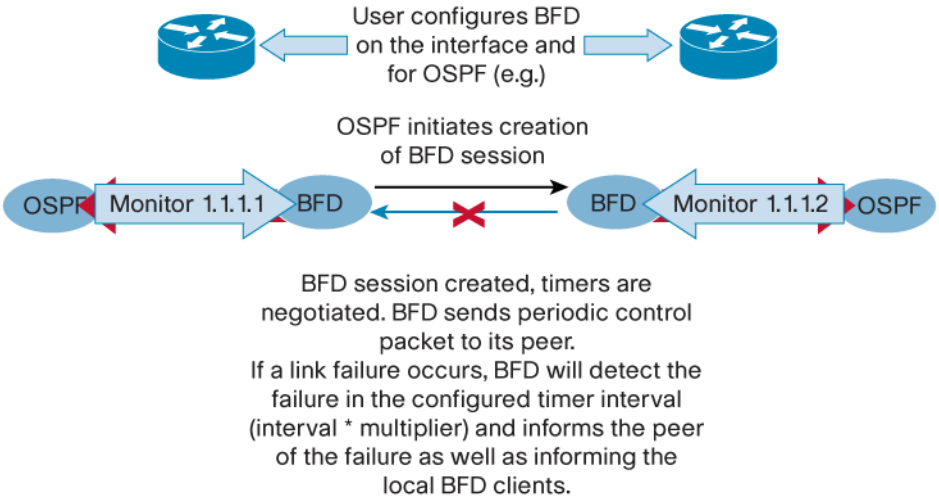
The convergence of business-critical applications onto a common IP infrastructure in Enterprise and Service Provider networks is becoming more common. Given the criticality of the data, these networks are typically constructed with a high degree of redundancy. While such redundancy is desirable to increase network availability, its effectiveness is dependant upon the ability of individual network devices to quickly detect failures and reroute traffic to an alternate path.

Routing protocol convergence is a key issue in these converged network designs since it determines the routes available to send data packets on and the reachability of the network. In order to maintain the integrity of routing data, it is vital to have accurate information regarding the status of links and whether they are up or down. Bidirectional Forwarding Detection (BFD) is an IETF draft based mechanism used to detect link failures for routing protocols. It addresses some of the important problems in link status detection:

- Link Layer detection mechanisms vary significantly in the temporal resolution they offer for link status detection. Techniques like Automatic Protection Switching (APS) on SONET offer sub-50 ms resolution for the detection of link failures while Ethernet or traditional WAN link methods offer a few seconds of resolution at best.
- Link Layer detection mechanism may not help with Layer 3 Network level failures. This is important when there is a routing flap in the routing protocol at Layer 3 but the underlying Layer 2 Link is fine.
- Typical mechanisms that work at Layer 3 offer 15-20 seconds of temporal resolution for failure detection times. This is slow in terms of times which applications require for network connectivity to be maintained.

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD delivers fast router peer failure detection times independent of all media types, encapsulations, topologies, and routing protocols including EIGRP, IS-IS, OSPF, and BGP (single-hop peers over Ethernet interfaces). Cisco currently supports the BFD Asynchronous mode, which depends on the sending of BFD control packets between two systems for liveness detection between the forwarding engines of the BFD neighbors.

Figure 51. Bidirectional Forward Detection (BFD) Support for Cisco Integrated Services Routers



Benefits

- Facilitates faster network convergence due to faster failure detection of link/neighbor
- Allows for media independent link-failure detection
- Enables easier network profiling and planning

Considerations

- Cisco IOS Software Release 12.4(15)T supports BFD for EIGRP, OSPF, ISIS, and BGP single-hop peers over Ethernet interfaces only.
- BFD is not supported over OSPF virtual links or sham links, as the current specification for BFD usage on IP links limits BFD to one-hop adjacencies.
- Care should be taken while configuring BFD timers. Consider CPU utilization, link speed, and speed of light constraints before setting low values.
- BFD is not intended for use as a protocol to detect Cyclic Redundancy Check (CRC) errors or packet loss between two adjacent routers.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800 Series Routers

Product Management Contact: Harmen Van Der Linde (havander@cisco.com)

5.5) Connectivity

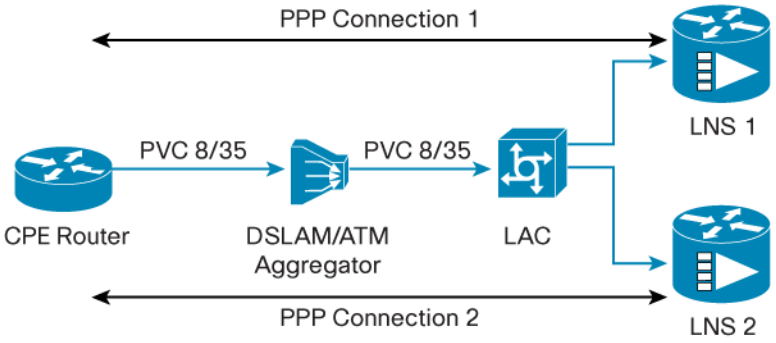
5.5.1) Multiple PPP-over-Ethernet (PPPoE) Clients per VC Support

The Multiple PPPoE Client feature is an enhancement over the existing PPPoE client support for ATM Virtual Circuits. Previously, an ATM PVC could only be configured with one PPPoE dialer interface. Now, multiple Dialer interfaces may be configured on a single Virtual Circuit (VC). This can be used to configure redundancy to multiple L2TP Network Servers (LNS's), providing an easy backup path, should the primary LNS stop responding. This capability is especially useful in situations where only one PVC can be configured between Customer Premises Equipment (CPE) and the Asynchronous Transfer Mode (ATM) aggregator.

Key **Benefits** for using Multiple PPPoE Clients per VC include:

- Increased flexibility in defining PPPoE Dialer Interfaces
- Provide multiple services to a CPE using separate logical PPP interfaces across the same VC
- Improved availability using a single VC

Figure 52. Multiple PPPoE Clients



Hardware

Routers	• Cisco 800, 1800, 2800, 3800 Series Routers

Product Management Contact: Ben Strickland (bstrickl@cisco.com)

5.5.2) Layer 2 Tunneling Protocol (L2TP) Forwarding of PPPoE Tags

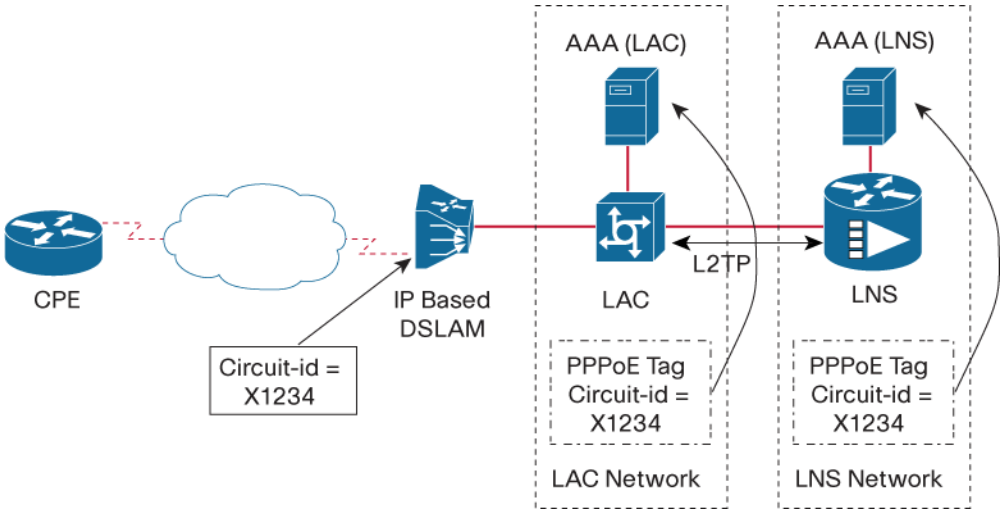
In an Ethernet access aggregation network, there are no unique mappings between subscriber line ID and Ethernet interface like the Virtual Circuit (VC) in an ATM based network, especially when a separate Virtual LAN (VLAN) per subscriber is not used. DSL Forum TR-101 proposed a method by which the Digital Subscriber Line Access Multiplexer (DSLAM) sends a DSL Remote-ID and circuit-id in the discovery phase. By obtaining this information, future subscriber decisions can be made at later points during the call set-up phase. However, before this feature was introduced, the implementation did not extend to the LNS in a VPDN environment. This feature allows for the PPPoE tag information containing the DSL-Forum attributes to be forwarded from the L2TP Access Concentrator (LAC) to the LNS.

The DSLAM port information contained within the PPPoE tags can be used by the local Authentication, Authorization, and Accounting (AAA) servers on the LNS in addition to the LAC. This is especially useful in wholesale environments where the LAC and LNS may belong to different owners.

Key benefit for using Multiple L2TP Forwarding of PPPoE Tags:

- Increased LNS security by being able to authenticate users based on DSLAM port information

Figure 53. Forwarding the DSLAM Circuit-id over L2TP



Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200 Series Routers

Product Management Contact: Ben Strickland (bstrickl@cisco.com)

5.6) Management, Instrumentation, and User Interface

5.6.1) Cisco IOS Auto-Upgrade Manager

Cisco IOS Auto-Upgrade Manager simplifies the Cisco IOS Software upgrade process by providing a simple interface to specify, download, and upgrade (or downgrade) to a new Cisco IOS Software image. Cisco IOS Auto-Upgrade Manager includes CLI-based management of automatic software downloads and upgrades, including:

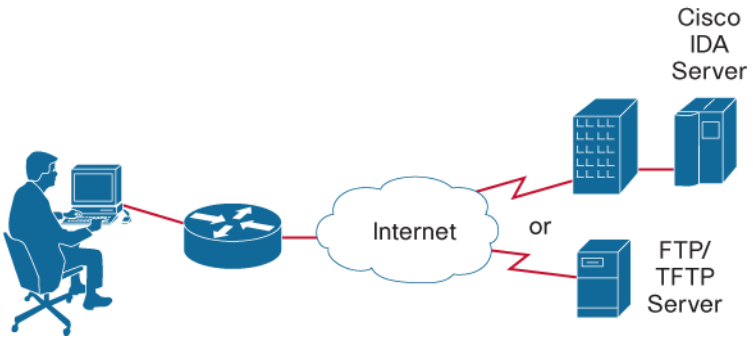
- Locating and downloading the new Cisco IOS Software image
- Checking memory requirements
- Managing secondary storage
- Validating the image
- Scheduling a Warm-Upgrade
- Providing roll-back support on failure

New software images can be automatically downloaded from Cisco with a valid Cisco.com login via SSL, or any other Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) server in the user's network or elsewhere that contains the desired software image. The software upgrade is scheduled either immediately or at a convenient future time using a "Warm-Upgrade" to minimize down time.

Automatic notifications can include a status email sent upon completion of successful warm upgrade or failure and roll-back, error messages indicating any incompatible CLI statements, and should the upgrade fail for any reason, error messages are generated and sent to the console and syslog buffers.

Cisco IOS Auto-Upgrade Manager can be invoked with either an interactive dialog that will walk a novice user through the upgrade process and options, or a single line CLI User Interface for more experienced users.

Figure 54. Cisco IOS Auto-Upgrade Manager Simplifies Cisco IOS Software Upgrades



Benefits

- Makes upgrading Cisco IOS Software easier for less experienced staff and easier to walk through with telephone support
- Reduced time to upgrade Cisco IOS Software
- Lower Total Cost of Ownership (TCO) of Cisco routers with single provisioning method for access and work group products

Hardware

Routers	• Cisco 1800, 2800, 3800 Series Routers

Product Management Contact: Tom Cramer (tcramer@cisco.com)

5.6.2) Cisco IOS Embedded Resource Manager

The Embedded Resource Manager (ERM) feature provides a method to monitor internal system resource utilization. Finite resources such as buffer, memory, and processor utilization are monitored.

ERM works by monitoring resource utilization from the perspective of resource owners and resources users. These owners and users are various subsystems within Cisco IOS Software. Network administrators can define thresholds to create notifications according to the real-time resource consumption.

The ERM infrastructure is designed to be extensible and to allow for very granular monitoring on an IOS task basis. It goes beyond simply monitoring for total CPU utilization for example. Through the use of ERM, network administrators and operators can gain a better understanding of the device's operational characteristics leading to better insight into system scalability and improved system availability.

Features and Benefits

The Embedded Resource Manager (ERM) infrastructure tracks resource utilization, depletion and resource dependencies across processes and within a system. ERM represents a framework for monitoring any finite resource within the software. Support for monitoring CPU, buffer, and memory

utilization at the global or task level is available today. The ERM framework is extensible and will be further enhanced to provide more function in future software releases.

The ERM framework provides a mechanism to send notifications whenever the specified threshold values are violated by any Resource User (RU). This notification helps in diagnosing any CPU, buffer, and memory utilization issues.

The Embedded Resource Manager feature allows you to:

- Monitor system resource usage to better understand scalability
- Set resource thresholds at a granular level
- Generate alerts when resource utilization reaches specified levels
- Generate internal events using the Cisco IOS Embedded Event Manager feature and take local automated action
- Gain a better understanding of how network changes might impact system operation

Resource Accounting and Thresholds

ERM tracks the resource usage and allocation for each Resource User (RU) internally. A RU is a subsystem or process task within the Cisco IOS Software. As an example, the OSPF hello process is a resource user. Threshold limits are used to notify network operations of specific conditions. The ERM infrastructure provides a means to notify the internal RU subsystem of threshold indications as well. The resource accounting is performed by individual Resource Owners (ROs). ROs are part of the Cisco IOS Software responsible for certain resources such as the memory manager. When the utilization for each of the RUs crosses the threshold value you have set, the ROs send internal notifications to the RUs and to network administrators in the form of Syslog messages or SNMP alerts.

You can set rising and falling values for critical, major, and minor levels of thresholds. When the resource utilization crosses the rising threshold level, an Up notification is sent. When the resource utilization falls below the falling threshold level, a Down notification is sent.

ERM provides for three types of thresholds to be defined:

- System Global Threshold—Used when the entire resource reaches a specified value; sent to all RUs
- User Local Threshold—Used when a specified RUs utilization exceeds the configured limit
- User Global Threshold—Used when the entire resource reaches a configured value; sent only to the specified RU

Table 15. ERM Features and **Benefits**

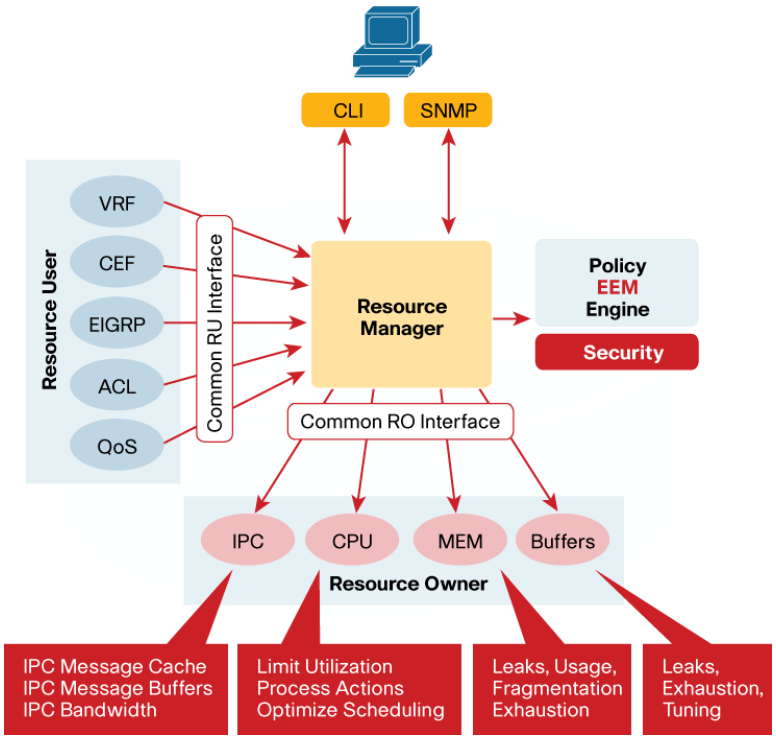
Feature	Benefit
System Monitoring and Management	
Flexible facility for monitoring finite resources	ERM provides a common facility for monitoring various finite resources within the system. CPU, buffer, and memory resources are monitored.
Embedded within Cisco IOS Software	ERM is part of the Cisco IOS Software infrastructure.
Granular, per subsystem statistics	ERM accounts for resource utilization on both a system level as well as on a per subsystem task level.
User defined thresholds	Network administrators can set the thresholds for specific conditions.
Multiple threshold levels	You can set rising and falling threshold values for minor, major, and critical levels of resource utilization for buffer, CPU, and memory ROs.

Feature	Benefit
Extended Statistics and Information	
Loadometer process	The loadometer process generates an extended load monitor report every 5 seconds. The loadometer function, which calculates process CPU usage percentages, is enhanced to generate the loadometer process reports.
Snapshot Management using event trace	Snapshot management manages the buffer where snapshots of reports are stored. The snapshot management infrastructure stores, displays, and releases the snapshots.
Automatic CPUHOG profiling	Troubleshooting data is collected automatically by the system to aid in problem resolution. The timer ISR starts profiling a process when it notices that the process has taken more than the configured value or a default of 2x (maximum scheduling quantum).
Improved memory statistics	Embedded Resource Manager enhances the memory manager in Cisco IOS Software to include memory usage history and memory accounting
Improved buffer management	Embedded Resource Manager addresses the most frequently faced problems to the Buffer Manager. They are: buffer manager tuning, buffer leak detection, buffer accounting and buffer usage thresholds.
Cisco IOS Feature Integration	
EEM integration	ERM is integrated with Cisco IOS Embedded Event Manager (EEM). ERM threshold violations are detected by the ERM Event Detector and can be used to trigger automated actions.
Additional Management Interfaces	
Embedded Resource Manager MIB	ERM SNMP support is added beginning with Cisco IOS Software version 12.4(15)T and 12.2(33)SRB. The ERM MIB will be available on Cisco.com Visit: http://www.cisco.com/public/sw-center/sw-netmgmt.shtml

Product Architecture

ERM is a feature within the Cisco IOS Software infrastructure. The ERM framework and architecture defines components in terms of Resource Owners (ROs) and Resource Users (RUs). An ERM Resource Manager (RM) component is also part of the infrastructure. ROs account for utilization by the resource users. The RM provides control and notification functions.

Figure 55. Cisco IOS Embedded Resource Manager Architecture



Hardware

Routers	• Cisco Integrated Services Routers, Cisco 7200 Series Routers

System Requirements

The ERM software subsystem does not consume any significant amount of resources.

Additional Information:

For more information about the Cisco IOS Embedded Resource Manager, visit http://www.cisco.com/public/support/tac/documentation.html and browse the appropriate Cisco IOS Software documentation.

Product Management Contact: Rick Williams (rwill@cisco.com)

5.6.3) Toolkit Command Language (TCL) Signing

Toolkit Command Language (TCL) was first introduced in Cisco IOS Software in 1994. Many components of Cisco IOS Software like EEM, ESM and IVR use TCL scripts. Signing of TCL scripts enables customers to execute only authenticated and approved scripts on the Cisco devices. It provides a mechanism for the customers to verify the source of the TCL scripts.

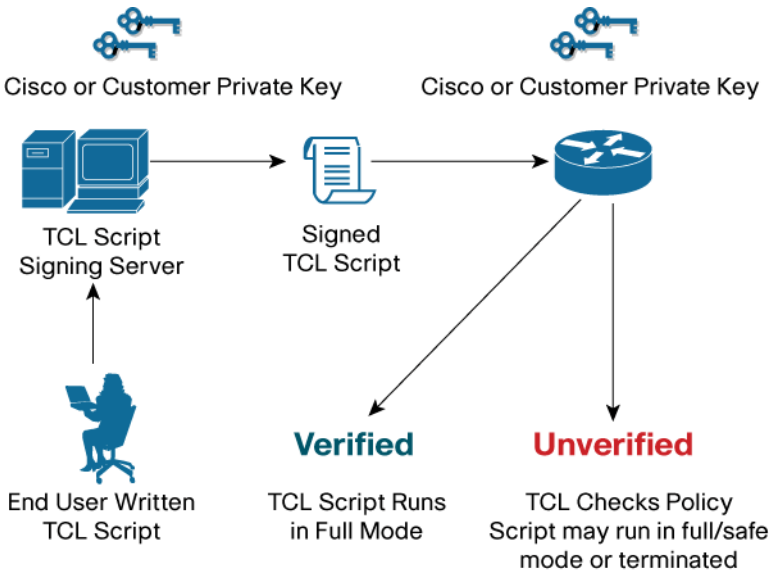
TCL is an interpreted language and scripts written in TCL do not have to be compiled before execution. TCL scripts can be created and modified dynamically. TCL provides a fundamental command set which can be expanded by adding “extensions” to the language to perform specific operations. As a result TCL is highly portable and extensible. It is used for rapid prototyping, scripted applications and testing.

Cisco is now innovating TCL scripts to a new level by introducing state of the art, reliable and web based “Signing Tool” application to verify the authenticity.

Key advantages to using the TCL Signing Tool include:

- Ability to configure safe and secure modes for execution
- Enhanced security (safe and whole modes) within security mode
- Allow various formats of TCL scripts—clear, signed with PKCS7, signed with PKCS and signature appended
- API to verify the signatures if customers customize the scripts
- Only trusted scripts to be executed in whole mode; all other scripts to be executed in safe mode
- Private keys stored in secure Hardware Security Module

Figure 56. Verification of Signed TCL Scripts Process



Hardware

Routers	• Cisco 800, 1700, 2600, 3600, 3700, 7200, 7301 Series Routers

Additional Information: http://forums.cisco.com/eforum/servlet/EEM?page=main

Product Management Contact: Madhu Vulpala (mulpala@cisco.com)

5.7) Mobility and Wireless

5.7.1) Mobile Ad Hoc Networking (MANET) Networking Enhancements for Router Radio Links
Cisco Mobile Ad Hoc Networking (MANET) enhancements address several of the issues faced when merging IP routing and mobile radio communications in ad hoc networking applications. In a MANET, highly mobile “nodes” communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network router, with the two devices interconnected via Ethernet. Key challenges in a MANET environment include:

- Convergence: Since nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET becomes a challenge because a node’s state can change well before the event is detected by the routing protocol’s normal timing mechanisms.
- Route Selection: Radio link quality in a MANET can vary dramatically due to a variety of factors such as noise, fading, interference, and power fluctuation. As a result, routers need the ability to factor these fluctuations into “best path” selection.
- Radios have limited buffering capabilities, and could be easily over-loaded with IP traffic.
- Directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multi-hop, multipoint router environments, as it increases the size of each router’s topology database and reduces routing efficiency when mobile nodes join and leave the network, based on neighbor up/down signaling from the radio.

This feature enables a Cisco router to use Layer 2 feedback from its partner radio to optimize Layer 3 processing. Intra-nodal communications between router and radio are supported by means of

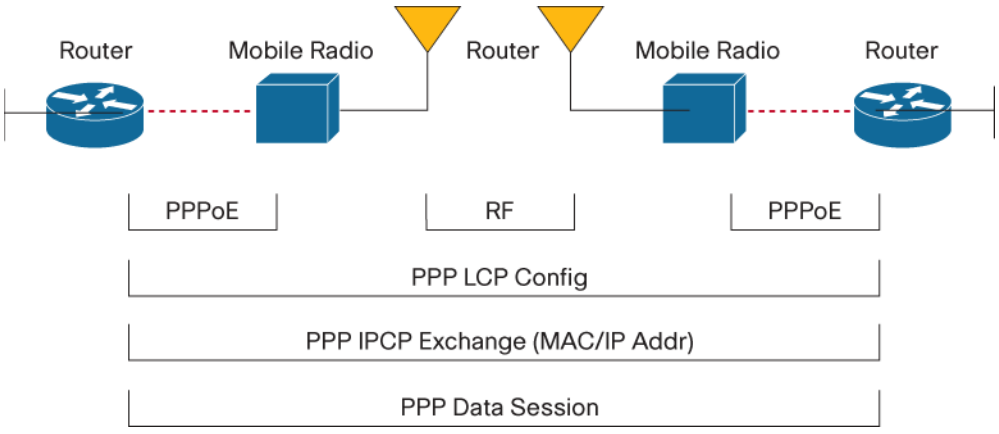
PPP-over-Ethernet (PPPoE) sessions. A PPPoE session is established between router and its partner radio on behalf of every other router/radio neighbor located in the MANET. Once the PPPoE sessions are established, a PPP session is established end to end. These Layer 2 sessions are the means by which radio network status gets reported to the router's Layer 3 processes. The Cisco IOS MANET enhancements provide several new capabilities for optimizing routing in a wireless, ad hoc environment:

- **Neighbor Up/Down Signaling:** Enables Cisco routers to provide faster network convergence by reacting to link status signals generated by the radio, rather than waiting for protocol times to expire. The routing protocols (OSPFv3 or EIGRP) respond immediately to these link status signals by expediting adjacency formation or tear-down.
- **Link Quality Metrics Reporting:** The PPPoE protocol has been extended to enable a radio to report link quality metric information to a router. Cisco routers have been enhanced so that OSPFv3 or EIGRP routing protocols can factor link quality metrics into route cost calculations.
- **PPPoE Credit-Based Flow Control:** This PPPoE extension allows the radio to control the rate at which the router can transmit data for each PPPoE session, so that the need for queuing in the radio is minimized.
- **Virtual Multipoint Interface:** Aggregates per-neighbor PPPoE sessions and maps these to appear as a single point-to-multipoint, multi-access, broadcast-capable network.

The Cisco IOS MANET enhancements provide the following critical advantages:

- Faster convergence when nodes join and leave the network
- Optimal route selection based on Layer 2 feedback from the radio network
- Flow-controlled communications between the radio and its partner router
- Efficient integration of point-to-point, directional radio topologies with multi-hop routing

Figure 57. MANET Enhancements for Router-Radio Links



Benefits

- Enables network-based applications and information to be delivered reliably and quickly over directional radio links
- Faster convergence and optimal route selection ensure that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queuing/buffering; also provides consistent Quality of Service (QoS) for networks with multiple radios

Hardware

Routers	• Cisco 2800, 3200, and 3800 Series Routers

Product Management Contact: Rex Craig (recraig@cisco.com)

5.7.2) Access Point Link Role Flexibility

Access Point Link Role Flexibility allows access point radios to operate in a combination of radio roles, such as access point root, bridge root (with or without clients), bridge nonroot (with or without clients). This provides a more flexible deployment scheme to support the various applications requirement. Please note that the Cisco Integrated Services Router (ISR) Access Point (AP) does not support access point repeater and Work Group Bridges (WGB).

There are thirteen new Access Point Link Role Flexibility features being introduced in Release 12.4(15)T:

1. Advanced Encryption Standard (AES)—CCMP

This feature supports Wi-Fi Protected Access (WPA2) which is the Wi-Fi Alliance specification for interoperable wireless LAN security that supports IEEE 802.11i authentication and AES-CCMP encryption.

2. Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an authentication protocol for the 802.1X framework for mutual authentication between the client and a RADIUS server. New EAP authentication types supported in this Cisco IOS Software release include EAP-TTLS, EAP-MD5, and EAP-SIM.

3. IEEE 802.1X Local Authentication Service for EAP-FAST

This feature allows an IEEE 802.1X enabled RADIUS Server supporting EAP-FAST authentication types to run on Cisco IOS Software, thereby allowing the access point to authenticate wireless clients when the WAN link is down or the RADIUS Server at the central site is not available.

4. Microsoft WPS IE SSIDL

SSIDL Information Element support.

5. Multiple Basic Service Set ID (BSSID)

This feature permits a single AP to appear to the WLAN as multiple virtual APs. It does this by assigning an AP with multiple Basic Service Set IDs (BSSIDs) or MAC address. The AP is able to use a different BSSID to advertise each SSID and is therefore able to appear to WLAN clients as if there are multiple physical APs. Each BSSID/SSID combination advertised by the AP is able to be configured to support encrypted or unencrypted traffic.

6. NAC—L2 IEEE 802.1x

Network Admission Control (NAC) L2 IEEE 802.1x extends NAC support to layer 2 switches and wireless access points. Combining it with 802.1x provides a unified authentication and posture validation mechanism at the layer 2 network edge. This helps protect the network from attack by machines with insufficient antivirus posture. Performing posture validation at the edge maximizes the portion of the network which is protected and allows posture validation to be performed within a VLAN.

7. Universal Client Mode

This feature allows the access point radio to act as a client to another Cisco or third-party access point. Please see caveats for known issues.

8. VLAN Assignment by Name

This feature provides the ability for the RADIUS server to assign an 802.11 client to a VLAN identified by NAME. Prior to the introduction of this feature, VLANs had to be identified by “VLAN_ID”.

9. Wi-Fi Multimedia (WMM) Required Elements

This feature supports WMM which is the Wi-Fi Alliance specification for QoS.

10. Wireless Non-Root Bridge

The wireless non-root bridge allows the access point radio to operate as the remote node in a point to point or point to multi-point network. Please see caveats for information on antenna support.

11. Wireless Root Bridge

The wireless root bridge role provides support for both point-to-point or point to multi-point bridging. Access point radio operating in universal client mode can only pass traffic across the network via a native VLAN. A workaround for this is to use the native VLAN to associate the client or if this is a Cisco access point that the client is associated to, upgrade the access point Cisco IOS Software image to Release 12.3(11)JA. See DDTS CSCsg58791 for more information.

12. Wireless Root and Non-root Bridging Antenna Support

The following antennas are certified by Cisco for the European Telecommunications Standards Institute (ETSI) and TUV Japan regulatory domains to be used with a low loss extension cable for the 2.4GHz radio in the Cisco HWIC-AP-AG(G)-E, HWIC-AP-G-J, and HWIC-AP-AG-P Access Points when its operating in Wireless Bridge mode:

- AIR-ANT2506
- AIR-ANT24120
- AIR-ANT2414S-R
- AIR-ANT1949
- AIR-ANT3338

For more information, see “Declarations of Conformity and Regulatory Information for Cisco Access Products with 802.11a/b/g and 802.11b/g Radios”. Please note that these antennas have not been certified by Cisco for use in the United States under Federal Communications Commission (FCC)

regulations. Additionally, no high-gain bridging antennas have been certified by Cisco for the 5GHz radio in the HWIC-AP-AG-x (all models and regulatory domains).

13. Security Device Manager Support

Wireless LAN features in Cisco Integrated Services Routers are configured through Cisco Command Line Interface (CLI) or through the Cisco Router and Security Device Manager (Cisco SDM) Graphical User Interface (GUI). However, current routers that upgrade to Cisco IOS Software Release 12.4(15)T (and later) for new wireless features, as well as newly introduced router models that require Release 12.4(15)T must initially use Cisco CLI for WLAN configuration. Cisco router models using Release 12.4(15)T (and later) can gain WLAN support through Cisco SDM when subsequent Cisco SDM versions are released.

Hardware

Routers	• Cisco 800, 1800, 2800, and 3800 Series Routers

Product Management Contact: Marc Bresniker (mbresnik@cisco.com)

5.7.3) IP Pool Address Holdback Timer
The IP Pool Address Holdback Timer feature is an enhancement over the existing mechanisms for IP address allocation using the local IP pools. Previously, an IP address assigned to a subscriber through local IP pools could be immediately reassigned to a new subscriber once it was released. In all-IP networks, where a subscriber's identity is tied to its IP address, this can cause inconsistency in the backend systems as it takes some time before the cached relationships between IP address and subscriber identity at these systems are flushed out. Now, a holdback timer may be configured for local IP pools to specify a time before which an IP address that is released will not be reassigned to a new subscriber, eliminating the inconsistencies of overlapped identities in the backend systems. This capability is especially useful in mobile networks like GGSN where frequent recycling of IP addresses causes the problem mentioned above to be more likely.

Key Benefit for Using IP Pool Address Holdback Timer Include:

- Increased reliability and accuracy in accounting by preventing overlapped identities in the backend systems.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200 Series Routers

Product Management Contact: Ben Strickland, (bstrickl@cisco.com)

5.8) Voice

5.8.1) Communications Manager Express (CME) 4.1 Voice Features
Cisco IOS Release 12.4(15)T contains several new features for customers using Communications Manager Express call processing:

1. Ad Hoc Conferencing for 8 party

The Cisco Unified CallManager Express 4.1 Multi-party Conferencing Enhancement adds Digital Signal Processor (DSP)-based ad hoc conferencing to Cisco Unified CallManager Express systems. Ad hoc conferences are created when one party calls another party, then either party adds one or more parties to the conference call.

This DSP or hardware-based conferencing allows more parties and more functionality than software-based conferencing which only allows three parties in a conference.

Customers can choose the legacy software based 3 party ad hoc conference or the new DSP based hardware conferencing feature, but not both.

Dedicated DSP's need to be pre-configured for add hoc or Meet-Me conferencing, where the DSP channels of the DSP chip can not be configured for PSTN or analog port Termination nor transcoding.

Details on DSP's, and number of conferences support, please refer to this location on Cisco.com on the PVDM2 DSP modules:

http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet0900aecd8016e845.html

2. Meet-me Conferencing for 32 party

The Cisco Unified CallManager Express 4.1 Multi-party Conferencing Enhancement adds Digital Signal Processor (DSP)-based Meet-Me hoc conferencing to Cisco Unified CallManager Express systems. Meet-me conferences are first created by one user by pressing the Cisco Unified IP Phone Meet-Me softkey, then an available conference bridge is created and others join by dialing the designated conference number. This DSP or hardware-based conferencing allows more parties and more functionality than software-based conferencing which does not support Meet-Me conference.

This Meet-Me conferencing feature is a on demand type solution, it does not support reservations nor passwords for entry in to the conference.

Dedicated DSP's need to be pre-configured for add hoc or Meet-Me conferencing, where the DSP channels of the DSP chip can not be configured for PSTN or analog port Termination nor transcoding.

For more details on DSP's, and number of conferences support, please refer to this location on Cisco.com on the High-Density Packet Voice digital signal processor (DSP) Module (PVDM2):

http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet0900aecd8016e845.html

Common features supported with the new DSP hardware conferencing:

- Creator of conference can display conference all parties joined in conference on the Cisco Unified IP phone 7940G, 7941G, 7960G, 7961G, 7970G, and 7971G-GE
- Conference creator can drop one party from conference using softkeys during display of Conference List
- A tone can be configured to play as users join and leave the conference
- An feature access code can be configured to mute or unmute the line
- All SCCP based IP phones with displays and softkeys can create a ad hoc or Meet-Me conference. SIP based phones can join an existing conference
- The Cisco 7935/36 soundstation can not create a conference
- Analog phones using SCCP can join an existing conference

Requirements; Dedicated PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-62 on Integrated Service Routers motherboard or NM-HDV2 or NM-HD-2VE. DSP modules can be on another router.

For details on configuration, limitations, and type of phones supported for Ad Hoc and Meet-Me conferencing, refer to the Communications Manager Express admin guide; http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html

3. Support for New Cisco Unified IP Phones

This release includes support for these new Cisco Unified IP Phone models:

- Wireless IP Phone 7921G
- 7906G IP Phone
- 7931 Multi-button IP Phone
- 7985 Personal Video-telephony end point
- VTA 2.0 and Cisco IP Communicator interoperation on the same PC

4. Extension Assigner for Ease of New Site Deployments

Communications Manager Express Extension Assigner is a TCL based script that allows for resellers or larger retail customers to quickly deploy new sites without need to configure each Communications Manager Express site with individual IP Phone MAC address information. Now the installer can have a default configuration where phones, when connected to the system, will auto-register with a temporary extension number. Then the installer from the phone dials in to the password protected Extension Assigner and via audio prompts and the phone dial pad, tells the system the extension number the phone should be. The phone will then verify the extension number choice, and will reset the phone as this new extension number. Extension Assigner can also be used to replace broken phones without having to touch the configuration though CLI or GUI tools. Communications Manager Express Extension Assigner is available as a free download from Cisco.com Software Download Center.

5. Busy Lamp Field/Phone Status Display on Missed Calls Directory

Users with Cisco IP Phones using Signaling Connection Control Part (SCCP) loads can now display the phone status of other phones connected to the Communications Manager Express system when viewing missed directory calls.

6. SIP Phone Support for Newer Phones

Communications Manager Express 4.1 with this release now supports Session Initiation Protocol (SIP) loads on Cisco Unified IP Phones 7906G, 7911g, 7941G, 7961G, 7970G and 7971G-GE. Using SIP with CME delivers RFC3261 functionality. Customers can choose to use Cisco Unified IP phones using SIP or SCCP.

7. New SIP Phone Features

The following new features are supported when using Cisco Unified IP Phones using SIP loads:

- Corporate/system and personal speed dial
- Music on Hold (MoH)
- SIP Subscribe for line status for presence applications

8. SIP Based Trunking Features

This release includes two new SIP Trunking features for SMB or Enterprise customers.

- For customers using a SIP trunk from Service Providers, you can now disable refer/3xx messages during transfer and forward to allow the transfer to be handled by the Service Providers network.
- SIP based Message Waiting Indicator (MWI) messages can be passed through Q Signaling (Q.SIG) protocol to Time-Division Multiplexing (TDM) Private Branch Exchanges (PBX) and to voice mail.

Hardware

Routers	• Cisco 2800 and 3800 Series Integrated Services, UC500 Series Routers

Product Management Contact: Ron Lewis (ronlewis@cisco.com)

5.8.2) Survivable Remote Site Telephony 4.1 Voice Features
Cisco IOS Software Release 12.4(15)T contains new features for customers using Cisco Unified Survivable Remote Site Telephony (SRST) for backup call control with a centralized Communications Manager cluster:

1. SIP Phone Support for Newer Phones

Survivable Remote Site Telephony 4.1 with this release now supports SIP loads on Cisco Unified IP Phones 7906G, 7911g, 7941G, 7961G, 7970G and 7971G-GE. Customers should remember that during SRST mode, call features are based on RFC3261 functionality, and do not deliver the same number of features as available with Communications Manager or if using SCCP phone loads.

2. Key Pad Markup Language (KPML) and Dialplan on SIP Phones for Ease of Dialing

This release also offers the feature where information about the dial plan is stored on the SIP phones, allowing for easier user dialing during a WAN outage.

3. E911 Support

New with this release for SRST customers is the option to configure E911 features for use during a WAN outage. The E911 features include:

- Option to define unlimited number of Emergency Response Locations (ERL) for handling 911 calling party translation
- Each Emergency Response Location can have two (2) Emergency Location Identification Numbers (ELIN) for handling two calls at once from the ERL
- Phones registered to the SRST router during a WAN outage are assigned to a ERL by use of IP address subnets
- On an outbound call to 911 (or any defined emergency number) the IP Phone calling party number is changed to the ELIN to allow the Public Safety Answering Point to know the location of the caller
- Return calls from the Public Safety Answering Point to the IP Phone are routed back to the original 911 caller

- History of E911 calls placed can be viewed using Cisco IOS CLI Show command, or tracked via Radius Call Detail Record (CDR) collection
- Use of SRST E911 requires Primary Rate Interface (PRI) or Centralized Automated Message Accounting (CAMA) trunks

Features not supported include integration with Cisco Emergency Responder or tracking phones using Cisco Discovery Protocol or use with Communications Manager Express.

Hardware

Routers	• Cisco 2800 and 3800 Series Integrated Services Routers

Product Management Contact: Ron Lewis (ronlewis@cisco.com)

5.9) Hardware

5.9.1) Cisco 7201 Router

The Cisco 7201 Router is the latest generation of the Cisco 7200 Series Family. It is a compact, high performance Single Rack Unit (RU) router that uses the latest Cisco 7200VXR Network Processing Engine NPE-G2 coupled with a comprehensive range of interface options.

Figure 58. Cisco 7201 Router

The Cisco 7201 Router addresses the demand for the same performance enhancements, and Cisco IOS Software features of the latest Cisco 7200VXR NPE-G2 but in a smaller form-factor and with low power consumption. Cisco 7201 provides four built-in Gigabit Ethernet ports and one Port Adapter (PA) slot which makes it ideal for various Service Providers and Enterprise applications. It also offers redundant and field-replaceable AC and DC power supplies

With its combination of scalable performance, compact architecture, high density, and low price per port, the Cisco 7301 is ideally suited for a variety of key applications within both the Service Provider and Enterprise markets.

Key Applications for Enterprise deployments:

- **Large-branch-office router:** High-performance with features enabled branch-office router with support for up to OC-3/STM-1 or Gigabit Ethernet connectivity. It is ideal for Brach-office Internet gateway, Voice (IP-to-IP) Gateway and Site-to-Site Gateway
- **Enterprise High Speed Internet Gateway:** Dedicated High performance Internet gateway with the option to connect to Service Provider by either using on board FE/GE Ethernet ports or traditional WAN PA in one PA slot
- **Secure Internet gateway:** Support for features such as IP Security (IPsec) Protocol and stateful firewall at very high speeds make it an ideal Internet gateway (security) appliance.

- **Key in different Enterprise applications:** Master Controller in Optimized Edge Routing (OER) application, Key server or group member in Group Encrypted Transport (GET) VPN application, DMVPN hub, and Cisco IOS IP SLAs

Key Applications for Service Providers:

- **Broadband aggregation:** PTA/LAC or LNS/TS (Tunnel Switching) aggregation router capable of handling up to 8,000 subscribers with per sessions features enabled and up to 16,000 simultaneous sessions with basic non-CPU intensive features and allowing for a pay-as-you-grow “rack and stack” architecture.
- **Managed services:** High-end Customer Premises Equipment (CPE) or Multiprotocol Label Switching-Customer Edge (MPLS-CE) devices due to its high-performance, feature-rich support with both Gigabit Ethernet LAN connectivity and WAN port adapter connectivity.
- **High-availability design:** 100 percent redundancy via 2 CPEs configured for Hot Standby Router Protocol (HSRP) or Layer 3 load balancing.
- **Cost-effective BGP Route Reflector:** Ideally suited as a low cost route reflector with its ability to hold one million routes with its default minimum of 1 GB memory installed. It can also support a 2 GB memory.

By enabling the multifunction capabilities of the Cisco 7201 router, customers can simplify their network architectures, significantly reduce initial equipment costs, and increase revenue opportunities through value-added services.

Table 16. Key Features of the Cisco 7201 Router

Feature	Description
Performance of up to 2 Million Packets per Second (pps) in Cisco Express Forwarding Switching	• Doubles the performance compared to Cisco 7301 Router • Dramatically increases the performance and scalability in Broadband, WAN and MAN applications for both Enterprises and Service Providers
Backward Compatibility with Existing Port Adapters (with a few exceptions)	• Provides investment protection through backward compatibility
Four Fixed Gigabit Ethernet Ports (2 SFP only ports, 2 SFP or 10/100/1000 RJ45 ports)	• Maximizes LAN connectivity and performance • Eliminates the need to use the PA slot for extra GE or FE ports and frees the PA slot for supporting other applications
Dual Field-Replaceable AC or DC Power supplies	• Offers high reliability and flexibility
1 GB of DRAM Default Memory	Delivers the most amount of memory by default compared to existing Cisco 7xxx 1 RU Routers, offering the following benefits: • Supports more routes and routing tables • Supports more Multiprotocol Label Switching (MPLS) virtual routing and forwarding instances (VRFs) • Supports more sessions for broadband aggregation • Helps enable higher scalability on features such as NetFlow, Network Address Translation (NAT), access control lists (ACLs), and more • Support for optional upgrade to 2 GB DRAM
Cisco IOS Software	• Supports a wide range of IP and non-IP network services, including Quality of Service (QoS), MPLS, broadband aggregation, integrated security, encryption, voice, and more
Dedicated Management for 10/100-Mbps Ethernet	• Reduces costs and protects port density of the chassis
One USB Port	• Provides a large, removable storage for files • Stores security e-tokens for VPN applications • Supports the 32 kb Aladdin Token key for VPN applications

Feature	Description
Digital Diagnostics on SFP Interfaces	• Provides a powerful tool that monitors many manageable parameters, including optical transmit and receive power, voltage and temperature measurement, and factory parameters
Time Domain Reflectometry (TDR) on Copper Interfaces	• Provides an effective method of isolating fault at the remote end of the copper wire by monitoring reflected pulsed signals
Front-to-back airflow	• Allows rack mounting of the router from either front or back

Additional Information:

For more information about the Cisco 7201 Router, please visit http://www.cisco.com/go/7200 or contact your local Cisco account representative.

Product Management Contact: Ahmad Chehime (chehime@cisco.com)

5.9.2) ATM T3/E3 for the Cisco 2800 and 3800 Series Integrated Services Router
The new Cisco T3/E3 ATM Network Module is now available for the Cisco ISR 2800 and 3800 Series Routers that provide ATM DS3 or E3 WAN connectivity for Service Providers and Enterprise customers for regional and medium-to-large size branch office connectivity. This combined T3/E3 ATM network module provides an ATM connection of either 44 Mbps for DS3/T3, or 34 Mbps for E3 using standard 75-ohm BNC connectors. Support is provided for ATM Forum compliant framing standard AAL5, as well as ATM Traffic Management support for Unspecified Bit Rate (UBR), UBR+ (For SVC's only), Variable Bit Rate real-time (VBR-rt), Variable Bit Rate non-real time (VBR-nrt), Constant Bit Rate (CBR), and Available Bit Rate (ABR) classes of traffic.

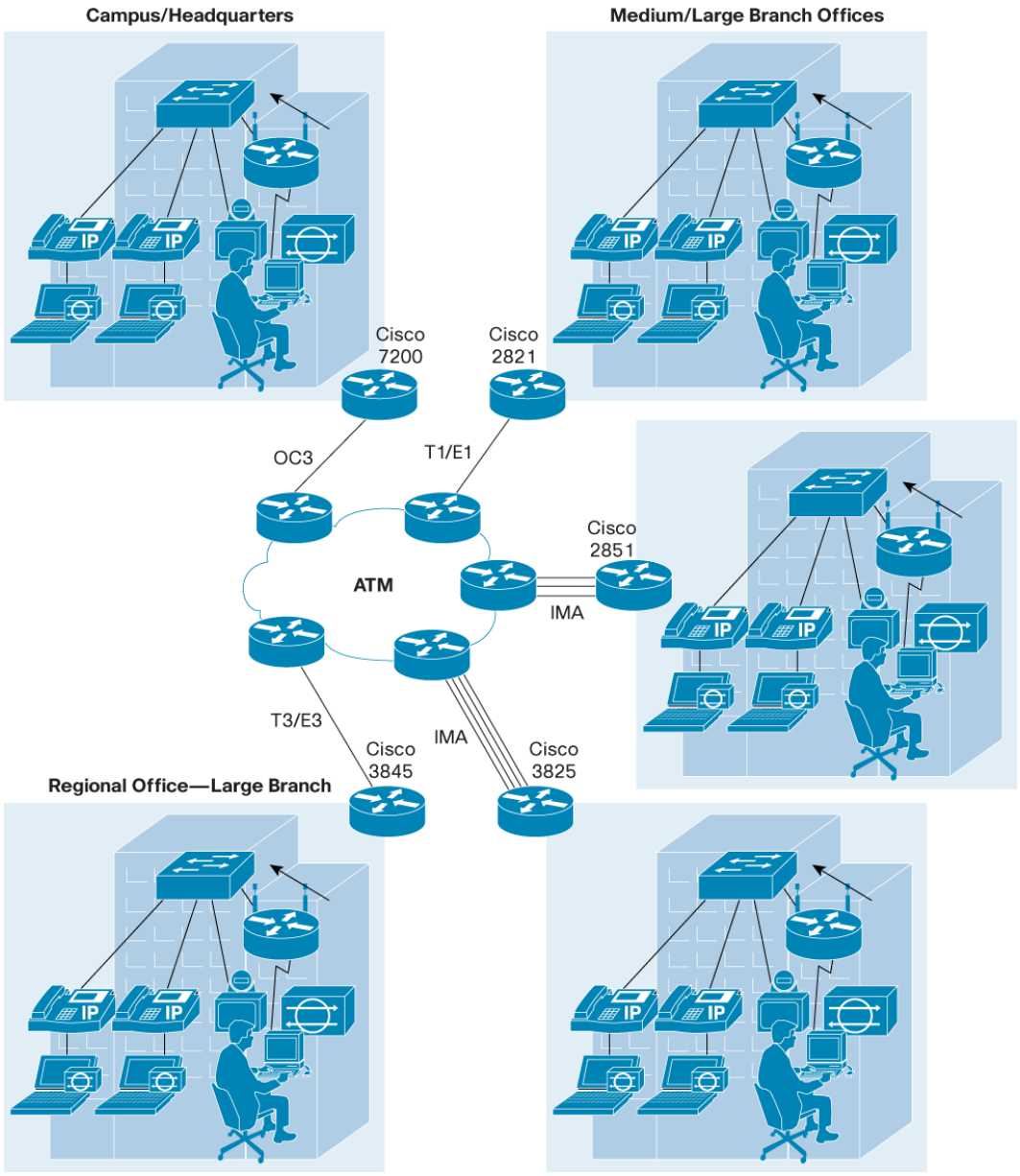
Figure 59. T3/E3 ATM Network Module

The T3/E3 ATM network modules provide a cost-effective solution that can be deployed in the Cisco 2800 and 3800 ISR's as Service Provider Managed Customer Premise Equipment (CPE) or by Enterprise customers for T3/E3 and Fractional T3/E3 connectivity to medium-to-large size branch and smaller regional office locations for consolidating multiservice data, voice and video services over a single ATM link.

The following key features are supported:

- ATM Classes of Service support for: Unspecified Bit Rate (UBR), UBR+ (SVC's only) Variable Bit Rate real-time (VBR-rt), Variable Bit Rate non-real time (VBR-nrt), Constant Bit Rate (CBR), and Available Bit Rate (ABR)
- RFC 1483 and RFC 1577 support
- 1024 maximum simultaneous Virtual Connections (VCs)
- 8 bits of VPI (VPI range 0-255), 16 bits of VCI (VCI range 0-65535)
- Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs)
- PLCP and HEC cell delineation support
- Operations and Management (F4,F5 OAM) cell support
- LANE support
- ILMI 1.0 support
- IETF PPP over ATM support
- Multiprotocol Label Swapping (MPLS) VPN support
- MPOA Client and Server
- Next Hop Routing Protocol (NHRP)
- On-line Insertion and Removal (OIR) on 3845
- Permanent Virtual Path (PVPs) support
- FRF.5/8 Interworking
- ITU-T G.703 Compliant
- ATM Traffic Management 4.1 compliant
- ATM Forum UNI 3.1/4.0 PVC compliant
- ATM Forum UNI 4.0 SVC compliant

Figure 60. ATM T3/E3 Typical Customer Deployments



Hardware

Routers	• Cisco 2811, 2821, 2851, 3825, and 3845 Series Routers

Additional Information: http://www.cisco.com/go/isr

Product Management Contact: Bill Massung (massung@cisco.com)

5.9.3) HWIC-2SHDSL & HWIC-4SHDSL

The 2-pair (HWIC-2SHDSL) and 4-pair (HWIC-4SHDSL) symmetric high-bit-rate DSL high-speed WAN interface cards (HWICs) are Cisco's next generation G.SHDSL based WAN connectivity modules for the Cisco Integrated Services Routers. The 2-pair and 4-pair G.SHDSL single-wide HWICs on the Cisco Integrated Services Routers provide high speed WAN connectivity to small medium businesses and Enterprise branch offices. The G.SHDSL HWICs provide symmetrical

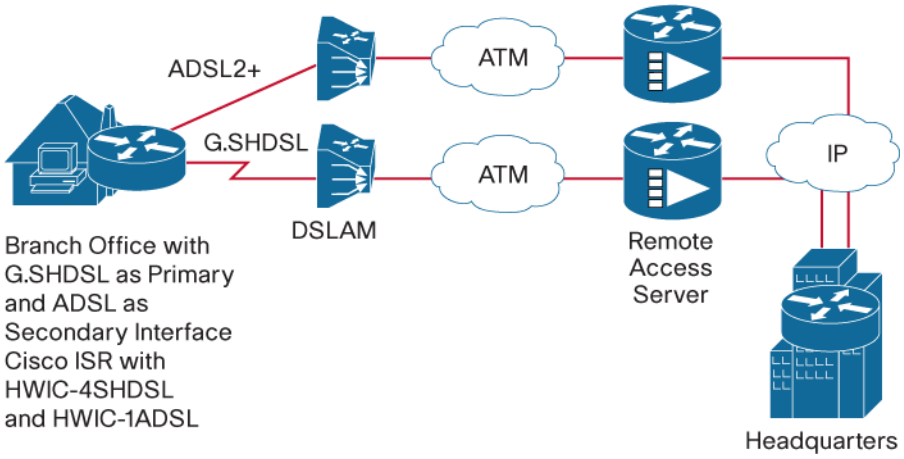
WAN data rates from 2.3 Mbps to 11.4 Mbps over single or dual pair G.SHDSL links. The 4-pair G.SHDSL HWIC also allows bonding single or dual-pair G.SHDSL links up to an 8-wire interface with symmetrical bandwidth up to 9.2 Mbps with Inverse Multiplexing over ATM (IMA), and upto 16 Mbps with M-pair mode.

G.SHDSL technology offers customers high-speed, symmetrical WAN connectivity at a lower monthly cost than traditional WAN circuits. The 2- and 4-pair G.SHDSL HWICs together with Cisco Integrated Services Routers provide businesses the necessary bandwidth for critical traffic such as voice and video conferencing, and enable customers to save money by integrating voice and data traffic on the same WAN link. Service Providers can increase subscriber revenue by bundling services and offering differentiated service levels through service level agreements.

Cisco Integrated Services Router with G.SHDSL HWIC Applications

- The Cisco Integrated Services Routers with the 2-pair and 4-pair G.SHDSL HWICs provide a business-class DSL solution for WAN access along with the option of a backup WAN interface (ADSL and ADSL2+, ISDN BRI, T1/E1, analog modem, cable modem, etc.) for mission-critical applications.
- The Cisco Integrated Services Router with the G.SHDSL HWICs can be optimized for Internet security with the Cisco IOS Firewall supporting stateful inspection firewall and intrusion prevention system features. These platforms can also be optimized for VPN, which allow secure use of the Internet for communications with the same policies and levels of security and performance as a private network.
- The G.SHDSL HWICs support Cisco IP QoS features including Class-Based Weighted Fair Queuing (CBWFQ), Low-Latency Queuing (LLQ), Weighted Random Early Detection (WRED), etc., and ATM CoS like CBR, VBR, UBR+, UBR. These features allow providers and resellers to offer services that can differentiate bandwidth based on a specific application or a specific user.
- The Cisco Integrated Services Router platforms with the G.SHDSL HWICs provide customers with a choice of converged platforms that offer best-of-class data, security, WAN access, and voice services all in a single system.

Figure 61. Typical Branch Office WAN Deployment using Cisco HWIC-4SHDSL and HWIC-1ADSL on a Cisco Integrated Services Router



Benefits

- **Lower Cost of Ownership:** The G.SHDSL HWICs on the Cisco Integrated Services Router provides users with an integrated branch office solution with security, routing, wan access, toll quality voice and application services minimizing the number of appliances in the network to provision and manage.
- **Extending Reach and Enabling Differentiated Services:** The 4-pair G.SHDSL HWIC supports IMA and M-pair mode of operation that allow Service Providers and end-user customers to bond single or dual pair G.SHDSL links to support higher data rates and extend reach (ie: support longer loop lengths). IMA and M-pair mode of operation also allows Service Providers to provide differentiated services based on bandwidth requirements at the customer edge.
- **Flexibility:** Single-wide form factor for the 2-pair and 4-pair G.SDSL HWICs allows the Cisco Integrated Service Routers to use the other HWIC slot(s) for backup WAN or LAN connectivity.

Hardware

Routers	• Cisco 1841, 2800, and 3800 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps5949/products_data_sheet0900aecd80581fa0.html

Product Management Contact: Subbu Mahadevan (smahadev@cisco.com)

5.9.4) Cisco 1- and 2-Port Enhanced Capability T3/E3 Clear Channel Port Adapters and Feature Offload Support for Multichannel T3 Port Adapters
Several new products and capabilities are being brought to the market in the Cisco IOS Software12.4(15)T release. The new products are the Cisco® 1- and 2-Port Enhanced Capability Clear Channel Port Adapters for the Cisco 7200 Series Routers, Cisco 7201 and Cisco 7301 Router are enhanced “two in one” versions (PA-T3/E3-EC and PA-2T3/E3-EC) of the earlier clear channel T3 and E3 port adapters (part numbers PA- T3+, PA-2T3+, PA-E3 and PA-2E3). These new “two in one” products assist network implentators by minimizing sparing of both T3 port adapters for the United States and E3 for European and Asian implementations. The new “two in one” port adapters provide a new software architecture that allows selecting either T3 or E3 by way of software configuration coupled with a more powerful chipset that lowers CPU utilization while performing at line rate. The new port adapters show that they lower CPU utilization by 14% but at the same cost. Line-rate performance with lower CPU utilization on the Cisco 7200 Series, Cisco 7201 and Cisco 7301 platforms provide scalable trunking services for both Enterprise and Service Provider customers. Table 10 lists the router platforms and Cisco IOS® Software releases that support these new port adapters.

The new offload features are supported on the Cisco® 1- and 2-Port Multichannel Enhanced Capability Port Adapters (PA-MC-T3-EC and PA-MC-2T3-EC). These new port adapters were released in Release 12.4(11)T and provide new scalability capabilities as well as heavy weight feature offload in Release 12.4(15)T. They offload advanced capabilities and features from the CPU such as Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), Link Fragmentation and Interleaving (LFI), and FRF.12. Table 11 lists the router platforms and Cisco IOS® Software releases that support these features. Each port adapter T3 interface can be independently configured for either multichannel T3 or clear-channel packet-over-T3 operation.

Table 17. Features Table for PA-T3/E3-EC and PA-2T3/E3-EC

Feature	Supporting Platform	Cisco IOS Software Release
Line-rate performance: Up to 34.368 Mbps per E3 port	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
Line-rate performance: Up to 44.736 Mbps perT3 port	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
Lower CPU Utilization	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC

Table 18. Features Table for PA-MC-T3-EC and PA-MC-2T3-EC

Feature	Supporting Platform	Cisco IOS Software Release
Line-rate performance: Up to 44.736 Mbps per port	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
MLPPP	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
LFI	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
MLFR	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC
FRF.12	Cisco 7204/7206VXR NPE-400, NPE-G1, NPE-G2, Cisco 7201, Cisco 7301	Releases 12.4(15)T and 12.2 SRC

New Features

The following list describes the features delivered by the intelligent hardware of the PA-MC-T3-EC and PA-MC-2T3-EC Port Adapters:

- **Multilink Point-to-Point Protocol (MLPPP):** Provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.
- **Link fragmentation and interleaving (LFI):** Reduces delay on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets with the smaller packets resulting from the fragmented datagram.
- **Multilink Frame Relay (MLFR):** Provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single bundle of bandwidth. It is supported on User-to-Network Interfaces (UNIs) and Network-to-Network Interfaces (NNIs) in Frame Relay networks.
- **FRF.12:** Allows long data frames to be fragmented into smaller pieces. This process allows real-time traffic and non-real-time traffic to be carried together on lower-speed links without causing excessive delay to the real-time traffic.

Upgrade Paths

- Cisco 7204VXR, 7206VXR, and 7301 customers who wish to upgrade from the earlier port adapters (part numbers PA-T3+, PA-2T3+, PA-E3 and PA-2E3) and require T3/E3 line rate should consider migrating to the “two in one” Cisco 1- and 2-Port Multichannel Enhanced Capability T3/E3 Clear Channel Port Adapters. These new adapters are supported by the Cisco NPE-400, NPE-G1, and NPE-G2 network processing engines as well as the Jacket Card.
- Cisco 7204VXR, 7206VXR, and 7301 customers who wish to upgrade from the earlier port adapters (part numbers PA-MC-T3 and PA-MC-2T3+) and require hardware offload support

of MLPPP, LFI, MLFR, and FRF.12 at T3 line rate should consider migrating to the Cisco 1- and 2-Port Multichannel Enhanced Capability Port Adapters. These new adapters are supported by the Cisco NPE-400, NPE-G1, and NPE-G2 network processing engines

Hardware

Routers	• Cisco 7200, 7201, and 7301 Series Routers

For More Information

- For more information about the Cisco 1- and 2-Port Enhanced Capability Clear Channel Port Adapters, please visit: http://www.cisco.com/en/US/products/hw/modules/ps2033/ps2956/index.html
- For more information about the Cisco 1- and 2-Port Multichannel Enhanced Capability Port Adapters, please visit: http://www.cisco.com/en/US/products/hw/modules/ps2033/prod_module_series_home.html

Product Management Contact: Ruben Rios (rurios@cisco.com)

5.9.5) USB eToken 64KB Enhancement

This feature enables device authentication through smartcard and the deployment and secure configuration of Cisco routers. It uses 32 or 64KB smart card technology in a USB form factor to facilitate the authentication and configuration process. The token provides secure access to the router-the token and a PIN are necessary to access the configuration, keys, and credentials. The token can also be used to securely provide the configuration to the router, because the configuration can be encrypted on the token.

Benefits

- **Flexibility and Ease of Roll-Out:** Customers are able to order routers directly from Cisco (or a reseller) with a desired Cisco IOS Software image installed, to have the routers shipped directly to the customer premises, and to provide configuration files in a touchless or low-touch manner by distributing an eToken device. This allows the customer or Service Provider to use deployment technicians of a lower skill set for router installations.
- **Higher Security and Customization:** Security credentials are physically separated from the chassis of the router.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800 Series Routers

Additional Information: http://www.cisco.com/go/usb

Product Management Contact: Christian Lorentz (clorentz@cisco.com)

5.9.6) Boot from USB Flash Enhancement

This feature provides an optional secondary storage capability and additional boot device for Cisco IOS Software images. Images, configurations, or other files can be copied to or from the Cisco USB Flash memory with the same reliability as storing and retrieving files using the Compact Flash card. Cisco USB Flash memory is available in 64, 128, and 256 MB sizes. With the latest common version, customers can also boot any IOS stored on USB Flash.

Benefits

New Cisco IOS Software images can be booted directly from the USB flash drive without having to transfer the image to the compact flash card.

Hardware

Routers	• Cisco 1841, 2800, and 3800 Series Routers

Additional Information: http://www.cisco.com/go/usb

Product Management Contact: Christian Lorentz (clorentz@cisco.com)

6) Release 12.4(11)T Highlights

Table 19. Release 12.4(11)T Feature Highlights

6.1) Cisco IOS Security	6.2) Layer 2 VPN	6.3) Multiprotocol Label Switching Management	6.4) IP Services
6.1.1) Cisco IOS SSL VPN Enhancements 6.1.2) SSL VPN Netegrity Single Sign-on (SSO) Support 6.1.3) SSL VPN Application ACL Support 6.1.4) SSL VPN Port-forwarding Enhancement 6.1.5) SSL VPN Debug Infrastructure 6.1.6) SSL VPN URL Obfuscation Support 6.1.7) Group Encrypted Transport (GET) VPN 6.1.8) MPLS VPN (RFC 2547) over Dynamic Multipoint VPN (DMVPN) 6.1.9) EasyVPN Phase 8.0 Enhancements 6.1.10) Cisco IOS Firewall H.323 Registration, Admission, and Status (RAS) Message Inspection Support 6.1.11) Cisco IOS Intrusion Prevention System (IPS) Version 5.0 Signature Format Support	6.2.1) L2VPNs over MPLS—Any Transport over MPLS (AToM) 6.2.2) Ethernet over MPLS (AToM) 6.2.3) VLAN ID Rewrite 6.2.4) Frame Relay over MPLS (FRoMPLS) 6.2.5) Any Transport over MPLS (AToM) Interworking 6.2.6) Multilink Frame Relay over MPLS (AToM) 6.2.7) Any Transport over MPLS (AToM) High Availability 6.2.8) AToM Pseudowire Redundancy 6.2.9) AToM Graceful Restart 6.2.10) Layer 2 Local Switching with Interworking 6.2.11) Layer 2 Tunnel Protocol Version 3 (L2TPv3) Enhancements	6.3.1) Cisco IOS Multiprotocol Label Switching Embedded Management	6.4.1) DHCP Relay per interface VPN ID support 6.4.2) DHCP Class Support for Option 60, 77, 124, 125 6.4.3) Hot Standby Routing Protocol Bidirectional Forwarding Detection Peering 6.4.4.) Enhanced Object Tracking support for Mobile IP, PDSN or GGSN 6.4.5) Show and Clear Commands for Cisco IOS Sockets 6.4.6) Cisco Express Forwarding (CEF) L4 Port Load Balancing 6.4.7) Tunnel Source Address Selection 6.4.8) Radius Server Load Balancing

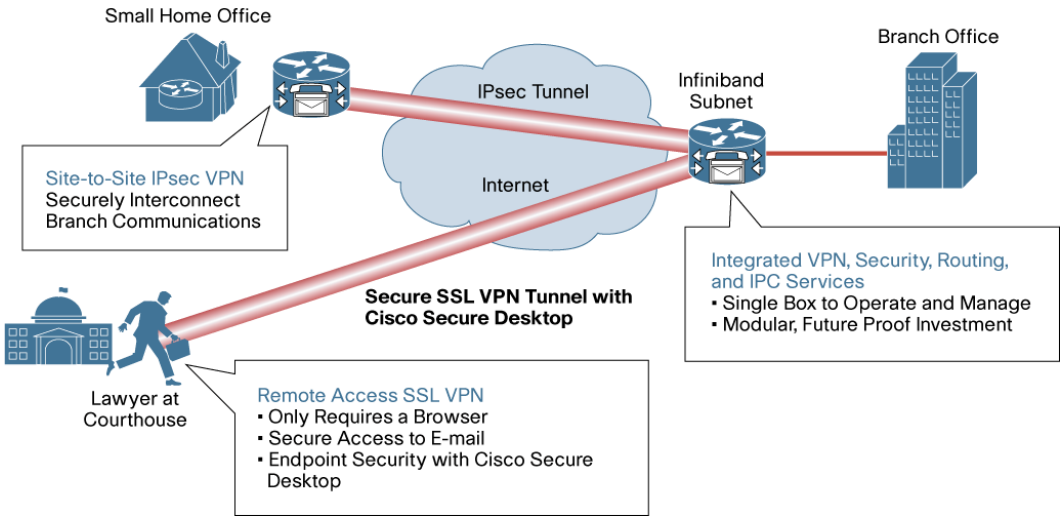
6.5) IP Mobility and Wireless	6.6) Quality of Service	6.7) Voice	6.8) Hardware
6.5.1) Mobile IPv6 Authentication Option Support 6.5.2) Mobile IPv6 Network Access Identifier (NAI) Support 6.5.3) Cisco Mobile Wireless Home Agent Release 3.0 6.5.4) Cisco Packet Data Serving Node (PDSN) Release 3.0	6.6.1) ATM QoS Features for the Asymmetric Digital Subscriber Line (ADSL2/ADSL2+) High-Speed WAN Interface Card (HWIC-1ADSL) for Cisco 1800, 2800, and 3800 Series Routers	6.7.1) Enhancements to Cisco IOS Session Border Controller (SBC)- Cisco Multiservice IP-to-IP Gateway 6.7.2) VoiceXML Browser Update—Support of W3C VoiceXML Forum Standard VXML 2.0 6.7.3) Internet Low Bit Rate (iLBC) Codec Support for SIP and H.323 6.7.4) Internet Low Bit Rate codec (iLBC) Support on IP-to-IP Gateway for Flow-through and Flow-around Modes 6.7.5) Support for the Second Generation 1- and 2-port T1/E1 Multiflex Trunk Voice (MTF) WAN Interface Cards on the 2430 Series Integrated Access Devices 6.7.6) Support for the Multiflex Trunk Dedicated Echo Cancellation (MFT ECAN) Modules on the 2430 Series Integrated Access Devices 6.7.7) Skinny Call Control Protocol (SCCP) Controlled Analog (FXS) Ports with Enhanced Supplementary Features in IOS Gateway	6.8.1) Network Processing Engine G2 (NPE-G2) for Cisco 7200 Series Router 6.8.2) VPN Services Adapter (VSA) for Cisco 7200VXR Series Routers

6.1) Cisco IOS Security

6.1.1) Cisco IOS SSL VPN Enhancements

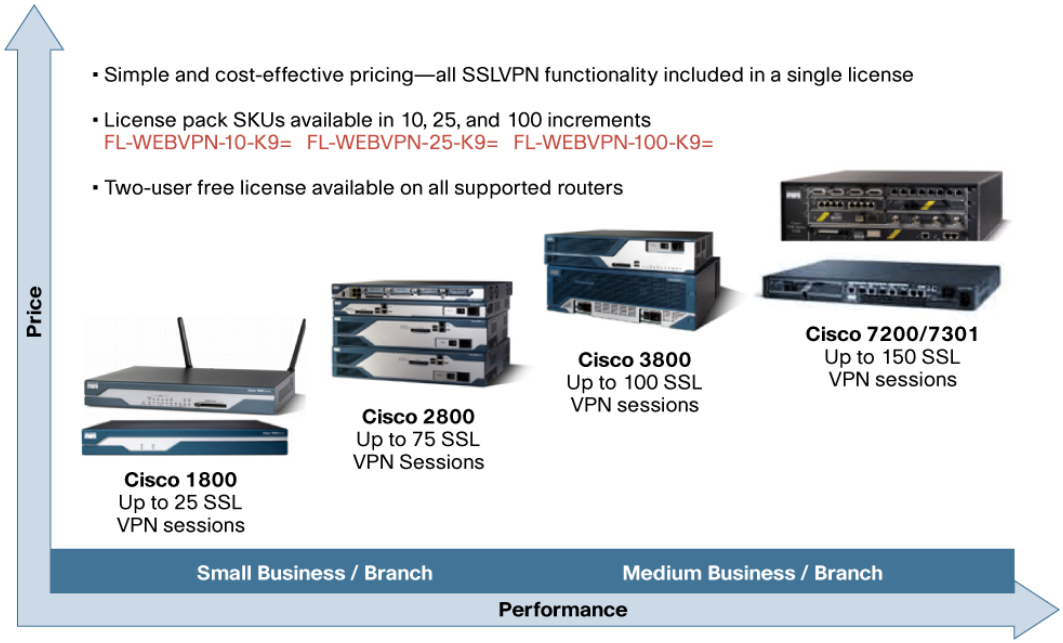
SSL VPN in clientless mode is an application aware technology. Using SSL VPN on the routers, companies can securely and transparently extend their companies' networks to any Internet-enabled location. SSL VPN is compelling because the security is transparent to the end user and is easy for an IT staff to administer and maintain. Using only a Web browser, companies can extend their secure Enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots, enabling higher employee productivity and protecting corporate data. Cisco IOS SSL VPN supports full tunnel client access and clientless access to applications such as HTML-based intranet content, email, network file shares, and Citrix. While this allows for a great end-user experience, it has to be balanced with proper access-control for the end-user to only get access to the corporate resources that are allowed by the corporate policy. Figure 49 illustrates a user case scenario for customers implementing Cisco IOS SSL VPN effectively at the branch router.

Figure 62. Cisco IOS SSL VPN Use Case Scenario



Cisco IOS SSL VPN is a licensed feature supported on Cisco 871, 1800, 2800, 3700, 3800, 7200, and 7301 routers running the Advanced Security image on Cisco IOS Software Release 12.4(6)T or higher. The feature license can be purchased in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com ordering tool or through your Cisco partner/account team. Figure 50 provides more portfolio and license pricing details.

Figure 63. Cisco Routers with SSL VPN
SSL VPN Portfolio and Pricing



SSL VPN functionality added in Release 12.4(11)T includes the following features:

- SSL VPN Netegrity Single Sign-on (SSO) Support
- SSL VPN Application ACL Support
- SSL VPN Port-forwarding Enhancement
- SSL VPN Debug Infrastructure
- SSL VPN URL Obfuscation Support

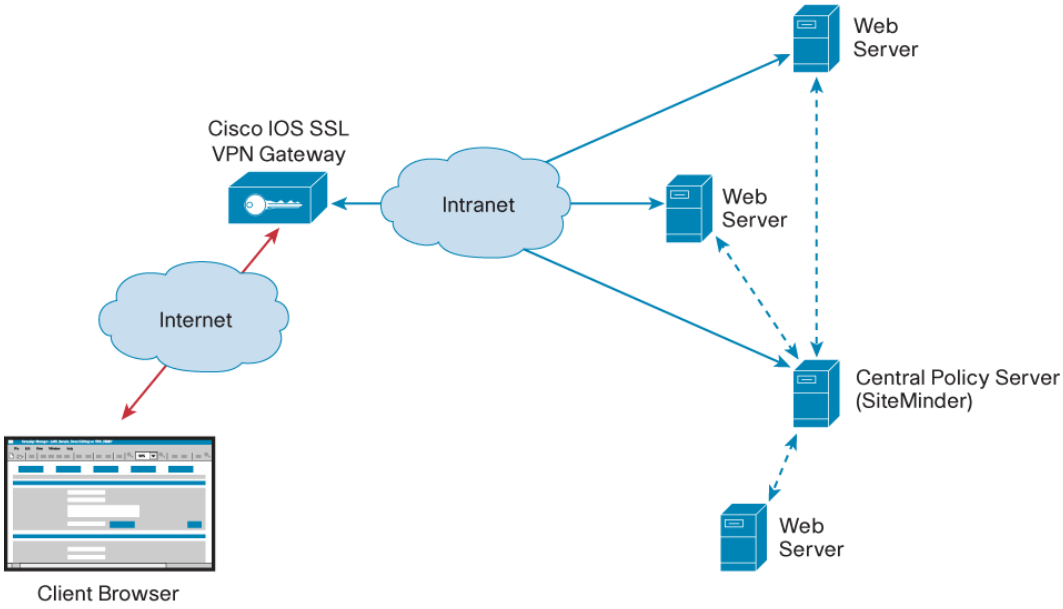
6.1.2) SSL VPN Netegrity Single Sign-on (SSO) Support

When users attempt to access web (HTTP/HTTPS) resources of a corporation or a partner, they may be prompted to authenticate in order to validate access to the particular information. Generally these credentials are specific to a particular application and access control information must be located on each individual web server. Basic centralized authentication options offered do not allow for granular access control. This may mean that a user needs to remember multiple passwords or to enter the same username/password multiple times.

Netegrity SiteMinder allows corporations to provide seamless access to many web resources, using almost any possible authentication option, and eliminates the need to authenticate to each individual server. This solution simplifies the authentication process for network resources by eliminating the need to constantly re-authenticate and removes the requirement for multiple distinct access control databases.

Netegrity SiteMinder functions by supplying an encrypted cookie back to the user's Web browser after authenticating to the first SiteMinder Agent-enabled web server. Other enabled servers use this cookie to identify this particular user and validate access to any available resources. Each web server must have a SiteMinder Agent installed, which performs verification of the cookie and access rights by communicating with a centrally controlled policy database (SiteMinder Policy Server). Figure 51 illustrates what the implementation would look like in a customer network.

Figure 64. SSL VPN Netegrity SiteMinder Single Sign-on implementation



Benefits

- **Seamless end-user access:** SSL VPN Netegrity SiteMinder Single Sign-on feature enables users to avoid redundant and tedious logins to different web servers/applications.
- **Flexible Intranet access:** This feature support provides the convenience of single unified login to all applications for the users logging in through the SSL VPN gateway.

6.1.3) SSL VPN Application ACL Support

The SSL VPN Application ACL feature provides administrators the ability to control end-user access to corporate applications, by filtering the connection requests based on URL and user/group policy. While developing this functionality, a balanced approach was adopted by keeping configuration as simple as possible while providing administrators the detail/flexibility they need to secure their corporate applications through applying corporate security application usage policy to each user.

The SSL VPN Application ACL functionality includes both Network-level and Application-level ACL support. In the application layer, the gateway may have a better idea regarding how to filter the traffic than it does in network layer; hence this feature provides great flexibility for customers to filter the traffic going through their SSL VPN tunnel. SSL VPN Application ACL enhances the already rich Cisco IOS SSL VPN feature-set, providing the necessary control on the traffic that traverses the SSL VPN tunnel to the inside network.

Network-level ACL, the SSL VPN gateway (router) will allow access control based on network protocols, source IP address and destination IP address.

Application-level ACL, the SSL VPN gateway (router) will allow matches based on the application filter URL string. The URL may include a wildcard for the server names, may be a partial URL, or may include a port number or server IP address/net mask.

Benefits

- **Flexibility in access methods:** Using SSL VPN, companies can securely and transparently extend their companies network to any Internet-enabled location, while using Application ACL to control what these end-users can access.

- **Broad Range of Filtering Options:** The administrator is allowed to match based on the application filter URL string. The URL may include a wildcard for the server names, may be a partial URL, or may include a port number or server IP address/net mask.

6.1.4) SSL VPN Port-forwarding Enhancement

The Port forwarding applet is started when the user clicks the “Start Application Access” link on the SSL VPN portal page. A new browser window will be launched with the applet. This Java-based Port forwarding applet is also known as the SSL VPN Thin-client mode. The Java-based application helper provides support for additional TCP-based applications that are not Web-enabled and supplements clientless access by providing connectivity to applications such as e-mail, instant messaging, Telnet, SSH etc.

The Port-forwarding enhancements were added to improve the existing thin-client support (application helper). As part of this enhancement, HTTP proxy functionality was added, like the one that might be found on the network (ie: an Internet Proxy). The HTTP proxy code modifies the browser’s proxy configuration on demand to redirect all browser HTTP/S requests to the new proxy configuration. This allows the Java Applet to take over as the proxy for the browser. For additional security, the applet needs to be digitally signed, since this allows for file modification, and port opening rights. It supports both HTTP and HTTPS connections.

Another possible use case for this functionality is to provide access to Web pages for which the mangling code isn’t supported. This occasionally occurs with sites that use Java, ActiveX and Flash. By auto-installing an HTTP proxy on the user’s workstation, the mangling code can be bypassed, while allowing connection to pass through the secure gateway.

The table below provides a quick comparison between the old and new port-forwarding enhancement.

Table 20. SSL VPN Port Forwarding Comparison by Cisco IOS Release

Feature	hosts file update	Ports <= 1024	Registry Modification
Original Port forwarding applet in Cisco IOS Release 12.4(6)T	Optional	Optional	Not needed
Enhanced Port forwarding using HTTP Proxy in Cisco IOS Release 12.4(11)T	Not needed	Not needed	

Note: It is recommended that Cisco Secure Desktop be used with the HTTP Proxy feature when used on a public terminal or a non-corporate owned workstation.

Benefits

- **Improved Performance:** The enhanced port-forwarding applet uses HTTP proxy which provides much better performance due to client side caching as compared to the older implementation.
- **Support for Virtually all client-side Web technologies:** No mangling is required at the SSL VPN Gateway which provides seamless support for all web content that cannot be mangled using the SSL VPN clientless functionality including embedded ActiveX and Flash content.

6.1.5) SSL VPN Debug Infrastructure

The SSL VPN Debug Infrastructure introduced in Release 12.4(11)T aims to provide an easy to use methodology to debug SSL VPN problems more efficiently. This release adds an extensive

debug infrastructure to help customers and Cisco Technical Assistance Center engineers better identify and filter the activity on the network.

Benefits

- **Increased Visibility and Troubleshooting Capabilities:** Using the SSL VPN Debug Infrastructure, customers and Cisco Technical Assistance Center engineers can easily identify and resolve problems by filtering data based on client information such as username, source IP address, and context name.
- **Timely resolution:** The Debug Infrastructure provides a better way to filter all the messages and resolve the problem in a timely manner.

6.1.6) SSL VPN URL Obfuscation Support

Employees or partners accessing internal resources via SSL VPN have visibility in to internal IP addressing and DNS names. This unnecessarily exposes internal host information to remote users accessing web resources. This feature would ensure that the directory path being accessed on the internal network is hidden from the remote user. The functionality provides the ability to hide (ie: obfuscate) the internal hostnames, IP addresses in the URL links presented at the client browser.

The benefit is the security of hiding/masquerading internal hosts for over-the-shoulder viewers at an Internet kiosk etc. If enabled, sites accessed become converted into masqueraded URLs containing randomly generated strings (cookies) instead of actual host names/IPs. This includes all bookmarks and sites accessed by entering in the URL in the appropriate location on the web page.

Example:

Accessing http://somesite.cisco.com/index.html which presently becomes something like:

https://testvpn.cisco.com/http/0/somesite.cisco.com/index.html

Would become a randomly generated URL:

https://testvpn.cisco.com/http/0/342FDSFDSCS0AFA5A1DSA/index.html

Benefits

- **Increased Security:** URL obfuscation provides the ability to hide the internal hostnames, IP addresses, directory path in the URL links presented at the client browser.

Considerations

The SSL VPN URL obfuscation feature is disabled by default.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: Aamir Waheed, (awaheed@cisco.com) or ask-stg-ios-pm@cisco.com

6.1.7) Group Encrypted Transport (GET) VPN

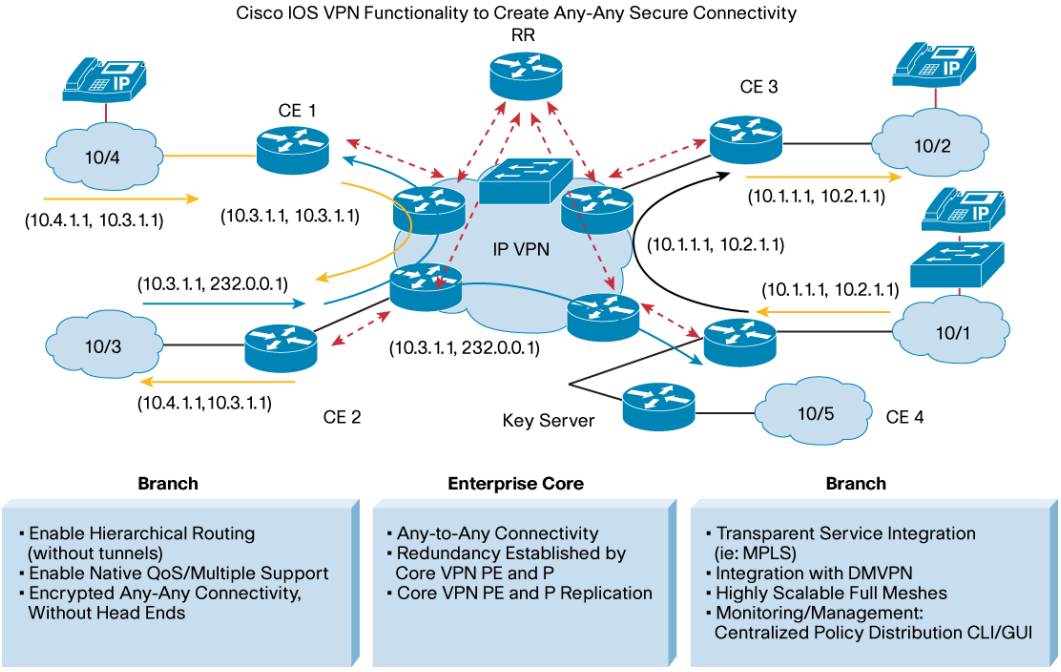
Today's networked applications such as voice and video drive the need for instantaneous, branch interconnected, and QoS-enabled WANs. The distributed nature of these applications results in increased demands for scale. At the same time, Enterprise WAN technologies force businesses to

make a trade-off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes paramount, Group Encrypted Transport (GET) VPN, a next-generation WAN encryption technology, eliminates the need to compromise between network intelligence and keeping data private.

GET introduces a new IPsec-based security model that is based on the concept of “trusted” group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. By utilizing trusted groups instead of point-to-point tunnels, meshed networks are able to scale higher while maintaining network intelligence features critical to voice and video quality—such as QoS, routing and multicast.

Group Encrypted Transport networks can be used in a variety of WAN environments, including IP/MPLS. GET-enabled MPLS VPNs are highly scalable, manageable and cost-effective, and meet government mandated encryption requirements. The flexible nature of GET allows security-conscious Enterprises to manage their own network security over a service provider WAN service or to off load encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks requiring partial or full mesh connectivity.

Figure 65. Group Encrypted Transport



Features

GET is built on standards based technologies and integrates routing and security seamlessly together in the network fabric. Secure group members are managed through an IETF standard, Group Domain of Interpretation (GDOI).

Table 21. Summary of key GET features

Group Domain of Interpretation	GDOI (RFC 3547) is the key management protocol that establishes security associations among authorized group member routers.
IP Header Preservation	The original IP header in IPsec packets is preserved.

Centralized Key and Policy Management	A centrally available key server, typically a head-end router, is responsible for pushing keys and re-key messages as well as security policies to authorized group member routers. Both local and global policies—applicable to all members in a group– are supported, such as “Permit any any,” a policy to encrypt all traffic.
Key Server High Availability	The key server, responsible for pushing keys and policies, supports high availability by synchronizing keys and the policy database with a secondary key server.
Support for Anti-replay	Anti-replay support protects against Man-in-the-Middle attacks.
Encryption Support	DES, 3DES and AES

Benefits

In extending GDOI by encrypting and authenticating both multicast and unicast traffic, GET provides benefits to a variety of applications:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- For MPLS networks, maintains the network intelligence such as full-mesh connectivity, natural routing path, and Quality of Service (QoS)
- Grants easy membership control with a centralized key server
- Ensures low latency and jitter by enabling full-time direct communications between sites—no inefficient central hub site traversal required
- Reduces traffic loads on CPE/PE encryption devices by leveraging core for replication for multicast traffic—no packet replication for each individual peer site

Hardware

Routers	• Cisco 870, 1800, 2800, 3800, 7200, 7301 Series Routers
Key Servers	• Cisco AIM-VPN/SSL module for Cisco Integrated Services Routers • Cisco VAM2+ for Cisco 7200 Series and 7301 Routers
Group Members	• Cisco Integrated Services Router (ISR) Series, Cisco 870, 1800, 2800, 3800

Product Management Contact: Siva Natarajan (sinatara@cisco.com) or ask-stg-ios-pm@cisco.com

6.1.8) MPLS VPN (RFC 2547) over Dynamic Multipoint VPN (DMVPN)

Enterprise customers increasingly require segmentation for a number of different reasons. Those reasons include:

- Closed User Groups (CUG)
- Virtualization
- Enterprises acting as an internal service providers
- Protection for critical applications

Enterprises require VPNs to be created and segmented based on practical considerations that conform to the business needs of the organization. For example, a company-wide multicast stream would need to be accessible by all the employees irrespective of their group association.

Segmentation to the end-user desktop is driving virtualization in the application server space. This means that even existing employees can be segmented into different Closed User Groups where they are provided access to internal services based on their group membership. For certain

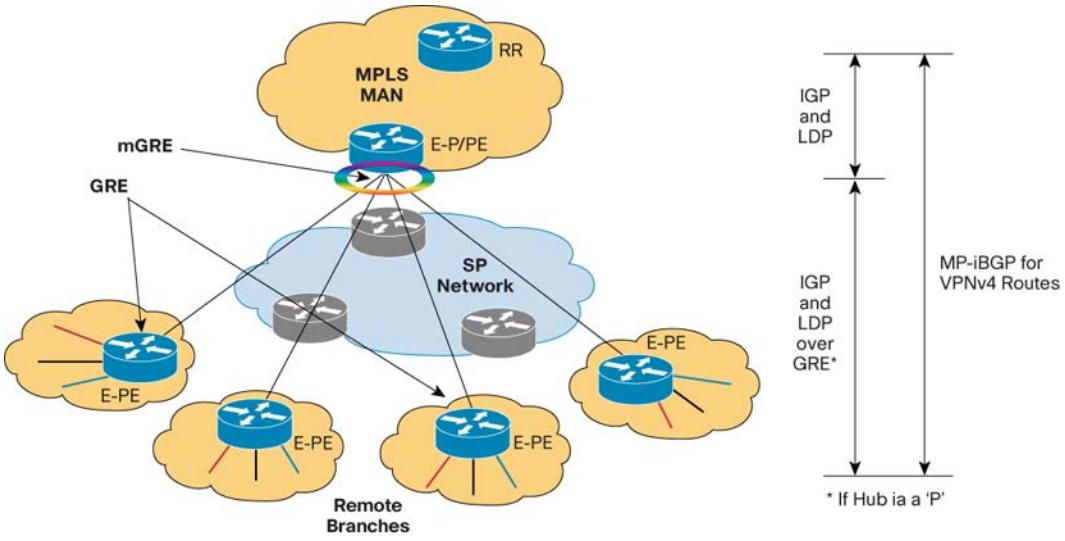
Enterprises, in addition to users, the applications themselves are driving the needs for virtualization. For example, an organization that feels that its critical applications need to be separated from everyday network users can create VPNs for each application or group of applications.

Initially, the solutions focused for virtualization requirements focused on the Enterprise core networks. Lately, the concept of virtualization has been expanded across the WAN edge to their remote branches. MPLS VPN (RFC 2547) over DMVPN is a deployment model for these Enterprises that have requirements for virtualizing their Enterprise branches.

DMVPN provides two key advantages—bulk encryption, and scalable overlay model--for extending MPLS VPNs to the branches. The large number of existing DMVPN deployments makes this an attractive deployment option. Since the branches are connected to the hub through a Layer 3 SP service, a tunneled model using GRE is needed to extend MPLS to the branches. DMVPN allows the hub to have a single multipoint GRE tunnel interface to support large numbers of spokes. The spokes can be point-to-point or multipoint GRE tunnels depending on the requirement of direct spoke-to-spoke communication.

The DMVPN model does not have some of the scale limitations of the Multi-VRF based solutions because the GRE tunnels are created outside the VRFs and a single tunnel can be shared for transporting many VRFs. The hub is configured with a single mGRE tunnel while spokes have a single GRE tunnel. It is important to note that the model is to be used for hub and spoke communication only.

Figure 66. MPLS VPN (RFC 2547) over DMVPN (Hub & Spoke Only)



As shown in Figure 53, in the control plane the following protocols exist:

- Routing protocol with the provider to learn the branch and head end router physical interface addresses (tunnel source address). Static routes could be used as well if they could be easily summarized.
- Static GRE tunnel between the branch PE and the head end P.
- IGP running in the Enterprise global space over the GRE tunnel to learn remote PE's and RR's loop back address (only if the head end is a P).

- LDP session over the GRE tunnel with label allocation/advertisement for the GRE tunnel address by the branch router (only if the head end is a P).
- MP-iBGP session with Route Reflector, where the branch router's BGP source address is the tunnel interface address—this forces the BGP next-hop lookup for the VPN route to be associated with the tunnel interface.

Additionally, IPsec can be used to encrypt the GRE tunnels; encryption happens after the GRE encapsulation.

Benefits

Key benefits and applications of MPLS VPN (RFC 2547) over DMVPN include:

- **Bulk Encryption:** Customers can use the MPLS VPN (RFC 2547) over DMVPN to do bulk encryption, satisfying security requirements.
- **Scalable overlay model:** Customers can use the MPLS VPN (RFC 2547) over DMVPN to build a scalable overlay model.

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200, 7301 Series Routers
Hub Devices	• Cisco 7200VXR with NPE-G1 or higher
Spoke Devices	• Cisco Integrated Services Router (ISR) Series 1800, 2800, 3700, 3800, 7200, 7301

Product Management Contact: Siva Natarajan (sinatara@cisco.com) or ask-stg-ios-pm@cisco.com

6.1.9) EasyVPN Phase 8.0 Enhancements

EasyVPN Manageability Enhancements

These enhancements include new filters for existing show, clear, and debug commands. It also includes new commands for group and individual session viewing and debugging.

The specific enhancements include:

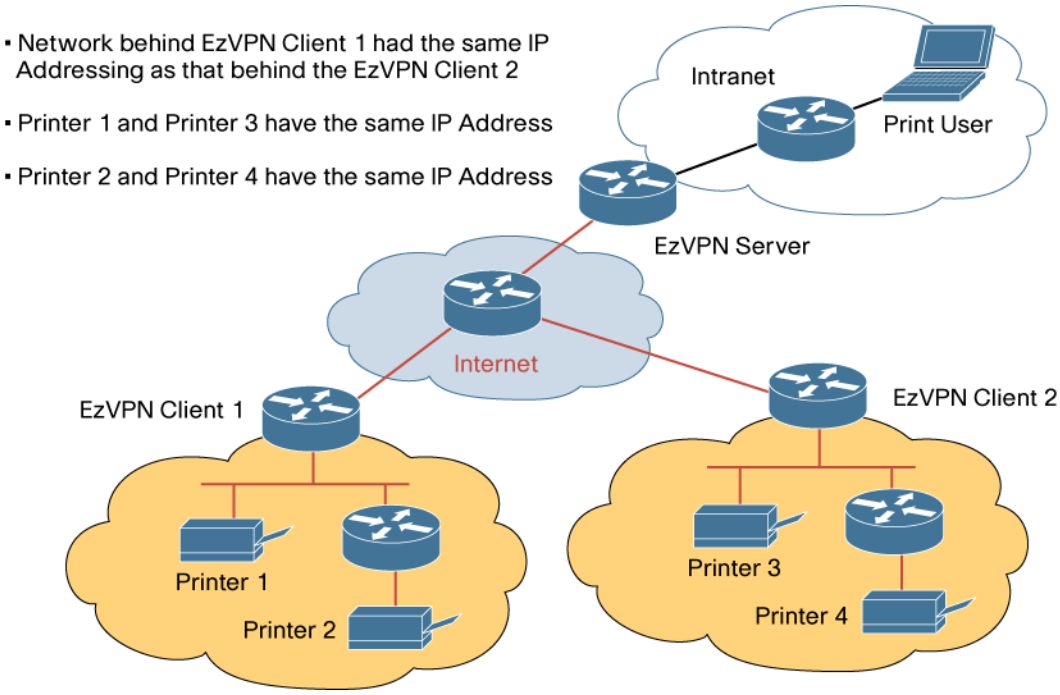
- New filters for the "show crypto session" command. The filters include username, isakmp-profile, group, local-address, and interface.
- Extending the "show crypto session" and "show crypto session detail" displays to include username, isakmp-profile, group, assigned-address, fvrf, and ivrf.
- Providing one line session information using "brief" extension to "show crypto session" commands or any of the other "show crypto session" command variants such as "show crypto session isakmp group <group> brief."
- New filters for the "clear crypto session" command. The new filters include username and isakmp-group. The username filter is only valid when Extended Authentication (XAuth) is used.
- New filters for the "debug crypto session" command. The new filters include username, profile-name, and local-address.

EasyVPN Remote Identical Addressing Support

This feature supports having identically addressed LANs on EasyVPN Remotes. Network resources such as printers and Web servers on the LAN side of the EasyVPN Remote that have

overlapping addressing with other EasyVPN remotes can now be reachable. The EasyVPN Remote feature was enhanced to work with NAT to provide this functionality. The EasyVPN Server requires no changes to support this functionality. This feature is supported in network extension modes only (network-extension and network-plus).

Figure 67. Easy VPN Remote Identical Addressing Support



Notes

- This is an EasyVPN Remote functionality enhancement and involves no change on the existing EasyVPN Server configuration.
- The restriction to use this feature is that it is supported on Enhanced EasyVPN with Network-Extension mode only.

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, 7200 Series, and 7301, Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

6.1.10) Cisco IOS Firewall H.323 Registration, Admission, and Status (RAS) Message Inspection Support

The Registration, Admission and Status (RAS) signaling protocol is part of the H.323 protocol suite and is generally used between voice gateways and gatekeepers. The H.323 RAS message inspection support feature provides users/customers a secure way to allow RAS messages between zones without having to enable entire UDP protocol inspection for the H.323 RAS port (1719 by default). H.323 RAS messages between peers are tracked to establish their request-response relationship and accordingly, only RAS messages from known peers are accepted for inter-zone traffic. This feature is only supported in the new zone based firewall policy configuration model. This feature is also supported for messages originated from the router or terminating on the router.

Please note that the ports registered by an endpoint are NOT opened automatically for H.225 connection acceptance through the Cisco IOS Firewall. The user has to include H.323 inspection separately to allow connections to an endpoint.

Benefits

Customers who previously had to enable “inspect UDP” for RAS messages on port 1719 can now only enable “inspect h.323-ras” and achieve better performance and security because not all UDP messages on port 1719 are allowed through/inspected.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Router

Additional Information: http://www.cisco.com/go/iosfirewall

Product Management Contact: Darshant Bhagat (dabhagat@cisco.com) or ask-stg-ios-pm@cisco.com

6.1.11) Cisco IOS Intrusion Prevention System (IPS) Version 5.0 Signature Format Support
The Intrusion Prevention System (IPS) feature now supports using the same signature format as Cisco IPS appliances/modules (also known as Cisco Intrusion Prevention System version 5.x signature format). This enhancement allows the Cisco IOS IPS feature to support more signatures. It also provides a “Risk Rating” value (calculated based on signature severity and fidelity) within the IPS alarms sent to event monitoring applications for easier and more effective event correlation.

Due to this change in IPS signature format in Release 12.4(11)T, existing users of the Cisco IOS IPS feature will have to follow the update procedure to migrate to the new format while upgrading their routers to this new release. More information on can be found at http://www.cisco.com/go/iosips.

To configure and manage Cisco IOS IPS features in Release 12.4(11)T, Cisco highly recommends using one of the two management applications: The next release of Cisco Security Manager Software and Cisco Router and Security Device Manager (SDM) will support Cisco IOS IPS 5.x. SDM will also include a IPS migration wizard to assist existing Cisco IOS IPS users to migrate their configuration and signature files from previous Cisco IOS Software Releases to Release 12.4(11)T.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, 7300 Series Routers

Product Management Contact: Kemal Akozer (kemal@cisco.com) or ask-stg-ios-pm@cisco.com

6.2) Layer 2 VPN

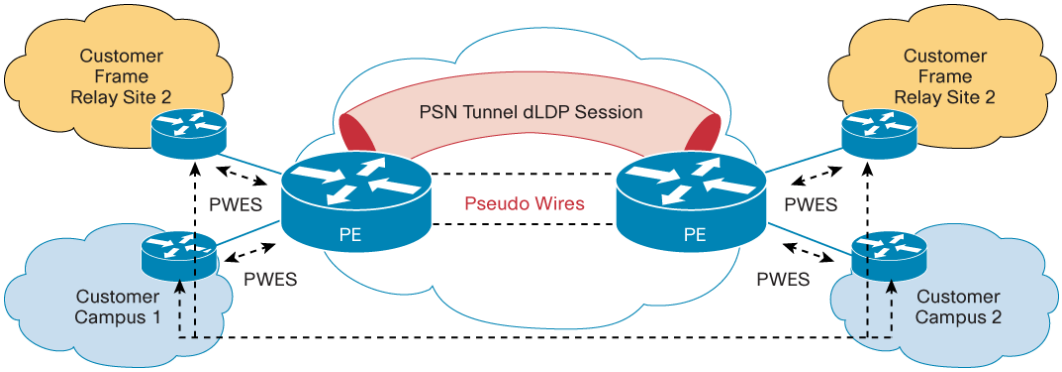
6.2.1) L2VPNs over MPLS—Any Transport over MPLS (AToM)
The fundamental benefit of an MPLS network is being able to support a multitude of applications over a single infrastructure. Any Transport over MPLS (AToM) is Cisco’s Layer 2 (L2) Virtual Private Network (VPN) over MPLS network solution. Prior to the availability of AToM, Enterprises and service providers had to build separate networks for providing L2 connectivity based on the subscriber’s existing network encapsulation. For example, a provider could be required to build separate Asynchronous Transfer Mode (ATM) and Frame Relay networks, which would result in

increased operational and capital expenses. AToM enables Enterprise and service providers to consolidate these different networks so they can save significant capital and operational expenses.

AToM also allows Enterprise and service providers the ability to expand their services portfolio without having to build a new infrastructure to accommodate L2 VPN service. With AToM, the same Provider Edge (PE) router can support both Layer 3 (L3) VPNs as well as L2 VPNs. Adding or removing VPN sites doesn't require network wide changes. Only the adjacent PE routers need provisioning. In case of connectivity problems, troubleshooting is also narrowed down to the adjacent PEs.

The MPLS L3 VPN approach was the most popular MPLS connectivity service before the advent of AToM. AToM allows subscribers to extend the reach of their network without changing any L3 network implementation or policies.

Figure 68. AToM Architecture



As illustrated in the figure above, a Pseudowire (PW) is a connection between two PE devices that connects two Pseudowire Emulated Service (PWES) end points. The PWES end points connect to the PE router using various attachment circuit types. Pseudowires are setup using directed label distribution protocol (dLDP) sessions between two PE devices. Ingress (local) PE routers allocate virtual circuit (VC) labels for new interfaces and binds to its relative (configured) Virtual Circuit ID (VCID). VC labels are exchanged with the egress (remote) PE router using dLDP label mapping messages. In the forwarding plane, VC labels are appended to the VPN traffic by the local PE router and switched through the pseudowire connection to the remote PE. The remote PE removes the VC label and sends traffic to the subscriber's network in its original encapsulation.

Benefits

- Supports current subscriber network encapsulations
- Requires no configuration changes in the core network
- Enables greater CAPEX/OPEX savings as providers can consolidate L2 and L3 services
- Additional L2 service choice for subscribers for point to point connectivity requirements
- No Layer 3 changes required in subscriber networks
- Provides like-to-like circuit support
- Accommodates like-to-unlike circuit support without any changes on the subscriber side

AToM Encapsulations

The following AToM encapsulations are supported in Cisco IOS Release 12.4(11)T:

- Ethernet—Port Mode

- Ethernet—VLAN Mode
- Frame Relay—Port Mode
- Frame Relay—DLCI—DLCI Mode

Hardware

AToM features are supported by the following platforms in Cisco IOS Software Release 12.4(11)T

Features	Routers
EoMPLS Port Mode	• Cisco 1800, 2800, 3800, 7200, and 7300 Series Routers
EoMPLS VLAN Mode	• Cisco 3800 and 7200 Series Routers
FRoMPLS	• Cisco 1800, 2600, 2800, 3700, 3800, 7200, 7300 Series Routers

Additional Information:

- http://www.cisco.com/en/US//tech/tk436/tk428/technologies_q_and_a_item09186a008009d4e3.shtml
- http://www.cisco.com/en/US/tech/tk436/tk428/technologies_q_and_a_item09186a00800949e5.shtml

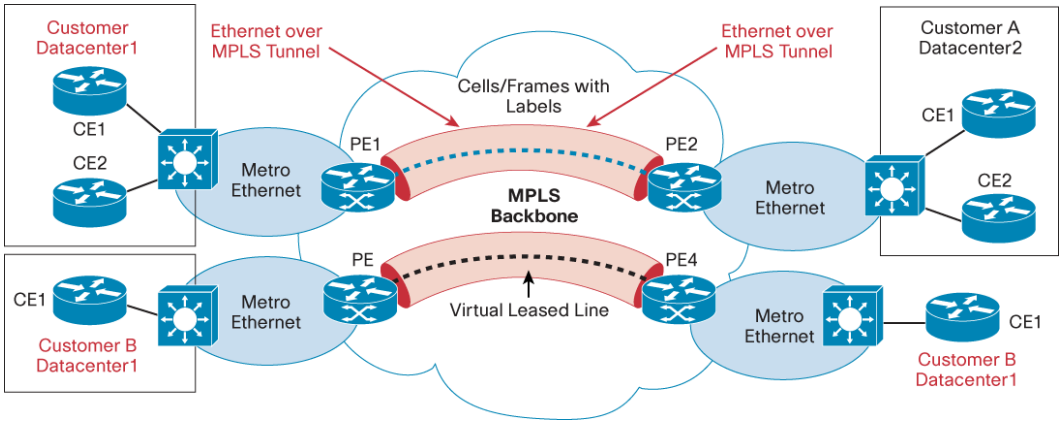
Product Management Contact: Tim McSweeney (timcswee@cisco.com)

6.2.2) Ethernet over MPLS (AToM)

EoMPLS allows Enterprises and service providers the ability to extend the reach of metro area Ethernet networks.

As shown in the figure below, it extends reachability among subscriber LAN islands by providing transport over the MPLS core network. Subscribers with VLAN mode or port mode can transparently connect into the providers' network.

Figure 69. Topology for Ethernet over MPLS

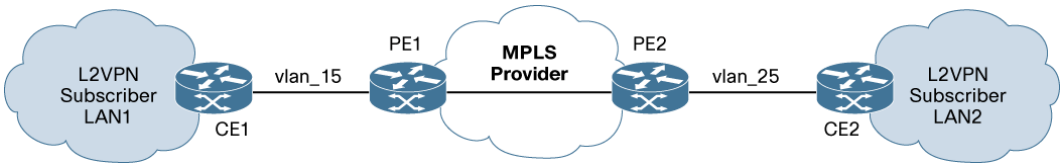


6.2.3) VLAN ID Rewrite

Today's networks are growing and evolving at a faster pace. It is critical that the new architecture facilitates and builds upon the original infrastructure, requiring minimal changes. The VLAN ID Rewrite feature allows connectivity between networks with different VLAN IDs. It allows subscribers to keep their original network parameters and VLAN model, but allow connectivity between previously isolated networks.

As described in Figure 57 VLAN ID Rewrite allows Enterprises and service providers the ability to build pseudowire (PW) connectivity between VLAN interfaces with disparate VLAN IDs. MPLS VPN subscribers can interconnect VLAN islands without changing VLAN IDs in their networks.

Figure 70. VLAN ID Rewrite Topology



6.2.4) Frame Relay over MPLS (FRoMPLS)

FRoMPLS provides leased line type of connectivity between two Frame Relay islands. Frame Relay traffic is transported over the MPLS network. Both port and Data Link Connection Identifier (DLCI) DCLI-DLCI mode are supported. A control word is used to carry additional control information. It is required for DLCI-DLCI mode but not for the port mode. When a Provider Edge (PE) router receives a Frame Relay protocol packet from a subscriber site, it removes the Frame Relay header and Frame Check Sequence (FCS) and appends the appropriate Virtual Circuit (VC) label. The removed Backward Explicit Congestion Notification (BECN), Forward Explicit Congestion Notification (FECN), Discard Eligible (DE) & Command/Response (C/R) bits are (for DLCI-DLCI mode) sent separately using a control word. In the port mode, VCs are not individually visible. The control word flag is set to zero and ignored.

6.2.5) Any Transport over MPLS (AToM) Interworking

This feature builds on AToM functionality by allowing disparate attachment circuits to be interconnected. For example, a corporation may have data centers in the campus as well as at remote Frame Relay sites that need connectivity. This will require interworking support between Ethernet and Frame Relay encapsulations. An interworking function facilitates the translation between different Layer 2 encapsulations on PE devices, making the service transparent to subscriber Customer Edge (CE) devices.

AToM interworking in Cisco IOS Software Release 12.4(11)T is supported for the following combinations:

- Ethernet Port mode to Ethernet VLAN
- Ethernet VLAN to Frame Relay

6.2.6) Multilink Frame Relay over MPLS (AToM)

Multilink Frame Relay is a logical grouping of one or more physical interfaces between two devices of the User-to-Network Interface/Network-to-Network Interface (UNI/NNI) as one single Frame Relay data link. The Multilink Frame Relay over MPLS feature enables Multilink Frame Relay switching over AToM.

A logical bundle interface is associated with physical interfaces and PWs are created between bundled interfaces. The feature works with like-to-like interfaces and disparate interfaces to support L2VPN interworking.

MFRoMPLS supports Frame Relay DLCI-DLCI mode only. Multilink Frame Relay interfaces supports Frame Relay DLCI mode to Ethernet VLAN mode interworking only.

6.2.7) Any Transport over MPLS (AToM) High Availability

It's essential to build highly available networks to minimize service disruptions due to network failures. Highly available and quickly converging networks reduce down time enabling Enterprises and service providers the ability to improve Service Level Agreements (SLAs). Subscribers benefit from better quality and application performance.

Network failures could occur due to hardware or software failures.

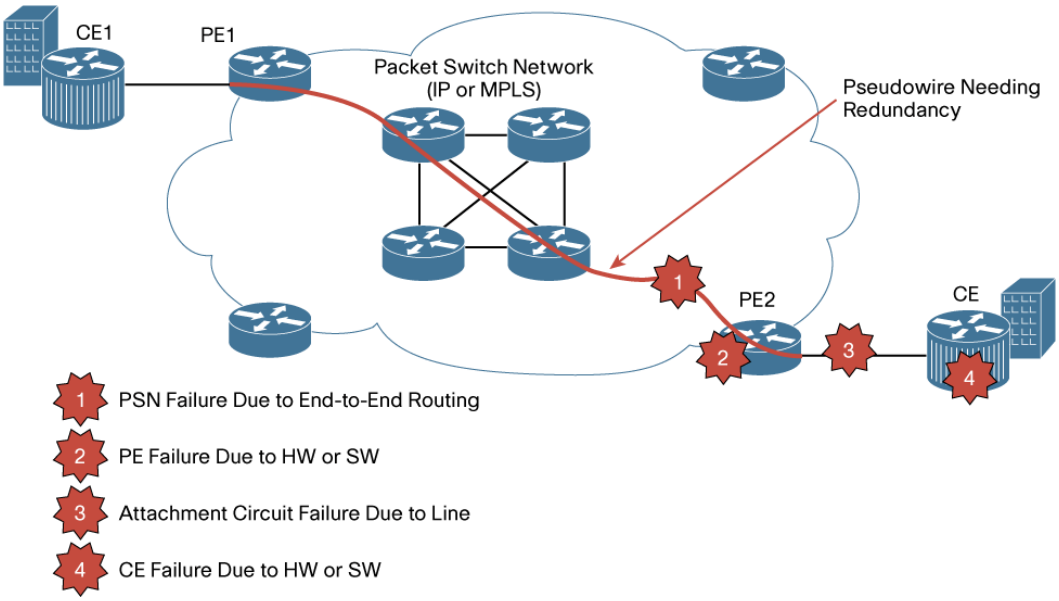
- Hardware failure: Route Processor, link, or node failures, recovery can be improved by adding backup links and devices
- Software failure: Recovery can be improved by building intelligence in network protocols

AToM Pseudowire Redundancy and AToM Graceful Restart capabilities are supported in Cisco IOS Software Release 12.4(11)T.

6.2.8) AToM Pseudowire Redundancy

It's critical to identify hot spots in the network and provide redundancy around them to help recover from possible failures. AToM Pseudowire Redundancy enables providers to set up a network that detects a failure in the network and reroutes the Layer 2 service to another endpoint that can continue to provide service.

Figure 71. AToM Pseudowire Redundancy Requirements



As illustrated in the figure above, Pseudowire Redundancy allows for recovery from a failure on either the remote Provider Edge (PE) router, or the link between the PE and CE routers.

AToM Pseudowire Redundancy Functionality

To recall, directed Label Distribution Protocol (dLDP) is used to build AToM pseudowires in an MPLS network. AToM pseudowire failure is discovered by LDP timeout. If a failure is detected in the Packet Switched Network (PSN), on a remote PE, or in remote PE-CE connection, Pseudowire End (PWE) services switches to the alternate PE or a link.

The following mechanisms are used to detect a failure:

- Label-switched Paths (LSP) Ping/Traceroute and Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV)
- Local Management Interface (LMI)
- Operation and Maintenance (OAM)

To support this functionality, at least one redundant Pseudowire Endpoint (PWE) on either side is required. Switchover to the redundant device can also be done manually. When the primary pseudowire fails, the PE router can switch to the backup pseudowire. The primary pseudowire can resume operation after the primary comes back. Dampening can also be configured to prevent switching back and forth between the primary and backup PE routers during periods of instability.

6.2.9) AToM Graceful Restart

Non Stop Forwarding/Stateful Switch Over (NSF/SSO) and Graceful Restart (GR) capabilities are supported on some Cisco platforms that have dual Route Processors (RP). NSF/SSO capability allows a device with dual route processors to continue forwarding traffic while the backup RP switches to the primary RP role and reestablishes a new control and forwarding plane state in the event of primary route processor failure.

Routers with dual RPs, NSF/SSO, and GR capabilities are called NSF/SSO capable devices.

NSF/SSO capable devices require that neighbor routers are also able to perform GR capability. Routers with GR capability only are called NSF/SSO aware devices (this would include GR supported Cisco router platforms with a single route processor only).

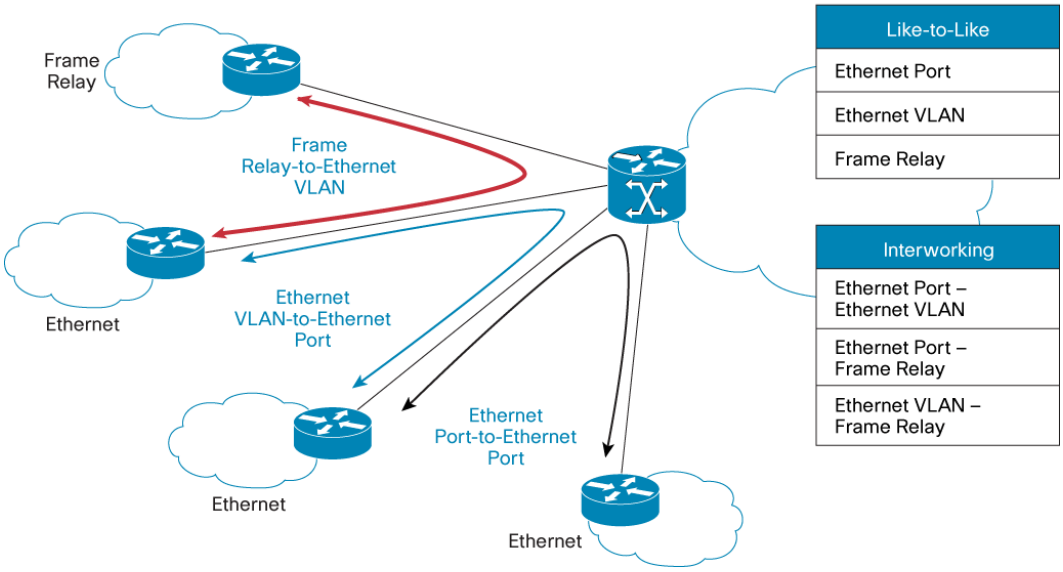
To support GR for Any Transport over MPLS (AToM), Label Distribution Protocol (LDP) was enhanced. GR capability is exchanged between capable peers during directed-LDP session setup. In the case of network disruptions, peers continue forwarding traffic using the old forwarding plane information until the new routes and label bindings are generated. This minimizes packet loss and network downtime. Once the new forwarding plane information becomes available, and network is converged, old entries are refreshed (if same), or discarded (if different).

6.2.10) Layer 2 Local Switching with Interworking

Layer 2 (L2) Local Switching allows switching L2 data between two interfaces of the same type (for example, Ethernet Port to Ethernet Port, or Frame Relay to Frame Relay) or between interfaces of different types (for example, Ethernet Port to Frame Relay) on the same router. The interfaces can be on the same line card or on two different cards. During these types of switching, the L2 address is used (not the Layer 3 address). Additionally, same-port local switching allows you to switch L2 data between two logical subinterfaces (circuits) on the same physical interface.

Figure 72. Layer 2 Local Switching with Interworking

Provides like-to-like and interworking local switching between transport protocols



Benefits

Layer 2 Local Switching supports like-to-like switching and interworking between the following protocols:

Like-to-Like

- Ethernet Port to Ethernet Port
- Ethernet VLAN to Ethernet VLAN, including same-port local switching
- Frame Relay to Frame Relay, including same-port local switching

Interworking

- Ethernet Port to Ethernet VLAN
- Ethernet Port to Frame Relay
- Ethernet VLAN to Frame Relay

Ethernet Port Mode enables the user to take all of the Ethernet on an associated interface and tunnel it across an IP core to a remote destination. Ethernet VLAN Mode enables the tunneling of individual VLANs. This method offers the granularity of controlling which of the traffic is tunneled to a given destination.

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 & 7301 Series Routers

For the latest platform support information refer to Cisco Feature Navigator at http://www.cisco.com/go/fn.

Additional Information:

Layer 2 Local Switching

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801ea88d.html

Layer 2 VPNs

http://www.cisco.com/en/US/products/ps6603/products_ios_protocol_group_home.html

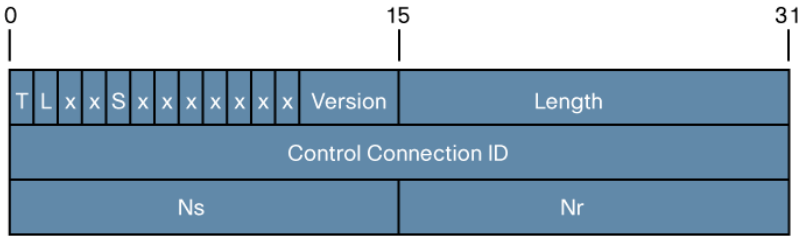
Product Management Contact: Tim McSweeney (timcswee@cisco.com)

6.2.11) Layer 2 Tunnel Protocol Version 3 (L2TPv3) Enhancements

Several enhancements for Layer 2 Tunnel Protocol Version 3 (L2TPv3) are included in Cisco IOS Release 12.4(11)T:

- L2TPv3 Control Message Hashing
- L2TPv3 Control Message Rate Limiting
- Multilink Frame Relay over L2TPv3 and AToM
- Frame Relay support for IPv6 protocol demux over L2TPv3

Figure 73. L2TP3 Control Message
Control message header format:



T – Set to 1, indicates this is a control message
L,S – For a control message, this must be set to 1 indicating the presence of Length and Sequence fields.
x – Reserved for future extensions.
Ver – Indicates which version of L2TP is in use. This field must be set to 3.
Length – Indicates the total size of the control message in octets, starting with the T bit
Control Connection ID – A locally significant ID, it will the peer's ID not it's own.

Benefits

- L2TPv3 Control Message Hashing adds hashing to control messages as per extensions specified in the latest versions of the L2TPv3 draft specification.
- L2TPv3 Control Message Rate Limiting safeguards against one type of denial of service attack by limiting the processing rate of L2TPv3 control messages.
- Multilink Frame Relay over L2TPv3 and AToM enhances existing Frame Relay capabilities for pseudowires.
- Frame Relay support for IPv6 protocol demux over L2TPv3 allows Enterprises and service providers the capability of providing both IPv4 and IPv6 services to a CE router on single FR PVC even though there is no IPv6 stack on the PE router connected to a customer.

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 & 7301 Series Routers

For the latest platform support information refer to Cisco Feature Navigator at http://www.cisco.com/go/fn.

Additional Information:

L2TPv3 Enables Layer 2 Services for IP Networks

http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns155/networking_solutions_white_paper09186a008017fa6e.shtml

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

6.3) Multiprotocol Label Switching Management

6.3.1) Cisco IOS Multiprotocol Label Switching Embedded Management
Cisco IOS Multiprotocol Label Switching (MPLS) embedded management offers standards-based management capabilities for IP/MPLS networks, including Pseudowire (PW) connectivity supporting Layer 2 VPN services. In addition to RFC4379-based MPLS OAM capabilities for MPLS core networks, Cisco's industry leading MPLS management feature portfolio now also offers network operators detailed Layer 2 MPLS VPN resource monitoring and connectivity troubleshooting capabilities, which include the following MPLS Pseudowire (PW) MIBs and Layer 2 VPN MPLS OAM features:

MPLS MIBs:

- PW-STD-MIB (based on draft-ietf-pwe3-pw-mib-00.txt)
- PW-MPLS-STD-MIB (based on draft-ietf-pwe3-pw-mpls-mib-00.txt)
- PW-ENET-STD-MIB: (based on draft-ietf-pwe3-enet-mib-00.txt)
- PW-TC-STD-MIB (based on draft-ietf-pwe3-pw-tc-mib-00.txt)

MPLS OAM:

- MPLS LSP Ping for L2 VPN Pseudowires (PWs) via Virtual Circuit Connection Verification (VCCV)

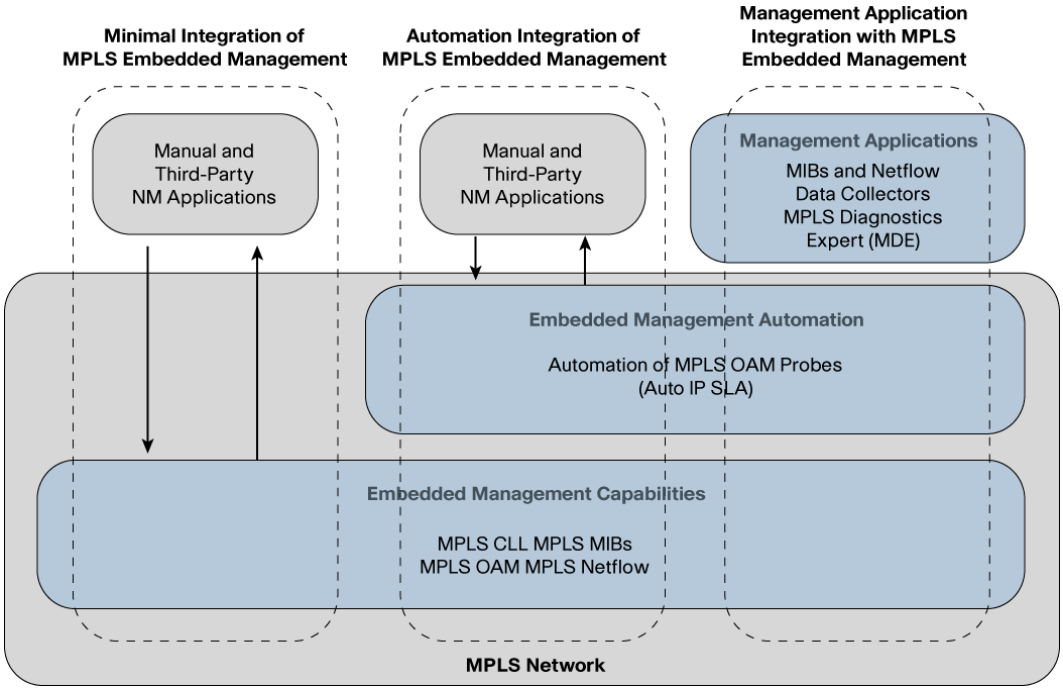
The embedded management capabilities for MPLS can be used in various usage scenarios ranging from manual CLI-based trouble shooting to fully automated trouble shooting systems.

Benefits

Key benefits of Cisco's MPLS embedded management and OAM features include the following:

- **Enhanced MPLS resource monitoring:** MPLS MIB modules provide standard SNMP access to a wide variety of MPLS-specific resources supported on Label Switched Routers (LSR), including MPLS label forwarding and LDP session information. Existing SNMP-based management applications can be configured to retrieve and collect MPLS-specific management information via the new MPLS MIB modules.
- **Increases operational efficiency:** MPLS OAM tools, such as LSP Ping and LSP Trace, enable fast detection and isolation of complex MPLS connectivity problems, which improves trouble resolution time and will help reduce network downtime.

Figure 74. Cisco IOS MPLS Management Framework



Hardware

Routers	• Cisco 2800 and 3800 Series Routers • Cisco 2600 and 3600 Series Routers • Cisco 7200 Series Router

Additional Information:

MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV

http://www.cisco.com/en/US/products/ps6566/products_feature_guide09186a008063d009.html

Product Management Contact: Harmen van der Linde (havander@cisco.com)

6.4) IP Services

6.4.1) DHCP Relay per interface VPN ID support
The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. The DHCP relay agent information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent.

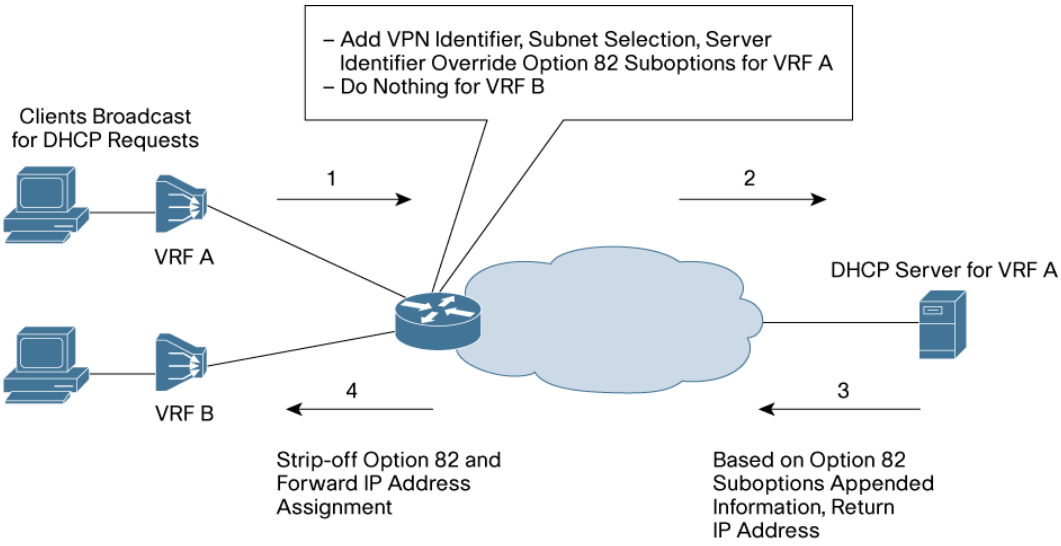
In some environments, a relay agent resides in a network element that also has access to one or more Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). A DHCP server that wants to offer service to DHCP clients on those different VPNs needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP Relay VPN ID Support feature allows the relay agent to forward this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

Addressing the ISP needs, the above mentioned capability can now be configured at an interface level, dramatically increasing the versatility of the solution. Typically it enables the aggregation of several DHCP services with different MPLS related option 82 suboptions support on the same router.

Figure 75. FDHCP Relay Per interface VPN ID support



Benefits

- The DHCP Relay VPN ID Support feature allows for better router resource utilization by aggregating several service types on the same router.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804412bf.html - wp1095795

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.4.2) DHCP Class Support for Option 60, 77, 124, 125

The DHCP class mechanism applies to the Relay and Server DHCP function. On the server side, DHCP classes can be defined so IP addresses are allocated based on the content on an option present in the DHCP request. On the relay side, the DHCP server address to forward to can be selected based on the content of an option present in the relayed DHCP packet.

The DHCP class mechanisms also supports options 60, 77, 124 and 125, so decisions can also be made based on content for those DHCP options.

Benefits

The DHCP relay supports service rich client environments where each service is managed by different DHCP servers. Different ranges of IP addresses of a pool can be dedicated to a specific application based on the content of a wide range of options.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series Routers

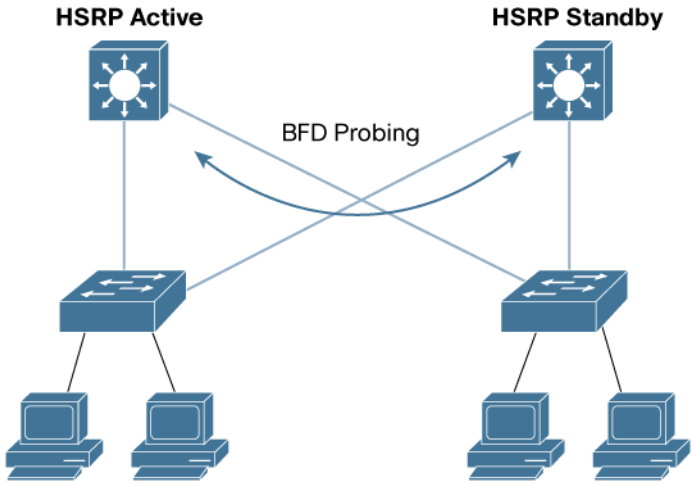
Additional Information:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804419eb.html - wp1097444

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.4.3) Hot Standby Routing Protocol Bidirectional Forwarding Detection Peering

Bidirectional Forwarding Detection (BFD) is introduced in the Hot Standby Routing Protocol (HSRP) group member health monitoring system. Previously group member monitoring relied exclusively on HSRP multicast message. These messages are relatively large, hence CPU consuming to produce and check. In architectures where a single interface hosts hundreds of groups there is a need for a lighter protocol. BFD addresses this issue and offers sub second health monitoring at a relatively low CPU impact.

Figure 76. HSRP BFD Peering Topology



Benefits

- HSRP BFD peering allows for quicker and more efficient failure detection of HSRP group members.

Hardware

Routers	• Cisco 7200 Series Routers

Additional Information:

http://www.cisco.com/en/US/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.4.4.) Enhanced Object Tracking support for Mobile IP, PDSN or GGSN

The Enhanced Object Tracking (EOT) feature is a separate standalone tracking process that can be used by any other process as well as any First Hop Routing Protocol. A client process, such as HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP), can register its interest in tracking objects and then be notified when the tracked object changes state.

A new capability is added to EOT so it can monitor the presence of the Mobile IP, Packet Data Serving Node (PDSN), or Cisco® Gateway GPRS Support Node (GGSN) traffic on a router for Mobile Wireless application.

When a redundant pair of Home Agent (HA) routers running HSRP between them loses connectivity, both HSRP nodes go active. Once the connectivity is restored between the two nodes, there is a need for a graceful way to restore proper HSRP states without losing HA bindings. During the time of no connectivity, one of the nodes will continue to process Mobile IP (or GGSN or PDSN) traffic while the other will not. The node which continues to process traffic needs to remain active once connectivity is restored. To achieve that, the priority of the HSRP group member which does not process Home Agent traffic is reduced. This ensures that this node will go standby after the connectivity is restored. Then the normal Home Agent state synchronization will get all bindings back into the inactive node and depending on the preempt configuration, it may switchover again. This ensures that there is no Mobile IP (or GGSN or PDSN) bindings lost.

Benefits

Enhanced Object Tracking support for Mobile IP, PDSN or GGSN tracks connectivity failures between redundant mobile gateway pairs without losing bindings or interrupting traffic processing.

Hardware

Routers	• Cisco 7200 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide_chapter09186a00804237d1.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.4.5) Show and Clear Commands for Cisco IOS Sockets

Routers and switches, like most computing platforms, have applications that use IP sockets. The Cisco IOS infrastructure provides these socket services to the processes or tasks. As the number of services and network applications grows there is increased need for more detailed information to be available pertaining to the application's use of the underlying software infrastructure. New CLI commands have been added to display and control IP sockets on a per-process basis.

These commands are useful when:

- Examining application and network usage
- Ensuring proper software behavior during testing

- Debugging problems

Some examples and use case scenarios could be:

- A voice or video application is using the socket library for voice calls. According to the current number of calls, there is still capacity for more sockets. However no more sockets can be opened. The ‘show’ command would help in this case, to find out if the socket space is indeed exhausted or whether there are some unused sockets.
- An application is waiting for a particular socket event to happen. The TCP segment was seen, but the application was never awakened. Is the event indeed being watched or has the socket library failed to wake up the application? The ‘show’ command would be useful to display the list of events being watched.
- There might be some need to forcibly close all of the sockets for a particular process. The ‘clear’ command would be useful in this case, which will not only close the sockets but will also close the underlying TCP connection or SCTP association.

Benefits

- **More Insight into Network Operation:** The user has more visibility into the inner working of Cisco IOS.
- **Increased Visibility and Troubleshooting Capabilities:** The commands provide more visibility and troubleshooting capabilities and may allow for recovery in case of some types of error conditions.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series Routers

Product Management Contact: Rick Williams (rwill@cisco.com)

6.4.6) Cisco Express Forwarding (CEF) L4 Port Load Balancing

Cisco Express Forwarding (CEF) load balancing allows you to optimize resources by distributing traffic over multiple paths. Load balancing is based on a combination of source and destination packet information such as:

- per-destination
- per-packet

Cisco IOS Software Release 12.4(11)T adds the capability to perform load balancing based on source and destination Layer 4 port numbers on software based routers. It is similar to the capability already offered on Cisco Catalyst 4500 and 6500 Series hardware.

Benefits

Improves load balancing when IP addresses alone cannot provide optimal traffic load balancing.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 3800, 7200, 7301, AS5000, 7200 7301 series Routers, MWR, MWAM

Additional Information:

http://www.cisco.com/en/US/products/ps6441/prod_literature.html

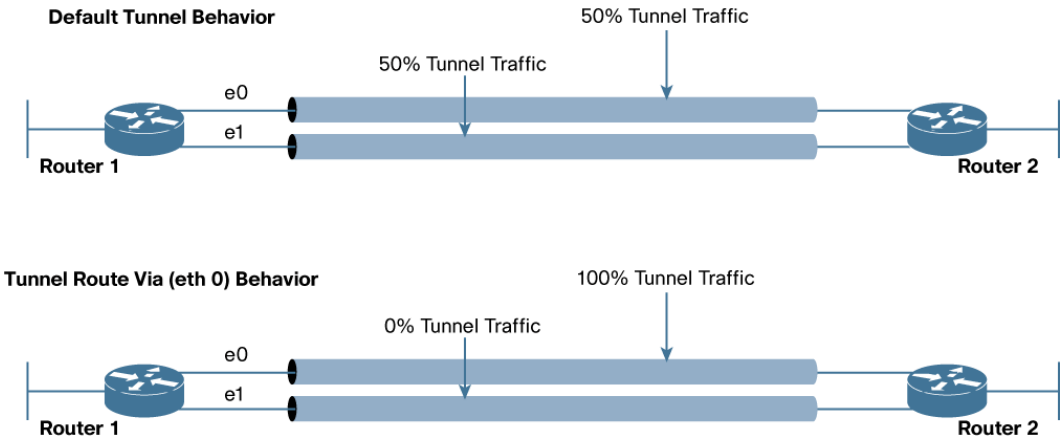
Product Management Contact: Patrick Grossetete (pgrosset@cisco.com)

6.4.7) Tunnel Source Address Selection

Tunnel Source Address Selection feature allows a tunnel transport to be routed via a subset of the routing table. When there are equal cost routes to a tunnel destination, normal tunnel transport behavior is to load balance the traffic across each available route. With the Tunnel Source Address Selection feature an interface can be specified and the tunnel transport will attempt to use routes via that interface.

The Tunnel Source Address Selection feature is not the same as an implementation of policy based routing for the tunnel transport, since the Tunnel Source Address Selection feature will only forward traffic using a subset of the routing table. This means the Tunnel Source Address Selection feature cannot introduce routing loops into the network.

Figure 77. Tunnel Source Address Selection



Benefits

This feature benefits customers running tunnel configurations where there are multiple routes or paths to the tunnel destination (examples: DMVPN or Mobile IP network topologies).

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 3800, 7200, 7301, AS5000, 7200, 7301 Series Routers, MWR, MWAM

Additional Information: http://www.cisco.com/en/US/products/ps6441/prod_literature.html

Product Management Contact: Patrick Grossetete (pgrosset@cisco.com)

6.4.8) Radius Server Load Balancing

The RADIUS server load balancing feature is an enhancement over the existing mechanism of sending Authentication, Authorization, and Accounting (AAA) authentication and accounting transactions to single server by distributing them across servers in a server group. These servers can then share the transaction load, resulting in faster responses to incoming requests by optimally using available servers.

Cisco IOS AAA network security services provide the primary framework to set up access control on a router or access server. A Cisco IOS AAA client resides on a router or Network Access Server (NAS) and can perform all AAA functions remotely via an external server using RADIUS protocol.

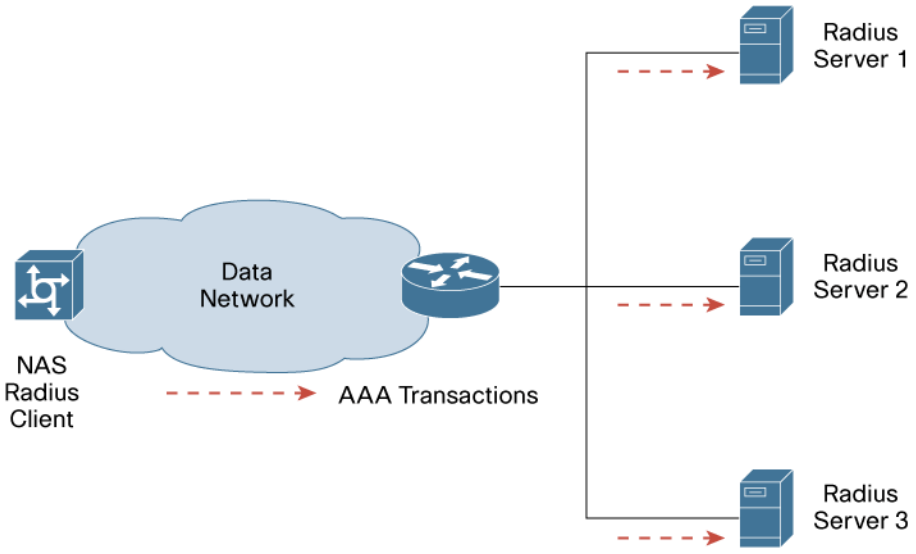
The protocol carries authentication, authorization and configuration information between a NAS and a RADIUS authentication server.

The AAA Radius Server Load Balancing feature allows an AAA client to concurrently use multiple AAA servers by grouping AAA transactions to a batch and assigning the batch to a server with the least number of outstanding transactions.

Key benefits to use RADIUS server load balancing includes:

- Improved response time to incoming requests by optimally using available servers
- Improved system throughput by using multiple servers concurrently

Figure 78. Radius Server Load Balancing Topology



Benefits

- **Performance Improvement:** By distributing AAA transactions across servers in a server group, improved response time to incoming requests as well as improved system throughput can be achieved.

Hardware

Routers	• Cisco 7200 Series Routers

Product Management Contact: Ted Qian (tqian@cisco.com)

6.5) IP Mobility and Wireless

6.5.1) Mobile IPv6 Authentication Option Support

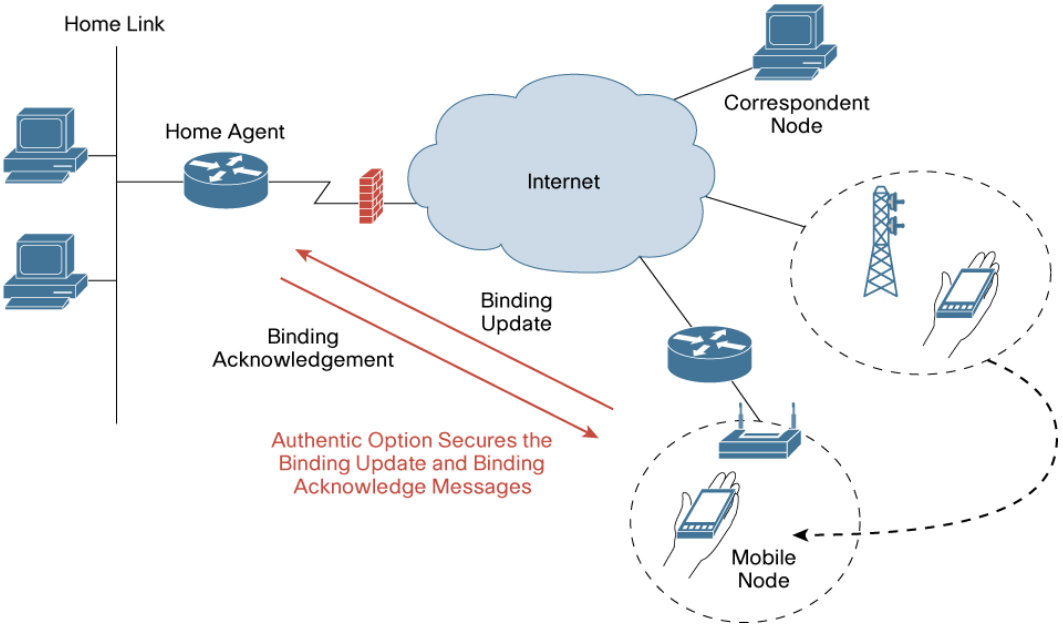
Mobile IP (both IPv6 and IPv4) provides mobile nodes with the ability to retain the same IP address and maintain uninterrupted network and application connectivity while traveling across networks. Before offering this ability, Mobile IP networks need to authenticate mobile nodes. This ensures the request of the mobility service is coming from an authorized user as well as ensuring traffic is forwarded to the right mobile node after a movement. In Mobile IPv4, a shared-key based authentication method is used between a mobile node and a home agent. The method secures control messages between the mobile node and home agent to establish the services.

The Mobile IPv6 Authentication Option Support feature provides the same shared-key approach to authenticate a Mobile IPv6 enabled node. The Authentication Option mechanism secures “Binding Update” and “Binding Acknowledge” messages exchanged between an IPv6 mobile node and an IPv6 home agent.

Mobile IPv6 Authentication Option Support is a relatively lightweight authentication mechanism as compare to the IPsec approach, therefore requiring less router CPU processing power and generating less control message overhead. The applicability of using the lightweight authentication approach includes when not all mobile nodes are Internet Key Exchange Version 2 (IKEv2) capable, conserving processing power on mobile nodes is desirable, and minimal network bandwidth consumption between mobile nodes and home agents is preferred.

Mobile IPv6 Authentication Option Support is compliant with RFC 4285.

Figure 79. Mobile IPv6 Authentication Option Support



Benefits

Secure mobility service offering by protecting signaling message between a mobile node and a home agent

Restriction

The current implementation will only support local authentication and will not support Mobile IP Extensions (MN-AAA) authentication option.

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7200, 7300, 7400 Series Routers

Product Management Contact: Richard Shao (rshao@cisco.com)

6.5.2) Mobile IPv6 Network Access Identifier (NAI) Support

Mobile IPv6 Network Access Identifier (NAI) support allows a mobile node to be identified by using a network access identifier instead of an IP address (home address). The NAI is used in

conjunction with Mobile IPv6 Authentication Option Support feature as an identifier during the authentication processes.

The NAI is a character string that can be a unique identifier (username@realm) or a group identifier (realm). The Mobile IPv6 NAI support is compliant with RFC4283.

Benefits

- Mobile IPv6 NAI support expands Mobile IPv6 authentication options beyond the IP address itself, increasing flexibility.

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7200, 7300, 7400 Series Routers

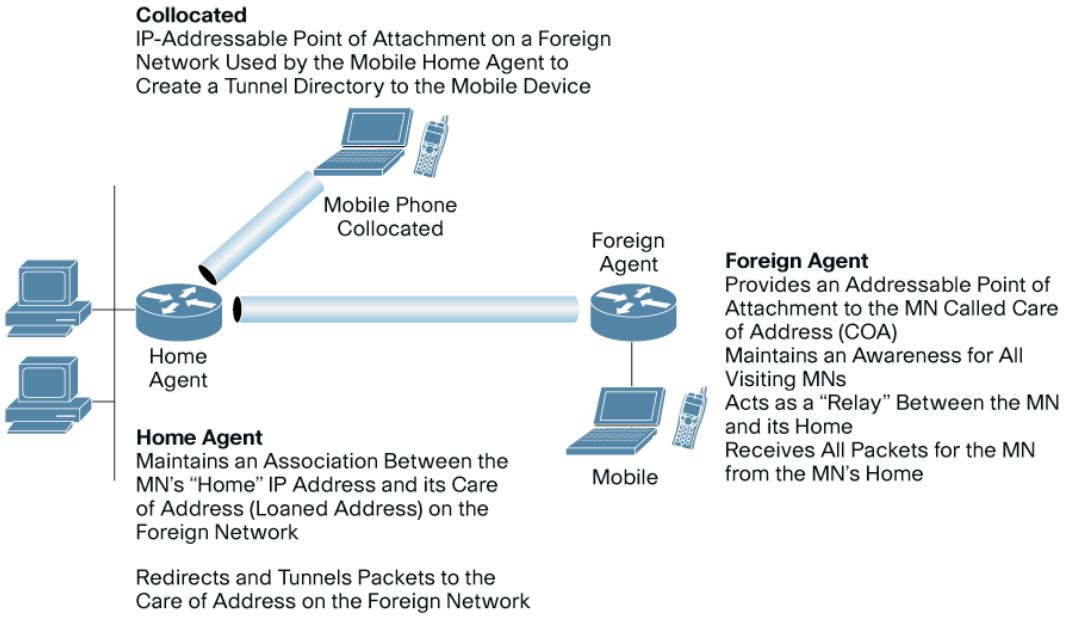
Product Management Contact: Richard Shao (rshao@cisco.com)

6.5.3) Cisco Mobile Wireless Home Agent Release 3.0

Mobile wireless data providers require features and enhanced capacity and performance to meet the demands of their customers and applications. The Cisco Mobile Wireless Home Agent product provides such features on platforms that meet the capacity needs. R2.x and R3.x introduced new features and enhancements in the areas of security, resource management, and user redirection.

Today's networking environment offers a multitude of different access technologies in wireless and wireline infrastructure. Mobile IP technology makes access technologies transparent and allows a constant connection for users, independent of their location and the type of infrastructure. The Cisco® Mobile Wireless Home Agent serves as an anchor point for subscribers, providing easy, secure roaming with Quality-of-Service (QoS) capabilities to optimize the mobile user experience. The Cisco Mobile Wireless Home Agent works in conjunction with a foreign agent and mobile node to provide an efficient Mobile IP solution. Figure 67 shows a basic topology.

Figure 80. Mobile Wireless Home Agent Release 3.0 Topology



The Cisco Mobile Wireless Home Agent maintains mobile user registrations—through a foreign agent or in collocated mode (CCOA)—and tunnels packets destined for the mobile device to the

foreign agent. It supports reverse tunneling, and can securely tunnel packets to the foreign agent using IP Security (IPsec). Additionally, the Cisco Mobile Wireless Home Agent supports dynamic and static home address assignment—for both public and private addresses—for the mobile device. Home address assignment can be from address pools configured either locally or remotely using Dynamic Host Configuration Protocol (DHCP) server access, or the Authentication, Authorization, and Accounting (AAA) server, or an On-Demand Address Pool (ODAP).

The Cisco Mobile Wireless Home Agent is the anchor point for mobile terminals for which mobile or proxy mobile services are provided. Traffic sent to the terminal is routed using the Home Agent. With reverse tunneling, traffic from the terminal is also routed through the Cisco Mobile Wireless Home Agent. Unique features such as Home-Agent redundancy and load balancing provide a high level of availability and reliability, allowing geographical dispersion while maintaining accounting integrity. Another unique feature, Network Address Translation (NAT) traversal, allows the Cisco Home Agent to be used as an anchor point across many access technologies. This allows users to transparently roam across different access networks while retaining a constant connection and addressability.

Key Features and Benefits

- **Accounting:** Provides robust accounting on the Home Agent, including packet count, byte count and additional accounting records.
- **Virtualized Home Agent:** Provides the ability to virtualize a Home Agent for full VPN service type, supporting multiple VPNs on the same Home Agent and allows address overlapping. This can reduce the amount of equipment needed, simplify administration, and help with IPv4 address scarcity.
- **Mobile user ACL:** Per-user access list information can be retrieved from AAA to fine tune access to network resources and services.
- **Hotlining:** This offers redirection of upstream user traffic, so users can be dynamically redirected during a session. This is useful for monitoring or security purposes.
- **IP Reachability and DNS Server Address Assignment:** These IS-835D compliant features enhance the user experience and services by facilitating user-to-user communication.

Hardware

Routers	• Cisco 7206VXR Series Router • Cisco 7600 Series Router (requires MWAM module)
Switches	• Cisco Catalyst 6500 Series (requires MWAM module)

Considerations

- The Mobile Wireless Home Agent requires a special software image to utilize the Mobile Wireless specific features. The image is an –h1is image. This image is only available on the above noted platforms.
- The Mobile Wireless Home Agent software image is available only with the purchase of the proper license. Please see the following webpage for ordering information: http://www.cisco.com/en/US/products/sw/wirelssw/ps4341/prod_bulletin0900aecd803dba07.html

- The Mobile Wireless Home Agent software image is installed and supported on the Multiprocessor WAN Application Module (MWAM) for the Cisco 7600 Series Router and the Cisco Catalyst 6500 Series Switch.

Standards Compliance

Complies with 3GPP2 TSG-P TSG-X (TIA/EIA/IS-835) and IETF RFCs.

Additional Information: http://www.cisco.com/en/US/products/ps5940/index.html

Product Management Contact: Tamara Anderson (tmeskuna@cisco.com)

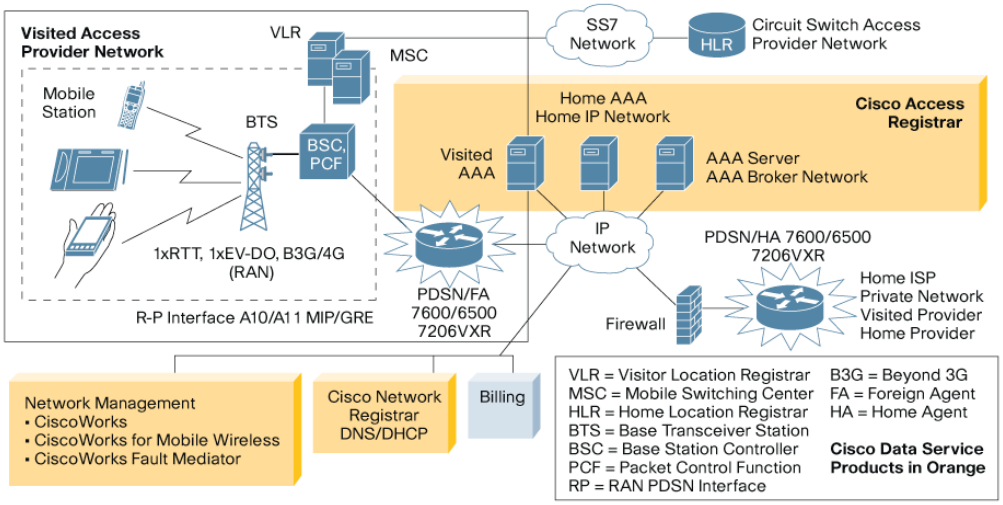
6.5.4) Cisco Packet Data Serving Node (PDSN) Release 3.0

The Cisco® Packet Data Serving Node (PDSN) helps mobile operators offer Code Division Multiple Access 2000 (CDMA2000) packet data services. Specifically, it provides gateway services between third-generation (3G) networks such as Code Division Multiple Access 2000 (CDMA2000) 1xRTT and 1xEVDO, and fourth-generation (4G) networks such as HC-SCDMA Radio Access Networks (RANs), and between IPv4 and v6 networks. The Cisco PDSN supports mobile-station (single stack or dual stack) access to the Internet, corporate intranets (through secure VPNs), and Wireless Application Protocol (WAP) servers. Standards-compliant, Cisco PDSN uses proven Cisco Systems® hardware and software, and offers several features to enhance availability, scalability, and security.

The Cisco PDSN acts as an access gateway and provides Simple IP and Mobile IP access, foreign-agent support, and packet transport for virtual private networking. It acts as a client for Authentication, Authorization, and Accounting (AAA) servers, and also enables prepaid billing services. Standalone PDSNs can also be logically tied together in a clustering architecture to provide scalability, redundancy, load sharing, and more. The figure below illustrates how the Cisco PDSN fits in a CDMA network.

Cisco Packet Data Serving Node Release 3.0 introduces new features and enhancements in the areas of resource management, redundancy, and IPv6.

Figure 81. CDMA2000 Network with a Cisco PDSN and Other Required Components for Packet Data Services



Cisco PDSN supports all required standards, including the Third-Generation Partnership Project 1 Technical Specification Group P and X (3GPP2 TSG-P, TSG-X) standard and the Wireless IP

Network Standard (also known as TIA/EIA/IS-835), which defines the overall structure of a CDMA2000 network. It includes features such as enhanced Mobile IP, carrier-class accounting, compression, security, and authentication. Cisco PDSN also supports 3GPP2 TSG-A, the Interoperability Specification for CDMA2000 Access Network Interfaces (also known as TIA/EIA/IS-2001). The 3GPP2 TSG-A standard focuses on the RAN and the interfaces between RAN and the PDSN.

Key Features and Benefits

- **Resource Management:** Through use of Packet of Disconnect (PoD) and/or Resource Revocation features, this helps enable faster resource release, enabling a provider to have greater control and to take action toward specific users.
- **Session Redundancy:** This provides support for transparent and automatic failover of the Cisco PDSN application and PPP protocol session for Simple IP and Mobile IP calls. This avoids session disruption and increases availability and reliability, maximizing the end user experience.
- **Simple IPv6:** This increases flexibility for providers. This helps introduction of IPv6 users, and solves problems of IPv4 address space.
- **ACL per user:** Per-user access list information can be retrieved from AAA to fine tune access to network resource and services.
- **Always-On Feature:** This helps enable Push-to-Talk (PTT) services.
- **Advanced debugging:** The enhanced ability to debug by MNID/username simplifies troubleshooting and user debugging.

Hardware

Routers	• Cisco 7206VXR Series Router • Cisco 7600 Series Router (requires MWAM module)
Switches	• Cisco Catalyst 6500 Series (requires MWAM module)

Considerations

- The PDSN software image is available only with purchase of the proper license. Refer to Cisco Packet Data Serving Node web page for more information: http://www.cisco.com/en/US/products/sw/wirelssw/ps4341/index.html
- The PDSN software image is required to be loaded on a Multiprocessor WAN Application Module (MWAM) in the Cisco 7600 Series Router and the Cisco Catalyst 6500 Series Switch.

Standards Compliance

Complies with 3GPP2 TSG-P, TSG-X (TIA/EIA/IS-835), and 3GPP2 TSG-A (TIA/EIA/IS-2001) standards.

Additional Information: http://www.cisco.com/en/US/products/sw/wirelssw/ps4341/index.html

Product Management Contact: Tamara Anderson (tmeskuna@cisco.com)

6.6) Quality of Service

6.6.1) ATM QoS Features for the Asymmetric Digital Subscriber Line (ADSL2/ADSL2+) High-Speed WAN Interface Card (HWIC-1ADSL) for Cisco 1800, 2800, and 3800 Series Routers

This is an incremental set of Quality of Service (QoS) features that allow customers to deploy differentiated services on ADSL/ADSL2/ADSL2+ lines with the HWIC-1ADSL WAN Interface Card (WIC) on the modular Cisco 1800, 2800 and 3800 Series Integrated Services Routers. This complements the rich set of IP and ATM QoS features already supported on these platforms with an ADSL2+ interface. These additional features allow users, applications, and traffic to get appropriate Service Level Agreements (SLA) as well as provide Enterprises and service providers with opportunities for incremental revenue generation through differentiated services.

Today, QoS is an important infrastructure component that facilitates the widespread adoption of broadband in commercial and Enterprise branch office environments. In response to customer requirements and pressures, network operators and network service providers are finding it critical to offer QoS features for Digital Subscriber Line (DSL) deployments. Cisco IOS Software Release 12.4(11)T enables customers with ADSL2+ deployments the ability to support critical features such as:

- Support for Unspecified Bit Rate Plus (UBR+) class of service
- Multi-queue support
- ATM oversubscription for DSL

UBR+ Support: Traditionally the Unspecified Bit Rate (UBR) service class has been used for data communications applications such as file transfer and email. UBR is a best effort service and is the lowest class of service in the ATM service class hierarchy. There are no guarantees to the actual bandwidth allowed. Therefore, UBR Virtual Circuits (VCs) are susceptible to a large number of cell drops or a high cell transfer delay as cells move from the source to the destination. Unspecified bit rate plus (UBR+) is a special ATM service class designed to provide a minimum bandwidth guarantee. With UBR+, the ADSL ATM interface has the ability to assure a minimum as well as maximum bandwidth on the line. As a result, the user can have some assurance of a range of bandwidth values necessary for QoS.

Multi-queue Support: Today's access networks are increasingly carrying voice, video and data traffic over physical lines. It is crucial for the access routers to honor latency, jitter and other requirements for delay sensitive traffic. The multi-queue feature provides for two separate hardware queues on the access router for every Permanent Virtual Circuit (PVC) in the system, one to carry high priority and the other to carry regular (data) traffic.

ATM Oversubscription for DSL: Today, more and more business customers demand high availability in the networks. In many cases they use primary as well as secondary WAN interfaces for 24x7 connectivity. In ADSL networks, loss of connectivity may arise when the ADSL line is down or when the PVC is non-functional because of equipment failure in core networks. In order to overcome the challenges posed by the latter case, Enterprises and service providers are increasingly deploying primary and backup PVCs on the ADSL interface. However with a backup PVC, the configurable bandwidth requirement of all the PVCs in the system may be greater than the ADSL line rate. This may cause PVCs that need minimum bandwidth guarantees to be downgraded to a UBR class of service. The ATM Oversubscription feature allows the operator to configure oversubscription on the ADSL interface up to a defined bandwidth. The operator can configure variable bit rate (VBR) and UBR+ service classes for PVC connections with a sum of Sustainable Cell Rates (SCRs) greater than the line rate. Resource limitations on Cisco xDSL interfaces require a way to configure bandwidth oversubscription up to a defined bandwidth (a finite oversubscription of bandwidth by a factor of two).

Benefits

- **Improved QoS features for ADSL/ADSL2/ADSL2+ interfaces:** These QoS features make the HWIC-1ADSL feature compatible with other Cisco xDSL interfaces. The features allow customizable traffic shaping, prioritization, and increased resiliency of the ATM interface for the ADSL access network. This makes end-to-end QoS possible for solutions that involve the Cisco modular access routers with an ADSL interface provided by the HWIC-1ADSL card.
- **Incremental revenue opportunities:** The features allow network providers the flexibility of offering differentiated services to customers that can generate incremental revenue opportunities.

Hardware

Routers	• Cisco 1800, 2800, 3800 Series Routers

Product Management Contact: Sanjoy Dey (sdey@cisco.com)

6.7) Voice

6.7.1) Enhancements to Cisco IOS Session Border Controller (SBC)- Cisco Multiservice IP-to-IP Gateway

The Cisco® Multiservice IP-to-IP Gateway is a Session Border Controller (SBC) that interconnects independent voice over IP (VoIP) networks for data, voice, and video transport. SBCs are critical components for scaling networks from islands within a single customer network to an end-to-end IP community. The Cisco Multiservice IP-to-IP Gateway is an integrated Cisco IOS Software application that runs on the Cisco 2800 Series and 3800 Series Integrated Services Routers (ISRs) and the Cisco 2600XM Series, 3700 Series, 7200 Series, 7301 Router and Cisco Universal Gateways AS5350XM and AS5400XM platforms. Today, the Cisco IP-to-IP Gateway is used by Enterprises, service providers, and commercial customers to interconnect Session Initiation Protocol (SIP) and H.323 voice and video networks.

Cisco IOS Software helps enable the simultaneous operation of the following:

- Cisco Multiservice IP-to-IP Gateway
- Cisco IOS H.323 Gatekeeper
- Cisco Time Division Multiplexing (TDM) Gateway

Several new features have been introduced in Release 12.4(11)T for Session Border Controller functionality:

1. H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC) Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261.
2. New H.323-to-H.323 features offered in this release on the Cisco 2800, 3800, 5350XM and 5400XM include: RFC 2833 to G.711 Inband DTMF
3. New H.323-to-SIP features offered in this release on the Cisco 2800, 3800, 5350XM and 5400XM include:
   - iLBC Codec
   - Dual Tone Multifrequency (DTMF) Relay

RFC 2833 to G.711 Inband DTMF

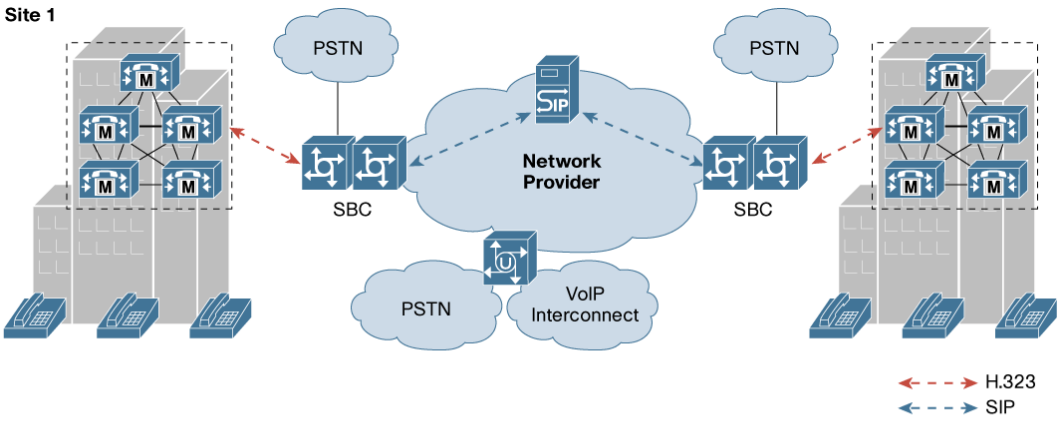
SIP Notify to SIP Notify

RTP Named Telephone Events (RTP-NTE) to RTP-NTE

- Voice Extensible Markup Language (VXML) standard 3.x support
- VXML support with SIP NOTIFY DTMF
- Tool Control Language (TCL) Scripts Interactive Voice Response (IVR) support with SIP NOTIFY DTMF
- Support H.323-to-SIP Supplementary services for Cisco Unified CallManager with Media Termination Points (MTP) on the H.323 Trunk.

4. New SIP-to-SIP features offered in this release on the Cisco 2800, 3800, 5350XM and 5400XM include:
   - iLBC Codec
   - RFC 2833 to G.711 Inband DTMF
   - IP to SIP Supplementary Feature Interworking with Media Flow Around

Figure 82. Cisco Multiservice IP-to-IP Gateway
Session Border Controller (SBC) Enhancements



- Interconnects independent Voice over IP (VoIP) networks for data, voice, and video transport

  Critical component for scaling network islands within a single customer network to an end-to-end IP community

- Release 12.4(11)T introduces support for H.323 to Session Initiation Protocol (SIP) supplementary services for Cisco Unified CallManager (CUCM) with media termination points (MTP) on the H.323 trunk

  Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261

Benefits

VoIP interconnects are on the rise, and for Cisco Unified CallManager (CUCM) Version 4.1.3 and above, the Cisco Multiservice IP-to-IP Gateway provides an elegant way of doing SIP trunks to providers maintaining the rich CUCM H.323 Trunk.

With Release 12.4(11)T, Cisco Multiservice IP-to-IP Gateway will support H.323-to-SIP Supplementary services for Cisco Unified CallManager with MTP on the H.323 Trunk.

Hardware

Routers	• Cisco 2600XMs, 2691,2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers
Universal Gateways and Access Servers	• Cisco AS5400XM Series

Considerations

1. RFC 2833 to G.711 Inband DTMF requires Digital Signal Processors (DSPs) on the Cisco Multiservice IP-to-IP Gateway
2. 323-to-SIP Supplementary services for Cisco Unified CallManager require a software MTP on the CUCM's H.323 Trunk.

Additional Information:
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a0080409b6d.html

Product Management Contacts:

Jayesh Chokshi (jayesh@cisco.com)

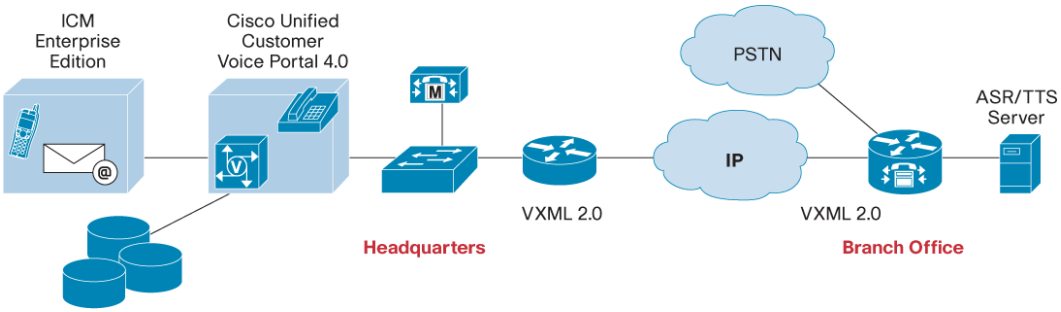
Darryl Sladden (dsladden@cisco.com)

6.7.2) VoiceXML Browser Update—Support of W3C VoiceXML Forum Standard VXML 2.0
VoiceXML is an XML-based language that provides the **Benefits** of a Web-based development environment and service delivery to Interactive Voice Response (IVR) applications and voice enabled Web browsers. Cisco IOS voice gateways provide VoiceXML browser services when used in conjunction with a VoiceXML server, like the Cisco Unified Customer Voice Portal (CVP). The Cisco IOS VoiceXML browser has been updated to conform to the VoiceXML 2.0 standard and is now certified with the VoiceXML Forum.

Features

- Supported on a wide variety of Cisco IOS voice gateway platforms delivering a broad range of IVR self-service port densities
- Integration with Cisco IOS voice gateway services for superior media treatment
- Solution tested with Cisco Unified Customer Voice Portal 3.1
- Support for many speech engines, including Nuance, IBM and Loquendo
- Industry leading standards compliance; VoiceXML 2.0 including the following new capabilities
  - Transfer enhancements include support for application to application information data passing, blind and bridged transfer conformance
  - Added options for "exact" versus "approximate" phrase recognition for more flexibility
- Remains backward compatible to earlier Cisco IOS VoiceXML versions

Figure 83. Cisco IOS VoiceXML Topology



Benefits

Cisco IOS VoiceXML browsers allows IVR and self service application logic to occur at the edge of the network in the branch, closer to the caller, off-loading the server and the WAN.

Enterprises can leverage existing hardware that may already be providing voice services in the branch. The Cisco IOS VoiceXML browser extends the broad range of VoIP services available on Cisco IOS voice gateways which include the Cisco 2800 and Cisco 3800 Integrated Services Routers, Cisco 3700 Series and the Cisco AS5000 Series.

Cisco IOS VoiceXML browser sessions may run concurrently with PSTN voice gateway services further increasing the return on investment in Cisco platforms.

VoiceXML applications can use the Enterprise's existing Web infrastructure which saves money and provides access to other Web-based data and applications.

VoiceXML allows significantly faster application development compared to traditional IVR development and modification. Cisco UCVP Studio, an Integrated Development Environment (IDE) powered by Eclipse, combines a full-featured suite of development tools with a graphical user interface for drag-and-drop development and can be used to build scripts that invoke services on the Cisco IOS VoiceXML browser.

Hardware

Routers	• Cisco 2600XM, 2691, 2800, 3700, 3800, AS5400XM, AS5350XM, AS5400HPX Series

Considerations

Service and Support: The Cisco IOS VoiceXML browser, when purchased with the appropriate support contract(s) is supported by the Cisco Technical Assistance Center (TAC). Questions and support issues related to custom VoiceXML scripts or application servers other than those related to interoperability with the Cisco Unified Customer Voice Portal (UCVP) are not covered by Cisco TAC. The Cisco TAC only supports problems related to the Cisco IOS VoiceXML browser and UCVP. Customers with custom scripts, third-party, VoiceXML-based applications should engage the Advance Services organization and/or the developers' services organizations. Developers' support information can be found on cisco.com.

http://www.cisco.com/cgi-bin/dev_support/access_level/product_support (CCO log in required)

Cisco Unified Customer Voice Portal Release 4.0, which supports VoiceXML 2.0, is scheduled to be available in the 4th quarter of 2006. CVP 3.1 does not support VoiceXML 2.0, therefore solution testing between the Cisco IOS VoiceXML browser and CVP did not include VoiceXML 2.0 features. Cisco IOS Software Release 12.4(11)T will not be solution tested with CVP 4.0. Customers that want to use CVP 4.0 with the Cisco IOS VoiceXML browser version which supports VoiceXML 2.0 are advised to use the Cisco IOS T train release subsequent to Release 12.4(11)T which will be solution tested with CVP for VoiceXML 2.0 support.

Product Management Contact: Teresa Newell (tnewell@cisco.com)

6.7.3) Internet Low Bit Rate (iLBC) Codec Support for SIP and H.323
The Internet Low Bit Rate (iLBC) codec is a low-bandwidth, narrowband codec that operates at 13.3 kbps with a 30 ms frame size or at 15.2 kbps with a 20ms frame size.

iLBC is supported with the SIP and H.323 signaling protocols.

iLBC is a good codec choice where a lower-bandwidth codec is required for impaired, unmanaged or congested IP networks that experience significant packet loss.

For example, iLBC is a good codec choice for a PC-based softphone client running over a congested VPN or for an internet telephony service that does not support adequate Quality of Service (QoS).

Benefits

- **Improved Voice Quality for a low-bandwidth Codec:** The iLBC codec offers slightly better voice quality than G.729a but less than G.711 or G.726. iLBC offers substantially better quality than G.729a in networks with over 1% packet loss.
- **Graceful Voice Quality Degradation in Impaired Network:** The iLBC codec performs well in networks with up to 5% packet loss.

Hardware

Routers	• Cisco AS5400XM and AS5350XM with the high-density packet voice feature card (AS5X-FC) and DSP module (AS5X-PVDM2-64)

Product Management Contact: Steven White (whites@cisco.com)

6.7.4) Internet Low Bit Rate codec (iLBC) Support on IP-to-IP Gateway for Flow-through and Flow-around Modes
This feature provides support for the Internet Low Bit Rate codec (iLBC) codec on the Cisco Multiservice IP-to-IP Gateway for both flow-through and flow-around modes.

This enables the iLBC codec to be deployed in both Enterprise and service provider environments that require interconnection between independent VoIP networks. A typical application for leveraging the packet-loss robustness of the iLBC codec would be for the interconnection of an Internet telephony service with a managed or hosted Enterprise VoIP network. The iLBC codec is supported on the Cisco Multiservice IP-to-IP Gateway for H.323 to H.323, SIP to SIP, and SIP to H.323.

Hardware

Routers	• Cisco AS5400XM and AS5350XM with the high-density packet voice feature card (AS5X-FC) and DSP module (AS5X-PVDM2-64) • Cisco 28/3800 Series Integrated Services Routers • Cisco 3700 Series Integrated Access Routers • Cisco 7200VXR and Cisco 7301 series Routers

Product Management Contact: Steven White (whites@cisco.com)

6.7.5) Support for the Second Generation 1- and 2-port T1/E1 Multiflex Trunk Voice (MTF) WAN Interface Cards on the 2430 Series Integrated Access Devices
The Cisco second-generation 1- and 2-port T1/E1 Multiflex Trunk Voice (MTF)/WAN Interface (MFT VWIC2s) are now supported on the Cisco 2430 Series Integrated Access Devices for both data and voice applications. The Cisco MFT VWIC2 are also supported on the Cisco 1721 (data only), 1751 and 1760 Modular Access Routers, the Cisco 2600XM Multiservice Router, the Cisco 2691 Multiservice Platform, the Cisco 3662 Telco Versatile DCN Access Platform, the Cisco 3725 and 3745 Multiservice Routers, and the Cisco 1841 (data only), 2801, 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers. The Cisco MFT VWIC2 combines WAN-interface-card (WIC) and voice-interface-card (VIC) functions to provide unparalleled flexibility, versatility, and

investment protection through its many uses. Customers who choose to integrate data and voice in multiple steps preserve their investment in a T1/E1 WAN interface because the Cisco MFT VWIC2 cards can be reused in packet voice applications. The 2 port T1/E1 MFT VWIC2 is shown below.

Figure 84. Cisco 2-Port T1/E1 Multiflex Trunk Voice (MTF)/WAN Interface (MFT VWIC2)

The Cisco MFT VWIC2 interface cards add numerous improvements over the Cisco 1- and 2-port T1/E1 Multiflex Voice/WAN Interface Cards (MFT VWICs). The MFT VWIC2 cards have an onboard slot for a Cisco MFT Dedicated Echo Cancellation (ECAN) Module (part number EC-MFT-32 or EC-MFT-64), offering an enhanced echo-cancellation capability for demanding network conditions. The T1/E1 MFT VWIC2 cards support both T1 and E1, providing additional flexibility in configuring the Cisco MFT VWIC2s for supporting T1, fractional T1, E1, and fractional E1 for both voice and WAN applications. All MFT VWIC2 modules now include the drop-and-insert multiplexing capability, which eliminates costly external third-party channel service units/data service units (CSUs/DSUs) and drop-and-insert multiplexers. The Cisco 2-port MFT VWIC2s also can enable each port to be clocked from independent clock sources for data applications. This independent clocking capability is not supported for voice applications or with the Cisco ATM/Voice Advanced Integration Modules (part number AIM-ATM, AIM-VOICE-30, AIM-ATM-VOICE-30).

The Cisco MFT VWIC2 cards can either be inserted into the WIC, VWIC and high-speed WIC (HWIC) slots on the supported Cisco 1721, 1751, 1760, 1841, 2600XM, 2691, 2801, 2811, 2821, 2851, 3662, 3725, 3745, 3825, and 3845 Access Routers, Cisco 2430 Series Integrated Access Devices, or they can be used in the VWIC or HWIC slot(s) on the Digital T1/E1 Packet Voice Trunk Network Module (NM-HDV), IP Communications High-Density Digital Voice/Fax Network Modules (NM-HDV2), IP Communications High-Density Digital Voice NM with 1 T1/E1 (part number NM-HDV2-1T1/E1), IP Communications High-Density Digital Voice NM with 2 T1/E1 (part number NM-HDV2-2T1/E1), 2 slot IP Communications Enhanced Voice/Fax Network Modules (NM-HD-2VE), 2 WAN Card Slot Network Module (NM-2W), 1 10/100 Ethernet 1 4/16 Token Ring 2 WAN Card Slot NM (NM-1FE1R2W), 1 10/100 Ethernet 2 WAN Card Slot Network Module (NM-1FE2W-V2), and 2 10/100 Ethernet 2 WAN Card Slot Network Module (NM-2FE2W-V2) when used with a supported access router.

The Cisco MFT VWIC2 cards are offered in single- and dual-port versions, which can be used and then redeployed as network requirements change, thereby addressing several applications:

- **T1/E1 data:** The Cisco 1- and 2- port T1/E1 MFT VWIC2 versions act as a WIC, supporting T1, fractional T1, E1, (including structured G.703 with G.704 framing), fractional E1, and E1structured G.703 applications. To simplify remote management, these MFT VWIC2 cards integrate a fully managed DSU/CSU for T1 deployments and a fully managed DSU for E1 deployments.
- **E1/G.703 data:** The Cisco 1- and 2- port G.703 MFT VWIC2 versions act as a WIC, supporting T1, fractional T1, E1 (including structured G.703 with G.704 framing), fractional E1, and unstructured E1 (G.703) applications. To simplify remote management, the G.703

version includes a fully managed DSU. The G.703 versions also support all the capabilities on the T1/E1 versions.

- **T1/E1 packet voice:** The Cisco 1- and 2- port T1/E1 MFT VWIC2 (voice and WAN) versions act as a VIC, supporting packet voice applications by providing T1, fractional T1, E1, and fractional E1 connections to Private Branch Exchanges (PBXs) and central offices, thereby enabling new services and reducing voice and fax toll charges.
- **Mixed data and packet voice:** The Cisco MFT VWIC2 interface cards can simultaneously support both data and voice, reducing the complexity and number of network components and facilitating a graceful migration to bandwidth-efficient packet voice.
- **Mixed data and packet voice with drop and insert:** The Cisco MFT VWIC2 cards can be deployed as a T1/E1 drop-and-insert multiplexer with integrated DSUs/CSUs, reducing the complexity of the network and the cost of the central-office ports by efficiently combining Time-Division Multiplexing (TDM) voice (PBX), IP voice, and data on the same trunks. Note the Cisco 1721, 1751 and 1760 support drop and insert between two ports over a single VWIC2 card while Cisco 2800 and 3800 ISR routers supports drop and insert between two ports over a single VWIC2 card and two ports over two different VWICs.

Benefits

Reduces Networking Lifecycle Costs

- Enables graceful migration from data-only to multiplexed data and voice to packetized voice applications
- Reduces training, deployment, management, and sparing inventory over single-purpose interfaces
- Maximizes investment protection
- Simplifies network configuration and sparing through the support of both T1 and E1 on the same card
- Offers multifunction support for LAN-to-LAN routing, multiplexed data and voice, and packetized voice
- Offers ability to share modules between Cisco 1700, 1800, 2800 and 3700 series and Cisco 3800 routers, select Cisco 2600 and 3600 series routers, and select network modules
- Increases configuration flexibility and reduces cost for data applications by allowing individual ports to be clocked from independent clock sources (not supported for voice and not supported with ATM/Voice Advanced Integration Module (part number AIM-ATM-VOICE-30) with ATM/Voice Advanced Integration Module (part number AIM-ATM, AIM-VOICE-30, AIM-ATM-VOICE-30)
- Supports E1 configurations for both balanced and unbalanced modes
- Supports (G.703 models) unstructured E1 (G.703) for using the full 2.048 Mbps
- Eliminates costly external third-party CSUs/DSUs and drop-and-insert multiplexers
- Provides optional support of a Cisco MFT Dedicated ECAN Module for demanding network conditions
- Simplifies remote network management by allowing a single management tool such as CiscoView or CiscoWorks to support router, CSU/DSU, or drop-and-insert multiplexer

Maximizes System Resources

- Increases T1/E1 port density on the supported Cisco 1700, 1800, 2600, 2800, 3600, 3700, and 3800 Access Routers—up to four T1/E1 connections with an integrated CSU/DSU in a single network-module slot or up to two T1/E1 connections in a single WIC slot
- Offers easy migration to bandwidth-efficient packet voice, enabling new services

Hardware

Routers	• Cisco 2430 Series Integrated Access Servers • Cisco 1721 (data only), 1751 and 1760 Modular Access Routers • Cisco 2600XM Multiservice Router • Cisco 2691 Multiservice Platform • Cisco 3662 Telco Versatile DCN Access Platform • Cisco 3725 and 3745 Multiservice Routers • Cisco 1841 (data only), 2801, 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers

Product Management Contact: Steven White (whites@cisco.com)

6.7.6) Support for the Multiflex Trunk Dedicated Echo Cancellation (MFT ECAN) Modules on the 2430 Series Integrated Access Devices

The Cisco Multiflex Trunk Dedicated Echo Cancellation (MFT ECAN) Modules are now supported on the Cisco 2430 Series Integrated Access Devices. The MFT ECAN Modules are dedicated resources for the Cisco Enhanced ITU-T G.168 ECAN feature, providing robust echo cancellation performance for demanding network environments. The modules are daughter cards that attach to Cisco Second-generation Multiflex Trunk Voice/WAN Interface Cards (MFT VWIC2 cards). The dedicated ECAN modules are available in 32- and 64-channel configurations, which match the requirements of the 1- and 2-port T1/E1 MFT VWIC2s, respectively. The 64-channel MFT ECAN Module is shown below.

Figure 85. Cisco 64 Channel Multiflex Trunk Dedicated Echo Cancellation Module

The Cisco Enhanced ITU-T G.168 ECAN feature can be run either on the dedicated ECAN modules or the general voice resources that reside on the platform, network module, or advanced integration module. For example, Cisco 2800 Series and 3800 Series Integrated Services Routers can use either the packet voice DSP modules (PVDM2s) mounted in the router chassis or the Digital Signal Processor (DSP) resources on network modules to run the G.168 ECAN feature. When the G.168 ECAN feature is run on general voice resources, processing and memory constraints limit it to having at most 64-ms echo tail coverage. Although this is adequate in most network conditions, a larger echo tail coverage is sometimes required. In these situations, the dedicated ECAN modules, attached to the appropriate MFT VWIC2, can be used. The processing

and memory resources of the dedicated ECAN modules enable the echo canceller to be configured with predefined settings and an extended 128-ms echo tail buffer, providing robust echo cancellation performance in these more demanding network environments.

Benefits

Benefits of the Cisco enhanced ITU-T G.168 ECAN feature using either Cisco dedicated ECAN modules or general voice resources include:

Investment protection through a state-of-the-art echo cancellation feature

- Enhanced ITU-T G.168 ECAN feature complies with and exceeds the performance requirements specified in the ITU-T Recommendation G.168 Digital Network Echo Cancellers (2000) standard
- Provides future echo cancellation enhancement capability through Cisco IOS® Software upgrades

Increased echo cancellation effectiveness by providing capabilities and controls

- Provides control of the echo canceller coverage through the size of the echo cancellation buffer, ranging from 8 to 64 ms (128 ms of echo cancellation coverage requires dedicated ECAN module)
- Configures the worst-case echo return loss (ERL), ranging from 0 to 6 dB
- Provides control over echo cancellation convergence, enabling faster convergence for multiple echo reflectors and improved double-talk detection
- Provides control for enabling and disabling the nonlinear processor (NLP), which replaces the residual echo at the output of the echo canceller with comfort noise based on the actual background noise of the voice path
- Improved network manageability by providing various echo cancellation performance metrics and testing capabilities
- Reports various metrics, including combined echo return loss (ACOM), ERL, and worst-case echo return loss
- Reports statistics for location of the largest reflector (tail) and the internal state of the G.168 ECAN feature
- Provides test-mode support for manually freezing, thawing, and clearing the echo canceller registers
- Additional benefits of the Cisco enhanced ITU-T G.168 ECAN feature when used with the Cisco dedicated ECAN modules include:

Additional echo cancellation effectiveness through extended capabilities and features

- Control of the echo canceller is provided through the size of the echo cancellation buffer, ranging from 8 to 128 ms.
- Additional processing and memory resources help ensure robust echo canceller coverage independent from the echo canceller configuration or the demand placed on the general voice DSP resources.

Hardware

Routers	• Cisco 2430 Series Integrated Access Servers • Cisco 1751 and 1760 Modular Access Routers • Cisco 2600XM Multiservice Router • Cisco 2691 Multiservice Platform • Cisco 3662 Telco Versatile DCN Access Platform • Cisco 3725 and 3745 Multiservice Routers • Cisco 2801, 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers

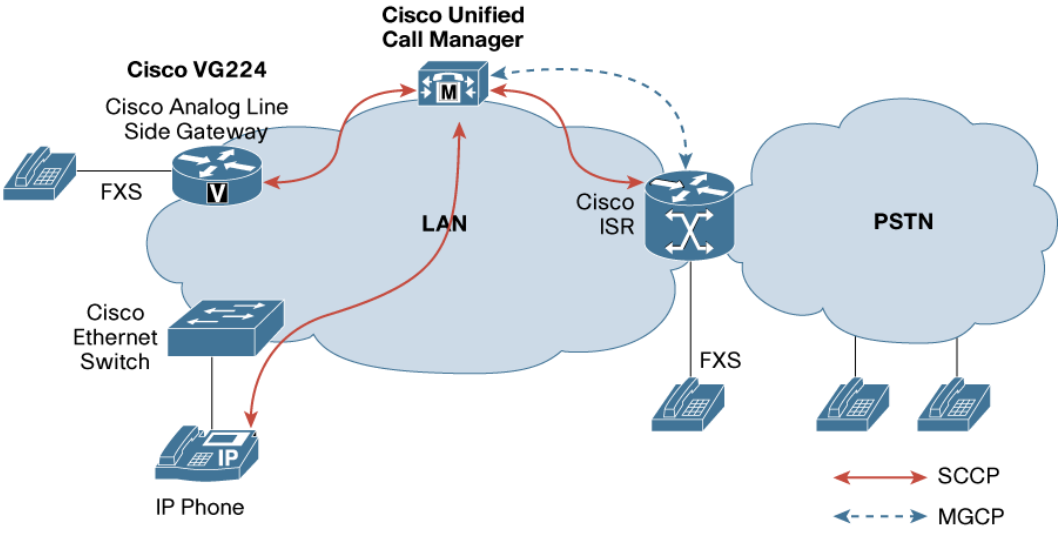
Product Management Contact: Steven White (whites@cisco.com)

6.7.7) Skinny Call Control Protocol (SCCP) Controlled Analog (FXS) Ports with Enhanced Supplementary Features in IOS Gateway
With Release 12.4(9)T, supplementary features were introduced for SCCP Controlled Analog (FXS) Ports on Cisco 2800 and 3800 ISR in addition to Cisco VG224. FXS ports on Cisco 2800 and 3800s could be controlled by Cisco Unified CallManager or Cisco Unified CallManager Express using SCCP protocol.

In Release 12.4(11)T, additional new features are being introduced for Cisco 2800,3800 and the Cisco VG224:

- RFC 2833 DTMF Relay support on SCCP analog end points
- Feature Mode:
  - Call Transfer
  - Call Conference
  - Drop Last Conferee
  - Hang up Last Call
  - Call Toggle
- SCCP Gateway controlled modem relay
- SCCP T.38 NSE fax relay and Cisco fax relay
- Visual Message Waiting Indicator(VMWI)
- Dial tone generation after remote onhook
- Support ground start FXS port as analog end point

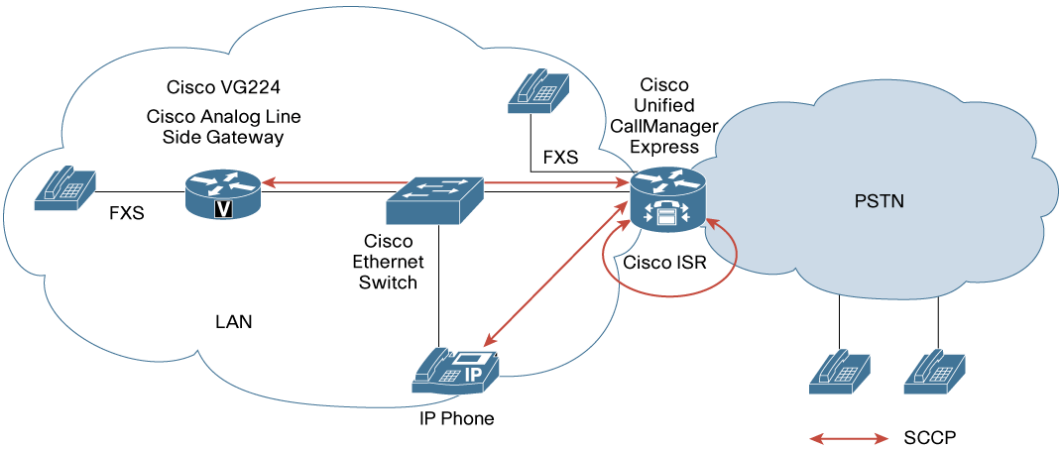
Figure 86. SCCP FXS Analog ports on Cisco ISR and Cisco VG224 Analog Phone Gateway with Cisco Unified CallManager



Benefits

- Support for SCCP FXS analog ports on Cisco 2800 or 3800 Series which can also act as a voice gateway and SRST gateway for end customers
- Supplementary feature enhancement with support for feature mode operation. Previously only standard mode was supported for analog phones. In the Standard mode, users use hook flash to transfer, conference and toggle calls. With the feature mode, users can now use hookflash and feature code combination to drop last active call (#1), transfer (#2), conference (#3), drop last conferee (#4), toggle between two calls (#5). Hookflash again will return to previous state.

Figure 87. SCCP FXS analog ports on Cisco ISR and Cisco VG224 Analog Phone Gateway with Cisco Unified CallManager Express



Benefits

- Support for SCCP FXS analog ports on Cisco 2800 or 3800 series and Cisco VG224 which can also act as a Cisco Unified CallManager Express voice gateway for end customers
- Supplementary feature enhancement with support for feature mode operation.

Hardware

Routers	• Cisco 2800 and 3800 Series
Network Module FXS carrier cards on Routers	• NM-HD-2V, NM-HD-1V, NM-HD-2VE • NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1 • EVM-HD-8FXS/DID, EM-HDA-8FXS, EM-HAD-3FXS/4FXO, • EM-4BRI-NT/TE
Voice Interface Card (VIC) on routers or Network Modules	• VIC2-2FXS, VIC-4FXS/DID, VIC2-2BRI-NT/TE
Voice Gateways	• Cisco VG224

Considerations

1. SCCP FXS ports on Cisco 2800 or 3800 Series and Cisco VG224 are interoperable with Cisco Unified CallManager 4.2 release and above.
2. RFC2833 DTMF Relay support on SCCP analog end points is supported with CUCM version 5.x and above.
3. SCCP FXS ports on Cisco 2800 or 3800 Series and Cisco VG224 are interoperable with Cisco Unified CallManager Express 5.x and above

Product Management Contact: Jayesh Chokshi (jayesh@cisco.com)

6.8) Hardware

6.8.1) Network Processing Engine G2 (NPE-G2) for Cisco 7200 Series Router

Increasingly, business applications and services affect aggregation requirements and router-integrated services across the WAN and metropolitan-area network (MAN), at both, the branch office and headquarter.

Consequently, to continue to meet the increasing need for performance for router-integrated services at the branch office and headquarters and to maintain exceptional value and flexibility, Cisco Systems® introduces the 7200VXR NPE-G2 Network Processing Engine (Figure 75). The Cisco NPE-G2 addresses the demand for performance and flexibility by further increasing its processing capacity and helping enable the latest Cisco IOS® Software features. The table below lists its features.

Figure 88. Cisco 7200 Series NPE-G2

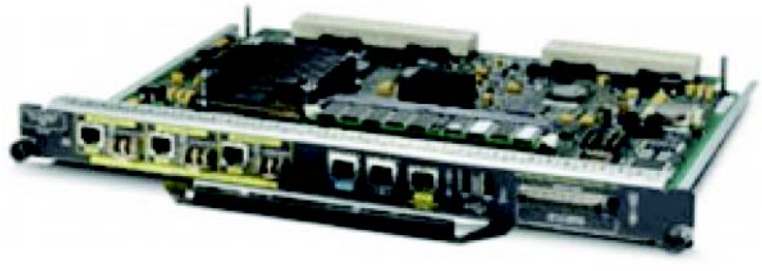


Table 22. Features of Cisco NPE-G2

Feature	Description
Performance of up to 2 Million Packets per Second (PPS) in Cisco Express Forwarding Switching	• Doubles the performance compared to Cisco NPE-G1 • Dramatically increases the performance and scalability of the Cisco 7200VXR Series in WAN and MAN applications for both Enterprises and service providers
Modularity	• Helps enable maximum investment protection through the ability to upgrade processors incrementally
Backward Compatibility with Existing Port Adapters (with a few exceptions)	• Provides investment protection through backward compatibility • Note: The following end-of-sale port adapters are not supported: • Cisco Fibre Channel over IP Port Adapter (PA-FC-1G; this port adapter is End-of-Sale status as of December 3, 2004) • Cisco 1-Port OC-12, Dual-Width DPT Port Adapter (PA-SRP-OC12; this port adapter is end-of-sale status as of July 15, 2005) • Cisco VPN Acceleration Module (SA-VAM; this service adapter is end-of-sale status as of April 28, 2006) • Cisco VPN Acceleration Module 2 (SA-VAM2; this service adapter is End-of-Sale status as of April 28, 2006)
Three Fixed Gigabit Ethernet Ports (10/100/1000-Mbps Copper or Small Form-Factor Pluggable Optics [SFP])	• Maximizes LAN connectivity and performance without taking up bandwidth points or midplane capacity
Built-in I/O Function (Compact Flash Memory, Console Port, Auxiliary Port, and Bootflash Memory)	• Reduces costs (Note: An I/O controller can still be used. The Cisco NPE-G2 is supported with the Cisco 7200VXR Series I/O controllers with the following part numbers: C7200-I/O, C7200-I/O-2FE, and C7200-I/O-GE+E.)
Support for Third Peripheral-Component-Interconnect (PCI) Bus to the I/O Controller Slot	• Frees the current I/O controller ports from bandwidth allocation, allowing two PCI buses to be dedicated to the port adapter slots • Provides cost-effective way for a slot expansion by using port adapter jacket card • Provides a dedicated slot for the high-performance VPN services adapter
Double the Speed of the PCI Bus on the I/O slot	• Dramatically increases the performance of Cisco 7200VXR Series VPN Services Adapter (VSA)
1 GB of DRAM Default Memory	• Delivers the most amount of memory by default compared to existing Cisco 7200VXR Series network processing engines, offering the following benefits: • Supports more routes and routing tables • Supports more Multiprotocol Label Switching (MPLS) virtual routing and forwarding instances (VRFs) • Supports more sessions for broadband aggregation • Helps enable higher scalability on features such as NetFlow, Network Address Translation (NAT), Access Control Lists (ACLs), and more • Offers post-First Customer Shipment (FCS) support for optional upgrade to 2 GB DRAM
Cisco IOS Software	• Supports a wide range of IP and non-IP network services, including Quality of Service (QoS), MPLS, broadband aggregation, integrated security, encryption, voice, and more
Dedicated Management for 10/100-Mbps Ethernet	• Reduces costs and protects port density of the chassis
Two USB Ports	• Provides a large, removable storage for files • Stores security e-tokens for VPN applications
Digital Diagnostics on SFP Interfaces	• Provides a powerful tool that monitors many manageable parameters, including optical transmit and receive power, voltage and temperature measurement, and factory parameters
Time Domain Reflectometry (TDR) on Copper Interfaces	• Provides an effective method of isolating fault at the remote end of the copper wire by monitoring reflected pulsed signals

New Features

The NPE-G2 provides the following capabilities (refer to the table above for additional details):

- Provides double the performance compared to the Cisco 7200VXR NPE-G1-up to 2 million pps in Cisco Express Forwarding
- Offers three 10/100/1000-Mbps copper Ethernet ports and optical ports that do not consume any bandwidth points
- Provides one dedicated 10/100-Mbps copper Ethernet port for management
- Provides two USB ports for general storage and security token storage
- Offers 1 GB of DRAM memory by default; post-FCS: Optional upgrade to 2 GB DRAM
- Eliminates the requirement for an I/O controller
- Extends the use of the available I/O slot for a single port adapter or a Cisco 7200VXR VPN Service Adapter (part number C7200-VSA) (when available)
- Offers greatly improved price/performance ratio

Availability

The Cisco NPE-G2 is supported in the Cisco 7204VXR and Cisco 7206VXR chassis.

For More Information

For more information about the Cisco NPE-G2, visit http://www.cisco.com/go/7200

Product Management Contact: Young Bae (ybae@cisco.com)

6.8.2) VPN Services Adapter (VSA) for Cisco 7200VXR Series Routers
The Cisco® VPN Services Adapter (VSA) for Cisco 7200 Series Routers provides high-performance encryption and key-generation services for IP Security (IPsec) VPN applications. It increases performance over the existing VPN Acceleration Module (VAM). Like the VAM2+, the VSA supports Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). It includes hardware acceleration for 128-, 192-, and 256-bit AES keys. The VSA requires the Cisco 7200 Series NPE-G2 Network Processing Engine. It fits only in the I/O controller slot on the Cisco 7204VXR or 7206VXR chassis, conserving valuable bandwidth points for other port adapters.

This combination of security features and high performance offers a flexible, integrated approach to accommodate the most diverse Enterprise or service provider network environments, while providing investment protection for existing Cisco 7200 Series Router customers.

Supported Features

Table 23. Cisco VPN Service Adapter Features

Features	Description
Physical	Service adapter; installs in the I/O slot on Cisco 7200 Series Routers
Platform support	Cisco 7200 Series routers with the NPE-G2
Throughput*	950 Mbs
Number of IPsec-protected tunnels	Up to 5000 tunnels
Hardware-based encryption	• Data protection: IPsec DES, 3DES, or AES· • Authentication: RSA and Diffie-Hellman • Data integrity: Secure Hash Algorithm (SHA) and Message Digest Algorithm 5 (MD5)
VPN tunneling	IPsec tunnel mode; generic routing encapsulation (GRE) and Layer Tunneling Protocol (L2TP) protected by IPsec

Features	Description
LAN or WAN interface selection	On Cisco 7200 Series, VSA works with most Cisco 7200 VXR-compatible port adapters
Standards supported	IPsec with Internet Key Exchange (IKE): RFCs 2401-2411 and 2451

* 1950 Mbps with 1400 byte packet

Additional Information

The table below lists the part numbers for the Cisco VSA. The Cisco 7200 Series security bundles that include the VSA are currently available for easy ordering at a bundle discount. For more information about VSA bundles, visit:

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

Table 24. Part Numbers for Cisco VSA

Part Number	Description
C7200-VSA	VSA for Cisco 7200 Series Routers
C7200-VSA=	VSA for Cisco 7200 Series Routers (spare)

Product Management Contact: Donovan Williams (dowillia@cisco.com) or ask-stg-ios-pm@cisco.com

7) Release 12.4(9)T Highlights

Table 25. Release 12.4(9)T Feature Highlights

7.1) Cisco IOS Security	7.2) Voice	7.3) Management Instrumentation	7.4) IP Routing
7.1.1) Cisco IOS Firewall Enhancements —HTTP Application Inspection and Control Enhancements, Session Policing and Ingress Rate Policing based on Firewall Policies, P2P Application Filtering*	7.2.1) Cisco Unified CallManager Express 4.0 *	7.3.1) Flexible NetFlow*	7.4.1.) Bidirectional Forwarding Detection (BFD) Echo Mode*
7.1.2) Cisco EasyVPN 7.1	7.2.2) Cisco Multiservice IP-to-IP Gateway—Hosted NAT Traversal	7.3.2) Cisco Networking Services (CNS) Security Enhancements	7.4.2) ACL-based Rate Based Satellite Control Protocol (RBSCP)
7.1.3) DMVPN Manageability Enhancements	7.2.3) Skinny Call Control Protocol (SCCP) Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateway	7.3.3) Netconf Access for Configuration over SSH and BEEP	7.4.3) Open Shortest Path First version 3 (OSPFv3) IPsec ESP Encryption and Authentication
7.1.4) Virtual Private Network (VPN) Advanced Integration Module (AIM) for Cisco 1841/2800/3800 Integrated Services Routers (ISRs)	7.2.4) High-Density Packet Voice for Cisco AS5400XM and AS5350XM Universal Gateways		
7.1.5) Cisco IOS WebVPN—Auto-Applet Port Forwarding Download			
7.1.6) Cisco IOS WebVPN—HTTP Authentication			
7.1.7) Cisco IOS WebVPN—RADIUS Accounting			

7.5) Mobility	7.6) IP Services	7.7) High Availability
7.5.1) Mobile IP—Mobile Router Multi-path Support	7.6.1) Enhanced Object Tracking (EOT) Support for Carrier Delay	7.7.1) Hot Standby Router Protocol—HSRP Group Shutdown
	7.6.2) Domain Name Service—Split DNS	

* Indicates Key Highlight

7.1) Cisco IOS Security

7.1.1) Cisco IOS Firewall Enhancements

Cisco IOS Firewall integrates stateful firewall and application inspection functionality as part of a complete set of threat defense features offered on Cisco routers. Routers with integrated firewalls enable cost-effective and easy-to-deploy security solutions at every access point in the network. A firewall combined with other integrated router security capabilities allows new classes of solutions to connect mobile workers, branch offices, telecommuters, partners and customers into the network.

Release 12.4(9)T introduces the following functionality to Cisco IOS Firewall:

- HTTP Application Inspection and Control Enhancements
- Session Policing and Ingress Rate Policing based on Cisco IOS Firewall Policies
- P2P Application Filtering

HTTP Application Inspection and Control Enhancements

HTTP is the most commonly used application-layer protocol on the Internet. HTTP offers a flexible, extensible mechanism to support numerous networked applications. Businesses, educational institutions, and government offices that rely on the Internet must allow HTTP traffic through their firewalls to accommodate most Web-based applications. Unfortunately, the pervasive nature of HTTP support has contributed to TCP port 80 being a transmission vector for malicious software such as worms and viruses, as well as offering an effective conduit for concealing other traffic generated by undesirable software such as Instant Messaging (IM) applications and Peer-to-Peer (P2P) file-sharing tools.

Cisco IOS Software HTTP Application Inspection (AI) offers flexible application-layer inspection to examine network traffic to detect and take action against malicious or unwanted HTTP traffic. This release offers the following enhancements in this area:

1. User Definable and Extensible Policies—Policies may be defined based upon various HTTP Protocol objects like HTTP methods, URLs, header names and values such as maximum URL length, maximum header length, maximum number of headers, maximum header-line length, non-ascii headers, or duplicate header fields. This allows the ability to limit buffer overflows, HTTP header vulnerabilities, binary or non-ascii character injections, exploits like SQL injection, cross site scripting and worms attacks.
2. Flexible CPL Based Configuration—Configuration and application is done using the Class-based Policy Language (CPL) to allow user defined patterns for policy definitions. This enables a very flexible, powerful and granular approach to prevent against HTTP attacks and vulnerabilities. This support comes in addition to the existing HTTP application inspection that allows for extensive RFC (2616 and 2068) conformance checking to prevent malicious HTTP traffic.

Session Policing and Ingress Rate Policing based on Firewall Policies

Denial of Service (DoS) attacks designed to cripple network routers and corporate computing resources by flooding networks with packets are an important security threat that needs to be defended against to maintain network integrity and availability for designated users. Additionally, controlling the allocation of network resources based on protocol is critical to engineering high performance networks. Preventing DoS attacks and controlling network resource utilization, both

require the ability to designate which users and/or applications can use the network and how much bandwidth they can consume.

To address this topic, Cisco introduces two new innovations for Cisco IOS Firewall policies:

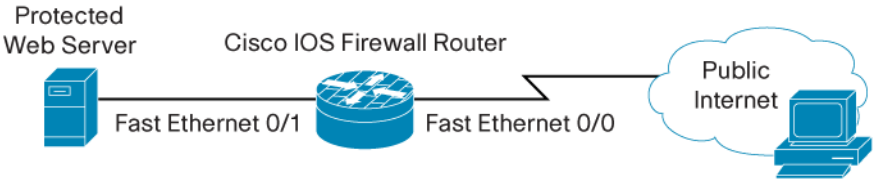
1. **Session Policing:** Session Policing is the ability to control the number of sessions for a particular protocol or user group allowed through a Cisco IOS Firewall. This session control limits the amount of resources a DoS attack can use on the router and offers a method to prevent and minimize DoS attacks.
2. **Ingress Rate Policing:** Ingress Rate Policing is the ability to control the bandwidth that is used by an application or a set of traffic through the firewall. This serves as a limiting factor to DoS attacks by preventing excessive bandwidth from being consumed by the packets from the DoS attack.

Although the above descriptions focus on the issue of preventing malicious users from gaining control of the network in DoS attacks, it is straightforward to see how these mechanisms can also be used to control the usage pattern of users and/or applications. This control allows network administrators to have a means of controlling network resource utilization.

P2P Application Filtering

Peer-to-Peer (P2P) Applications, like eDonkey, Kazaa, and Gnutella, are becoming an increasingly common form of network traffic that consumes valuable network bandwidth and can potentially become a security threat by carrying malicious traffic and applications. In order to address this issue, Cisco is introducing P2P Application Filtering as part of its firewall policies to help customers defend and protect their networks from P2P threats. A key differentiator of Cisco's offering is the ability for customers to load a protocol definition file, called a Packet Description Language Module (PDLM), for new P2P protocols; the Cisco IOS Firewall can then start dynamically recognizing the protocol and apply firewall policies on the protocol without requiring an update of the software image.

Figure 89. HTTP Application Inspection on Firewall Router for a Web Server



Benefits

- **Increased Security against HTTP Attacks and Vulnerabilities:** User definable and extendable HTTP inspection policies allows many methods to increase security of HTTP traffic and prevent attacks and vulnerabilities based upon HTTP.
- **Increased Security against P2P Attacks and Vulnerabilities:** PDLMs allow Firewall policy functionality to be used in the context of P2P Application Filtering to prevent security breaches and control network bandwidth usage from this traffic type.
- **Simplified Configuration:** HTTP Application Inspection policies defined and applied through CPL to simplify configuration process.
- **Prevents DoS Attacks:** Session Limiting and Ingress Rate Policing on Cisco IOS Firewall policies prevents DoS attacks from consuming bandwidth on firewall interfaces to minimize

the effects of these attacks. This functionality also offers greater control for network resource utilization.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers

Additional Information:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

Product Management Contact: Darshant Bhagat (dabhagat@cisco.com)

7.1.2) Cisco EasyVPN 7.1

Cisco EasyVPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for site to site, remote offices and tele-workers. Cisco EasyVPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments. Cisco EasyVPN enables integration of VPN remote devices, Cisco routers, Cisco Adaptive Security Appliances (ASA), PIX Firewalls, and Cisco VPN concentrators or software clients; it allows a consistent policy and key management method within a single deployment to enable simplified remote site administration.

Release 12.4(9)T introduces the following key functionality to Cisco EasyVPN:

- Cisco Tunnelling Control Protocol (CTCP) in Cisco IOS Software
- Split DNS
- DHCP Client Proxy support for EasyVPN

Cisco Tunnelling Control Protocol

In many situations, customers require a VPN client to operate in an environment where standard Encapsulating Security Protocol (ESP with protocol or next header field value 50) or UDP Port 500 (Internet Key Exchange - IKE) can either not function, or not function transparently (without modification to existing firewall rules). TCP tunnelling of IPsec packets is often requested by road warriors, operating out of hotels rooms, airports etc. to pass through third party firewall devices in their environments.

Situations where standard ESP or UDP 500 is often not acceptable/permitted include:

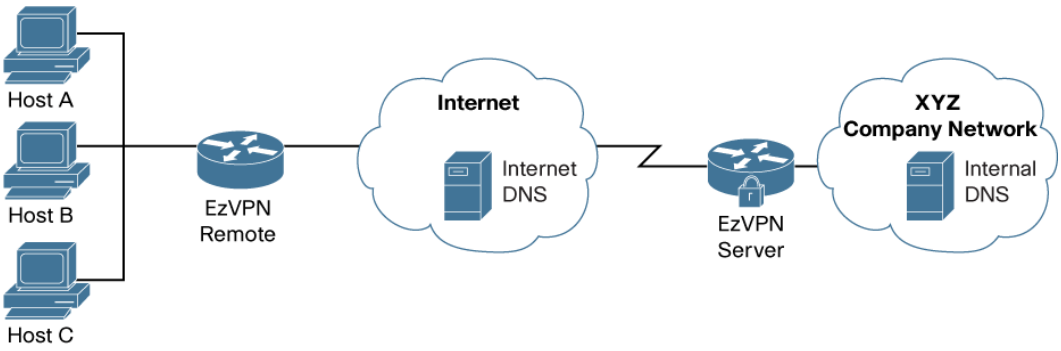
- Small/home office router performing Port Address Translation (PAT). This router usually supports both TCP & UDP translation by default.
- Network Address Translation (NAT) provided IP address behind a large corporate router. A hotel providing private address space to guests could fall under this category, or the previous PAT scenario.
- Non-NAT Firewall (packet filtering or stateful). This scenario is common at companies that wish to use routable address space on their internal networks. Particular TCP applications will function, but UDP outbound is not permitted as it is often considered a security hole.
- Proxy server. If a proxy server is smart enough to actually look at each packet to confirm that the activity occurring is the defined activity, native IPsec flows will not be able to work in this situation.

To solve this problem in the above situations, without modifying the rules configured in the firewall, Cisco has come up with a protocol called Cisco Tunneling Control Protocol (CTCP). When CTCP is enabled on client and head-end devices, IKE and ESP traffic will be encapsulated in TCP header, so that the firewalls in between the client and the head-end device would simply permit this traffic (considering it as TCP traffic).

Split DNS in EasyVPN

The Split-DNS functionality enables EasyVPN client to act as a “DNS proxy”, directing Internet queries to the DNS Server of the ISP and directing corporate DNS requests to the corporate DNS servers. Without Split DNS, enterprises typically must point their CPEs to the corporate DNS servers for all DNS queries, because only their internal servers can resolve all their internal domains. This means that the internal servers will also have to carry the load of resolving or proxying all the queries for Internet URLs. This puts an unnecessary extra load on this key corporate resource. If the Internet queries can be sent to the ISP, the load on the corporate DNS server will reduced. This feature accomplishes that functionality.

Figure 90. Topology for Split DNS



In the diagram above, DNS requests coming from hosts behind the router (EzVPN Remote), need to be sent out to the correct DNS server (ISP’s DNS or corporate DNS) based on domain name being queried for. For example, if a request is made to the Internet, this request will be sent to the ISP’s DNS server.

DHCP Client Proxy Support in EasyVPN

This functionality allows the EasyVPN server to assign a DHCP address to a client from the corporate DHCP Server rather than the local pool.

The Cisco IOS EzVPN server currently assigns an ip address to a client using either a local pool configured on the router or using the framed-IP-address attribute defined in radius. With this functionality, the EzVPN server will support DHCP for assigning ip address. The EzVPN server will act as a proxy DHCP client and acquire an ip address from the corporate DHCP server. The ip address will be pushed to the client.

The client supplies its hostname, in a mode configuration request. This should be forwarded to the DHCP server, so that DHCP servers that support Dynamic DNS (DDNS) registration will be able to register the hostname with the ip address assigned with the DDNS server. This will allow anyone in the corporate network to reach the client by its DNS hostname rather than an ip address.

Benefits

- **Increased Flexibility in Tunnelling IPsec Flows through Firewalls:** With cTCP, road warriors, operating out of hotels rooms, airports etc. can pass IPsec through third party firewall devices in their environments.
- **Reduced Load on Corporate DNS Servers:** With Split DNS, Internet queries can be sent to the ISP and the load on the corporate DNS server is drastically reduced. In some situations this reduction may be substantial such as home broadband connections used for home and telecommuting applications.
- **EasyVPN Client Reachability:** With DHCP Proxy functionality, it is now possible for branches to host servers behind the EasyVPN Clients. These servers will be assigned addresses from the corporate pool and will be reachable from any other host in the network. Further, if Dynamic DNS is enabled on the DHCP Proxy Server, these hosts would be reachable by their hostname. It is also useful for debugging purposes by system administrators trying to monitor VPN connections.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/easyvpn

Product Management Contact: Jai Balasubramaniyan (jsundar@cisco.com)

7.1.3) DMVPN Manageability Enhancements

DMVPN provides an easy and scalable way to create large and small IPsec VPNs by combining GRE tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP). Dynamic Multipoint VPN (DMVPN) enables zero-touch deployment of IPsec networks. DMVPN Spoke-to-Spoke Functionality is an enhancement that enables the secure exchange of data between two branch offices without traversing the head office. This improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

DMVPN functionality has been enhanced to allow easier manageability by including the following key features:

- Show commands dealing with DMVPN as a single entity
- Debug commands for debugging DMVPN session and NHRP
- Syslog commands to support DMVPN session, Crypto Socket and NHRP
- Traps to support DMVPN session, Crypto sockets, and NHRP

Benefits

- **Rapid Troubleshooting:** The combination of show/debug commands and Syslog and Traps information help to troubleshoot networking devices in DMVPN environments.
- **Ease of Management:** Syslog and Traps offer an easy method to identify critical network events for network operations as well as overall network management/operations.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Product Management Contact: ask-stg-ios-pm@cisco.com

7.1.4) Virtual Private Network (VPN) Advanced Integration Module (AIM) for Cisco 1841/2800/3800 Integrated Services Routers (ISRs)

Description

The Cisco VPN AIM optimizes the ISR platforms for virtual private networks in both IPsec and SSL WebVPN Deployments

This module is now designed to perform hardware based SSL Encryption for Cisco IOS WebVPN; the module also still supports VPN IPsec Encryption, Data Encryption Standard (DES&3DES) and Advanced Encryption Standard (AES 128, 192, 256), with the added hardware compression support of the IP Payload Compression Protocol (IPPCP). The ISR Router with AIM-VPN/SSL is ideal for use in small-to-medium sized businesses and small-to-large enterprise branch offices for connecting remote offices, mobile users, and partner extranets. The ISR VPN router is designed for both service provider managed-services Customer Premises Equipment (CPE) and Managed Security Service Providers (MSSPs). The ISR router together with the AIM-VPN/SSL module and Cisco IOS Advanced Security Feature set offers a rich, integrated package of routing, firewall, intrusion-protection system, and VPN functions. As an integral component of Cisco VPN solutions and the Cisco self defending network, the Cisco series VPN modules provide industry-standard encryption (IPsec), application-aware Quality of Service (QoS) and bandwidth management, together with robust perimeter security options.

Figure 91. AIM-VPN/SSL for Cisco 1841/2800/3800 ISRs

Benefits

Feature	Benefit
Offloads High Overhead IPsec Processing from the Main Processor	Reserves critical processing resources for other services such as routing, firewall, and voice.
IPsec MIB	The IPsec MIBs allow Cisco IPsec configuration monitoring and can be integrated in a variety of VPN management solutions.
Certificate Support Enables Automatic Authentication using Digital Certificates	Scales encryption use for large networks requiring secure connections between multiple sites.
VPN modules Easily Integrated into existing Cisco 1841, 2800, 3700 and 3800 Series Routers	Significantly reduces the system costs, management complexity, and deployment effort over multiple box solutions.
IPsec Provides Confidentiality, Data Integrity, and Data Origin Authentication	Enables the secure use of public-switched networks and the Internet for WANs.
Cisco IOS® WebVPN	WebVPN allows the ISR to be a single-box solution, unlike other vendor products that require multiple devices and management systems. WebVPN combined with the consolidated technology platform of the ISR, provides customers with unparalleled cost savings and competitive per-user pricing

Hardware

Routers	• Cisco 1841, 2800, 3700, 3800 Routers

Router	Part #	Description
1841	AIM-VPN/SSL-1	1841 DES/3DES/AES/SSL VPN Encryptions/Compression Module
2800	AIM-VPN/SSL-2	2800 DES/3DES/AES/SSL VPN Encryptions/Compression Module
3700	AIM-VPN/SSL-3	3700 DES/3DES/AES/SSL VPN Encryptions/Compression Module
3800	AIM-VPN/SSL-3	3800 DES/3DES/AES/SSL VPN Encryptions/Compression Module

Considerations

Requires Cisco IOS® Software with the Advance Security, Advance IP or Advanced Enterprise Feature Set

Additional Information:

http://www.cisco.com/en/US/products/hw/routers/products_promotion0900aecd8017150a.html

Product Management Contact: Kevin Sullivan (sullivan@cisco.com)

7.1.5) Cisco IOS WebVPN—Auto-Applet Port Forwarding Download

Description

The Cisco IOS WebVPN implementation has been enhanced to provide the ability to automatically download the Port Forwarding Applet at login time. Previously the user was required to click on “Start Application Access” on the portal page. This feature is configurable on the gateway under the group policy, as well as on the AAA server.

In the gateway, here is an example of the command line syntax:

```
policy group my_policy
  port-forward "email" auto-download
```

On the AAA server, administrator can define the following Cisco Attribute-Value (AV) pair under “Cisco IOS/PIX” section:

```
  port-forward-name=email
  port-forward-auto=1
```

Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

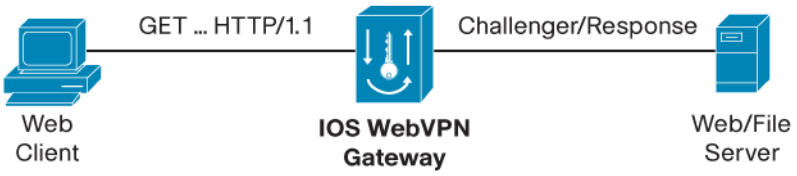
7.1.6) Cisco IOS WebVPN—HTTP Authentication

Description

The Cisco IOS WebVPN implementation has been enhanced to support HTTP Basic and NT LAN Manager (NTLM) authentication with password caching functionality. HTTP basic authentication uses a simple username/password scheme. NTLM employs a challenge-response mechanism for

authentication which is used by various Microsoft network servers. The Cisco IOS WebVPN gateway behaves as a proxy for the web client for HTTP authentication.

Figure 92. Cisco IOS WebVPN Authentication



Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

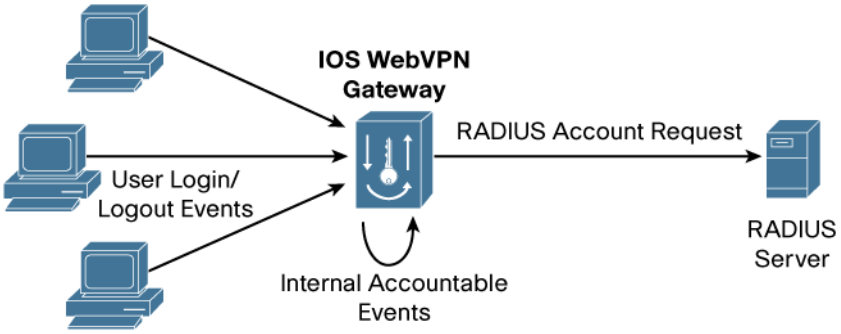
Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

7.1.7) Cisco IOS WebVPN—RADIUS Accounting

Description

The Cisco IOS WebVPN implementation has been enhanced to record user based session activity to a RADIUS server for auditing purposes. The user session start and stop accounting events are supported.

Figure 93. Cisco IOS WebVPN RADIUS Accounting



Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

7.2) Voice

7.2.1) Cisco Unified CallManager Express 4.0

Cisco® Unified CallManager Express provides call processing for Cisco IP phones for small office or branch office environments. It enables the large portfolio of Cisco ISRs to deliver IP telephony features that are commonly used by business users to meet the voice and video communications requirements of the small or medium-sized office. Cisco Unified CallManager Express enables the

deployment of a cost-effective, highly reliable communications system using a single ISR with Cisco IOS® Software for up to 240 users.

Unified CallManager Express key features:

- Support for either PBX or Key System functionality
- Support from 24 to 240 phones
- Legacy Telephony Features:
  - Call transfer, paging, intercom, call coverage
  - Call park, Music on Hold (MoH), night bell
  - Hunt groups, Basic Automatic Call Distribution (B-ACD) and reporting
  - Adhoc & “meet me” conferencing
  - Direct Inward Dial (DID), analog or digital trunks
  - Analog phone, fax and modem support
  - Integrated voice mail and auto-attendant with Cisco Unity Express
- Unified Communications Features:
  - Wireless phone (802.11) support
  - Single device for routing, switching, security and voice
  - Windows applications desk top Integration
  - HTML GUI application for admin changes
  - Networking between sites using H.323 or Session Initiation Protocol (SIP)
  - SIP Support

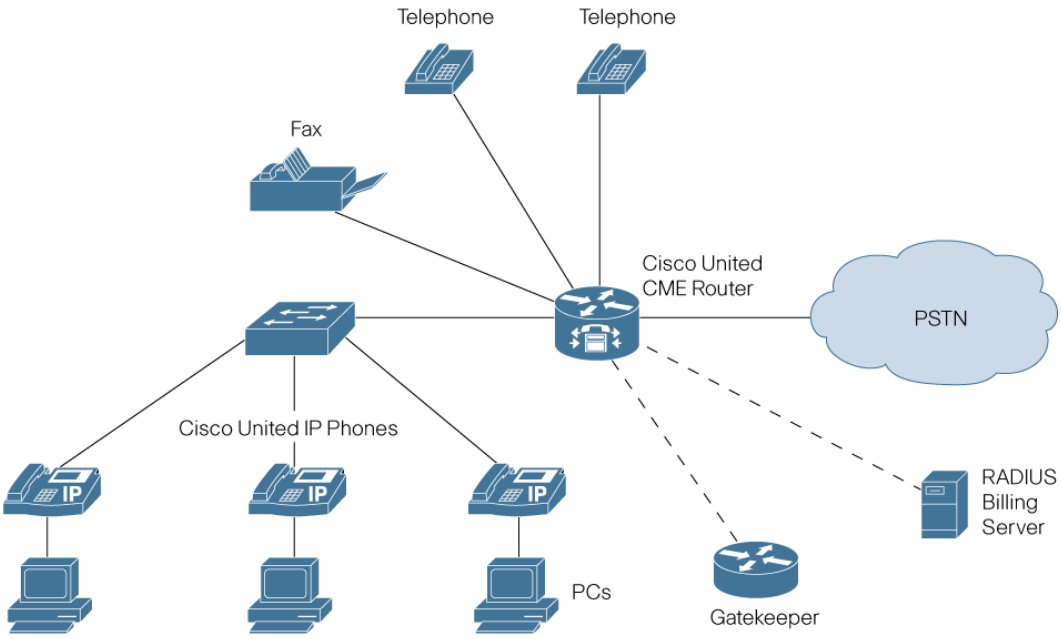
New features and enhancements with Cisco Unified CallManager Express 4.0:

- Legacy Telephony Features:
  - Dynamic login to hunt groups—answer B-ACD calls from any phone
  - B-ACD hunt group ready/busy mode (normal calls still allowed)
  - Optional Basic-ACD (B-ACD) reporting via Microsoft Excel template
  - Retain conference call when conference initiator drops
  - Night service call forwarding
  - Park call recall
  - Dedicated park slot per extension
- Enhanced Phone Features
  - Headset zip tone auto answer
  - Distinctive ring patterns for internal or external calls
  - Call coverage enhancements
- Integration with Legacy PBX
  - Support for Q.SIG protocol for support of basic calls and MWI to TDM-based PBX and voice mail
- Unified Communications Features
  - Remote tele-worker support over VPN
  - Video Telephony with Unified Video Telephony client

- IP Communicator 2.0 soft phone support
- Optional use of second router for redundancy

- Survivable remote site telephony fallback mode
  - Provide backup call control in branch office with centralized Cisco Unified CallManager telephony network
- New Phone Support
  - Cisco Unified IP Phone 7911G, 7941G, 7941G-GE, 7961G, 7961G-GE

Figure 94. Cisco Unified CallManager Express for the Small- and Medium-Size Office.



Benefits

- **Cost effective:** Deliver unified communications features plus routing and security all in a single Integrated Services Router reducing installation and maintenance costs for the small or medium-sized office.
- **Investment Protection:** Cisco Unified CallManager Express 4.0 interoperates with Cisco Unified CallManager and can be converted to Cisco Unified Survivable Remote Site Telephony as the business grows.
- **Breadth of Solution:** Wide variety of Cisco access router platforms, PSTN interfaces and IP phone endpoints to solve diverse problems.

Hardware

Routers	• Cisco 1751, 1760, 2600, 2800, 3700, and 3800 Series Routers • Cisco IAD 2430

Additional Information:

http://www.cisco.com/go/ccme

http://www.cisco.com/go/unified

http://www.cisco.com/go/isr

Product Manager:

Ron Lewis (ronlewis@cisco.com)

John Vickroy (jvickroy@cisco.com)

Or access-ccme-cue@cisco.com

7.2.2) Cisco Multiservice IP-to-IP Gateway—Hosted NAT Traversal

Description

The Cisco Multiservice IP-to-IP Gateway is used by service provider, enterprise, and small and medium-sized organizations to interconnect SIP and H.323 voice and video networks. The Cisco Multiservice IP-to-IP gateway provides organizations with all their Session Border Control (SBC) needs integrated into the network layer interoperating with many different network elements including voice gateways, IP phones, and call-control servers, in many different application environments, from advanced enterprise voice and/or video services with Cisco Unified CallManager or Cisco Unified CallManager Express, as well as simpler toll bypass and VoIP transit applications. The SBC provides a network-to-network interface point for signaling interworking, media interworking, security, billing, and QoS and bandwidth management. The SBC is also the critical component for scaling networks from single customer networks to an end-to-end IP network.

One application area for an SBC is in residential VoIP deployments which are on the rise. In this scenario as shown in Figure 82, when SIP phones are installed behind a home-router, NAT Traversal becomes an issue since home-routers typically only supports L3/L4 NAT. These routers typically do not inspect SIP packets or change the embedded information in these packets; hence SIP messages from/to SIP Proxy Server are not correctly routed back to the SIP endpoints.

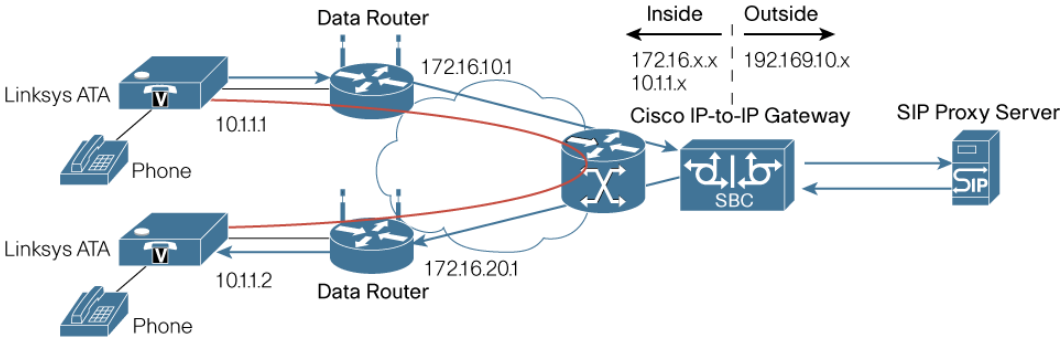
In order to preserve interoperability with the existing installed base of home routers, the Cisco Multiservice IP-to-IP Gateway introduces a Hosted NAT Traversal mode for resolving NAT traversal issue. With this functionality, the following sequences of actions occur:

1. The home router translates the Layer 3 IP address; the IP address in SIP messages is not translated by the home router.
2. In the hosted NAT Traversal mode, the IP-to-IP gateway intercepts these SIP messages, translates the embedded IP address, and sends the packet to the SIP Proxy Server.
3. Media traffic established between phones A and B flow around the IP-to-IP gateway (as shown by red line). Media traffic between phone A or phone B and the PSTN flows through the IP-to-IP Gateway.

With Release 12.4(9)T, Cisco Multiservice IP-to-IP gateway will support the following features:

- Hosted NAT Traversal for SIP phones
  - NAT-SIP SBC overlapping embedded address support
  - Support for SIP address-only fields which are presently left untranslated by NAT-SIP SBC
  - Support for media-flow-around & override-embedded addresses
- Supplementary service support for SIP-to-SIP calls based on REFER method
- AMR-NB codec support
- H.450.7 message waiting indication support
- AS5000XM Series platform support

Figure 95. Hosted NAT Traversal for SIP phones



Benefits

- **VoIP Interoperability:** Allows existing home routers used for service provider broadband applications to be used for VoIP.
- **VoIP Privacy:** Allows use of NAT with VoIP to preserve the privacy and identity of VoIP phones behind home routers.

Hardware

Routers	• Cisco 2600XMs, 2691, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router
Universal Gateways and Access Servers	• Cisco AS5000XM Series

Considerations

1. SIP phones supporting Symmetric Signaling and Media (ie: Linksys ATA) can be used behind the home router.
2. SIP phones not supporting Symmetric Signaling and Media, PAT should be disabled and traffic for port 5060 should be allowed to pass.
3. SIP Phones cannot have same IP Address
4. SIP Phones must send NAT keepalives to keep the home router's pin holes open.

Additional Information:
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a0080409b6d.html/

Product Management Contact:

Jennifer Blatnik (jennyng@cisco.com)

Jayesh Chokshi (jayesh@cisco.com)

7.2.3) Skinny Call Control Protocol (SCCP) Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateway

Description

SCCP Controlled Analog (FXS) ports with supplementary features in Cisco IOS Gateways allows customers to support natively in Cisco IOS Software all SCCP supplementary features previously only available on the Cisco VG224 including security based features such as v.150.1 secure modem relay and Multi-Level Priority and Precedence (MLPP) for US Government use. FXS ports

can now be controlled by Cisco Unified CallManager or Cisco Unified CallManager Express using SCCP protocol. Features supported include:

- Basic analog call
- Registration/de-registration with call control after Online Insertion/Removal (OIR) (Cisco 3845 ISR only)
- Switchover/switchback including Survivable Remote Site Telephony (SRST)
- Modem/fax pass through
- Call transfer
- Three way calling
- Call waiting
- Caller ID
- Call forward all and cancel call forward all
- Call pickup
- Speed dial
- Redial
- Private Line Automatic Ring-down (PLAR)
- Supervisory disconnect for loop start FXS ports
- Pulse dialing for loop start FXS ports (basic calls only)
- Audible Message Waiting Indicator (AMWI)

With Cisco Unified CallManager only, these additional features are supported:

- MLPP basic call
- BRI basic call
- Secure modem relay (v.150.1)
- Cisco Unified CallManager auto-configuration/download

Figure 96. CCP FXS Analog ports on Cisco ISR with Cisco Unified CallManager

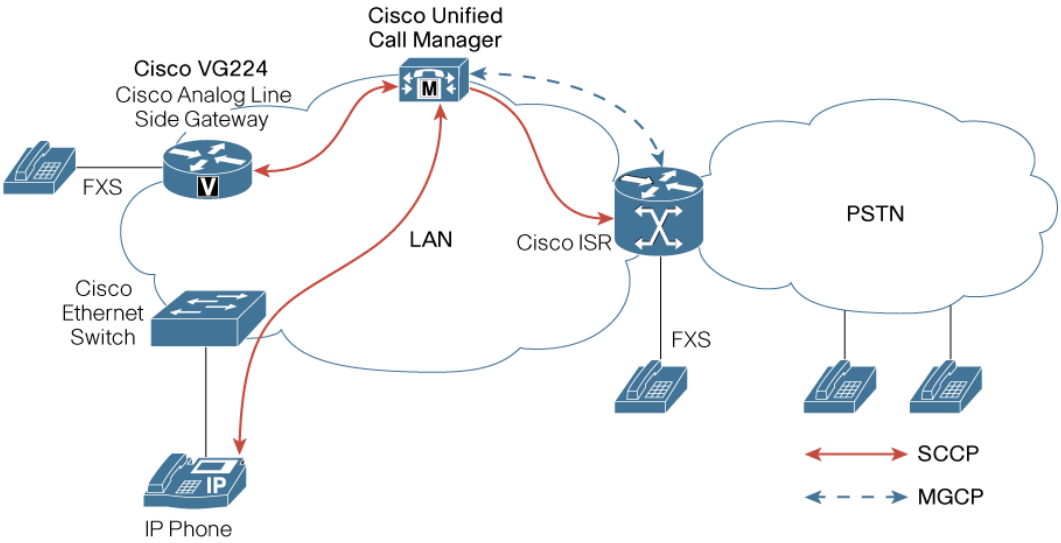
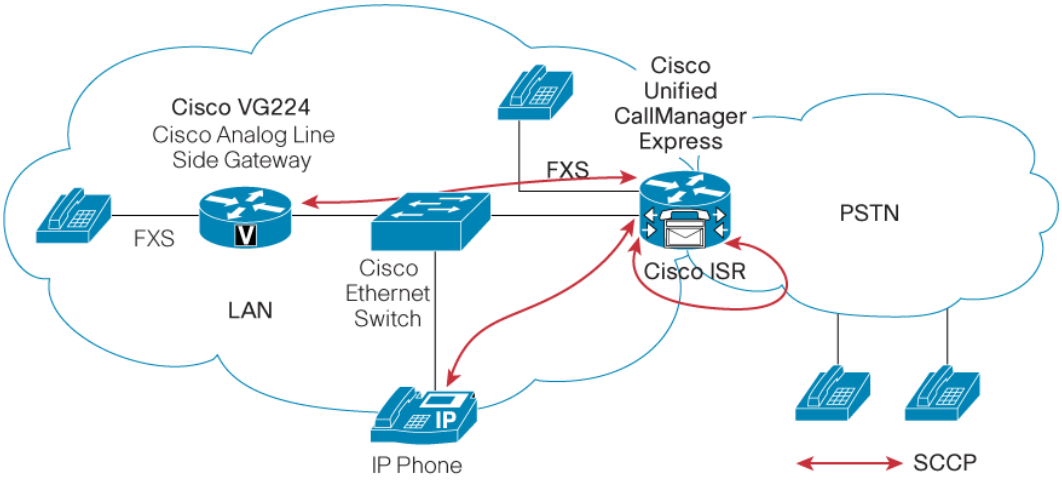


Figure 97. SCCP FXS Analog ports on Cisco ISR with Cisco Unified CallManager Express



Benefits

- **Analog Phone Interoperability:** Support for SCCP FXS analog ports on Cisco 2800 or 3800 Series Routers which can also act as a voice gateway, a Cisco Unified CallManager Express voice gateway, and/or a SRST gateway for end customers
- **Supplementary Feature Interoperability:** Supplementary feature interoperability with Cisco VG224 and Cisco IP Phones for Cisco Unified CallManager and Cisco Unified CallManager Express

Hardware

Routers	• Cisco 2800 and 3800 Series Routers
Network Module FXS carrier cards on Routers	• NM-HD-2V, NM-HD-1V, NM-HD-2VE • NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1 • EVM-HD-8FXS/DID, EM-HDA-8FXS, EM-HAD-3FXS/4FXO, EM-4BRI-NT/TE
Voice Interface Card (VIC) on routers or Network Modules	• VIC2-2FXS, VIC-4FXS/DID, VIC2-2BRI-NT/TE
Voice Gateways	• Cisco VG224

Considerations

1. FXS ports can either be in VIC slots on the Cisco 2800 or 3800 series chassis or in NM modules which are supported
2. SCCP FXS ports on Cisco 2800 or 3800 Series Routers are interoperable with Cisco Unified CallManager 4.1(3) and above
3. SCCP FXS ports on Cisco 2800 or 3800 Series Routers are interoperable with Cisco Unified CallManager Express 4.0 and above
4. MLPP basic call, BRI basic call, secure modem relay (v.150.1) were developed for specific use of the US Department of Defense (DoD)

Additional Information:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080483a76.html

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805f48e4.html

Product Management Contact:

Jennifer Blatnik (jennyng@cisco.com)

Jayesh Chokshi (jayesh@cisco.com)

7.2.4) High-Density Packet Voice for Cisco AS5400XM and AS5350XM Universal Gateways

Description

Cisco Systems® brings greater price/performance and higher density to the Cisco® AS5400XM and AS5350XM Universal Gateways with a new high-density packet voice/fax feature card and a new Digital-Signal-Processor (DSP) module. With these additions to the product line, the Cisco AS5400XM now offers increased capacity up to a full Channelized T3 (CT3) of voice calls with all codecs, and the Cisco AS5350XM offers 12-E1, 16-T1, and CT3 configurations using the G.711 codec.

The new Cisco High-Density Packet Voice/Fax Feature Card (part number AS5X-FC) for the Cisco AS5350XM and AS5400XM Universal Gateways supports up to six high-density packet voice/fax DSP modules, providing scalability from 64 to 384 channels.

The new Cisco High-Density Packet Voice/Fax DSP Module (part number AS5X-PVDM2-64) features the latest Cisco DSP technology, delivering up to 20-percent lower latency compared to earlier-generation DSPs to help ensure highest voice quality, and provides complete flexibility in channel allocation to achieve highest densities. The DSP module is a field-replaceable unit (FRU), making additions and servicing much easier while reducing downtime.

Figure 98. Cisco AS5350XM and AS5400XM High-Density Packet Voice/Fax Feature Card

Benefits

- **Enhanced call density per rack unit:** Expanded capacity makes the Cisco AS5400XM and AS5350XM Universal Gateways ideal for network operations centers and co-location sites where applications require high performance per port in a space-constrained environment. With support for tiered codec complexities, the Cisco High-Density Packet Voice/Fax Feature Card makes it easy to customize the voice-gateway DSP configuration to match individual network requirements. DSP resources are managed on a call-by-call basis to service all codec types (high, medium, and low complexity). The unique codec mix operating in the network determines the number of DSP modules required.
- **Commonality between service provider and enterprise networks:** Cisco AS5400XM and AS5350XM high-density packet voice/fax feature cards share common DSP technology with Cisco market-leading integrated services routers, facilitating the transparent integration between service provider and enterprise IP Communications networks and thereby offering new service provider revenue opportunities for managed and hosted services.

Hardware

Universal Gateways and Access Servers	• Cisco AS5400XM Universal Gateway • Cisco AS5350XM Universal Gateway

Additional Information:

http://cisco.com/en/US/products/ps6269/index.html

http://cisco.com/en/US/products/ps6268/index.html

Product Management Contact: Kathy Lewis (kalewis@cisco.com)

7.3) Management Instrumentation

7.3.1) Flexible NetFlow

Flexible NetFlow is the next-generation in flow technology allowing optimization of the network infrastructure, reducing operation costs, improved capacity planning and security incident detection with increased NetFlow flexibility and scalability.

NetFlow has become the standard for acquiring IP operational data for many customers. Visibility into the network is an indispensable tool. In response to new requirements and pressures, network operators are finding it critical to understand how the network is behaving including:

- Application and network usage
- Network productivity and utilization of network resources
- The impact of changes to the network
- Network anomaly and security vulnerabilities
- Long term compliance, business process and audit trail
- Understand who, what, when, where, and how network traffic is flowing

Applications for NetFlow data are constantly being invented but the key applications include:

- Real-time network monitoring
- Application and user profiling
- Network planning and capacity planning
- Security incident detection and classification
- Network data warehousing, forensics and data mining
- Troubleshooting
- Accounting and billing

Cisco is now innovating flow technology to a new level beyond what has been traditionally available. Cisco IOS Flexible NetFlow is Cisco's next-generation flow technology. Flexible NetFlow provides enhanced optimization of the network infrastructure, reduces costs, and improves capacity planning and security detection beyond other flow based technologies available today.

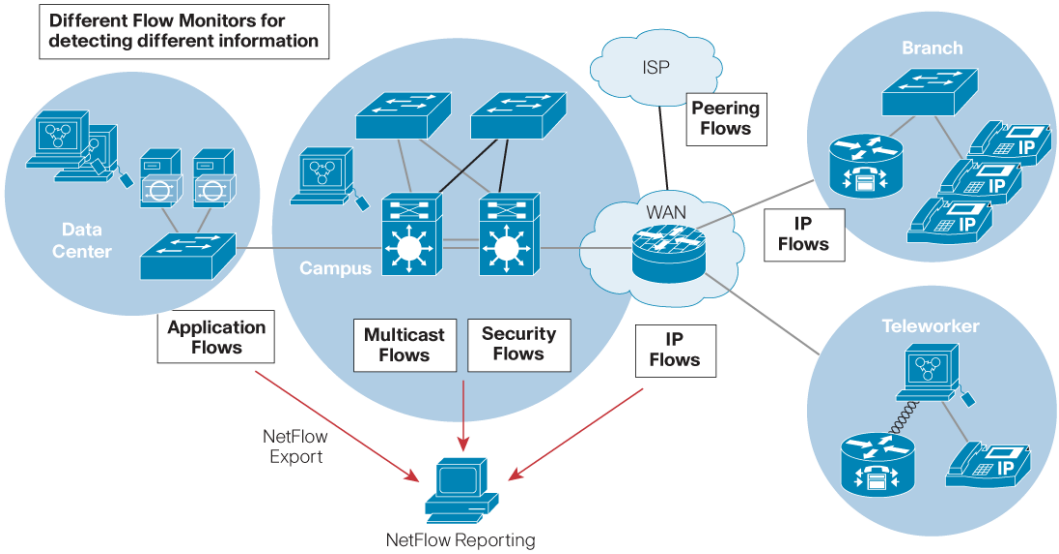
Key advantages to using Flexible NetFlow include:

- Flexibility, scalability, and customization of flow data
- The ability to monitor a wider range of packet information
- Enhanced network anomaly and security detection
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
- Convergence of multiple accounting technologies into one accounting mechanism

Flexible NetFlow has the ability to track multiple NetFlow applications simultaneously. For example, the user can create simultaneous and separate flow data for security analysis and traffic analysis.

Cisco IOS Flexible NetFlow provides enhanced security detection and or network troubleshooting by allowing customization of flow information. For example, the user can create a specific flow data to focus and analyze a particular network issue or incident. Cisco IOS Flexible NetFlow will enhance the already rich feature NetFlow capabilities allowing the tracking of information at layer 2 for switching environments, layer 3 and 4 for IP information and up to layer 7 with deep packet inspection for application monitoring.

Figure 99. Flexible NetFlow Customizable Flow Monitors



Benefits

- **Flexibility, Scalability, and Customization:** The user has the flexibility to select specific network information to be characterized by NetFlow. User selection improves usage and the scalability of NetFlow data.
- **Broad Range of Packet Tracking Options:** Flexible NetFlow allows the tracking of layer 2 though layer 7 packet information to provide the broadest range of flow monitoring information available.
- **Increased Visibility and Troubleshooting Capabilities:** Flexible NetFlow allows the creation of virtual flow monitors to provide more visibility and troubleshooting capabilities for improved specific network behavior and incident detection.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series Routers

Additional Information: http://www.cisco.com/go/netflow

Product Management Contact: Tom Zingale (tomz@cisco.com)

7.3.2) Cisco Networking Services (CNS) Security Enhancements

The Cisco Networking Services (CNS) Security Enhancement enables the authentication of end-user credentials in incoming CNS messages. The messages are formatted in the Simple Object Access Protocol (SOAP) where the SOAP header contains the sender's credential which is authenticated by a AAA server. When the CNS Security Enhancement is enabled, a device will reject CNS messages which do not have sender credentials.

For the messages sent from a device, CNS id will be sent in the username and CNS password will be sent in the password field. The value of CNS id is different for different agents. For example, the configuration agent's messages use the value of the config id while the image agent's messages use the value of the image id.

An error message will be sent as a result of failure in processing the security information in the SOAP header or authentication failures. Once the header is successfully processed, the application data in the body of the message will be processed by the specific agents.

Benefits

- **Secure Management:** Provides a secure environment for configuration and image management of network devices.
- **Consistent Security Mechanism:** The implementation of the SOAP message format and the associated security information in the SOAP header provides a consistent security mechanism across all of the CNS agents.
- **Standards Compliant:** SOAP is a lightweight protocol that is an industry standard for exchanging structured information in a decentralized, distributed environment.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, and 7200 Series Routers

Additional Information:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a00804402cd.html

Product Management Contact: Anita Freeman (anfreema@cisco.com)

7.3.3) Netconf Access for Configuration over SSH and BEEP
The NETCONF (Network Configuration) protocol defines a simple mechanism that allows: management of a network device; retrieval of configuration data; and manipulation/uploading of new configuration data. It uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages for the NETCONF protocol.

The NETCONF Server in Cisco IOS Software uses Secure Shell version 2 (SSHv2) or Blocks Extensible Exchange Protocol (BEEP) as the network transport to a NETCONF Network Manager. The NETCONF Network Manager acts as a NETCONF client to the NETCONF Server in Cisco IOS Software. The NETCONF Server in Cisco IOS Software has the ability to accept multiple client connections from different NETCONF Network Managers.

The userid and password of the SSHv2 session running NETCONF are used for authorization and authentication purposes. The user privilege level is enforced and the client session may not have full access to the NETCONF operations if the privilege level is not high enough. If AAA is configured, the AAA service is used identically as if a user had established a SSH session directly to the device. Using the existing security configuration makes the transition to NETCONF almost seamless.

For a Peer-to-Peer protocol, NETCONF over BEEP in Cisco IOS Software allows either the NETCONF Server or the NETCONF client to initiate the connection, thus supporting large networks of intermittently connected devices, as well as those devices that must reverse the management connection where there are firewalls and Network Address Translators (NATs).

The Simple Authentication and Security Layer (SASL) profile used by BEEP allows for a simple and direct mapping to the existing security model for CLI, while Transport Layer Security (TLS) provides a strong well tested encryption mechanism with either server or server and client-side authentication.

A new capability has been added to send notifications of any configuration change over NETCONF. A notification is an event indicating that a configuration change has happened. The change can be a new configuration, deleted configuration or changed configuration. The notifications are sent at the end of a successful configuration operation as one message showing the set of changes rather than individual messages for each line in the configuration that is changed.

Benefits

- **Secures Configuration:** Allows configuration over encrypted transports, SSHv2 or BEEP.
- **Simplifies Configuration:** NETCONF uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages for the NETCONF protocol.
- **Simplifies Migration:** Provides a natural migration from a CLI based configuration to a more powerful transactional based configuration by grouping CLI commands with the ability to back out the block of commands. The Cisco CLI is encapsulated using XML.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, and 7200 Series Routers

Product Management Contact: Anita Freeman (anfreema@cisco.com)

7.4) IP Routing

7.4.1.) Bidirectional Forwarding Detection (BFD) Echo Mode

The convergence of business-critical applications onto a common IP infrastructure in enterprise and service provider networks is becoming more common. Given the criticality of the data, these networks are typically constructed with a high degree of redundancy. While such redundancy is desirable to increase network availability, its effectiveness is dependant upon the ability of individual network devices to quickly detect failures and reroute traffic to an alternate path.

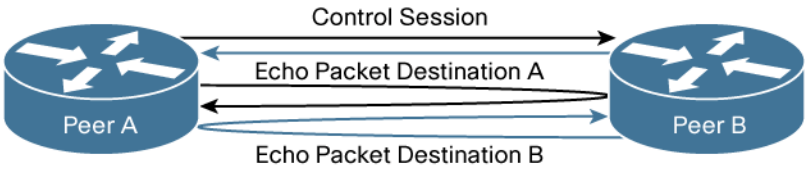
Routing protocol convergence is a key issue in these converged network designs since it determines the routes available to send data packets on and the reachability of the network. In order to maintain the integrity of routing data, it is vital to have accurate information regarding the status of links and whether they are up or down. Bidirectional Forwarding Detection (BFD) is a new, IETF standards based mechanism used to detect link failures for routing protocols. It addresses some of the important problems in link status detection such as:

1. Link Layer detection mechanisms vary significantly in the temporal resolution they offer for link status detection. Techniques like Automatic Protection Switching (APS) on SONET offer sub-50 ms resolution for the detection of link failures while Ethernet or traditional WAN link methods offer a few seconds of resolution at best.
2. Link Layer detection mechanism may not help with Layer 3 Network level failures. This is important when there is a routing flap in the routing protocol at Layer 3 but the underlying Layer 2 Link is fine.

3. Typical mechanisms that work at Layer 3 offer 15-20 seconds of temporal resolution for failure detection times. This is slow in terms of times which applications require for network connectivity to be maintained.

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD delivers fast router peer failure detection times independent of all media types, encapsulations, topologies, and routing protocols including EIGRP, IS-IS, OSPF, and BGP (single-hop peers over Ethernet interfaces). Cisco currently supports the BFD Asynchronous mode, which depends on the sending of BFD control packets between two systems for liveness detection between the forwarding engines of the BFD neighbors. With this release, Cisco enhances BFD with support for an Echo Mode Adjunct to the Asynchronous mode. The Echo Mode adjunct allows each router peer in a BFD session to send Echo packets with their own IP address as the destination address. These Echo packets loop back from the corresponding BFD router peer to provide the status of the BFD router peer. The major benefit of the Echo Mode is that it can reduce the burden of sending control packets for multiple BFD sessions for a head end router. For example, if a head end router is a BFD peer with 10 remote routers, it will need to send out 10 control packets to maintain the state of the BFD peers. With Echo Mode, this burden is reduced in that the interface only has to loopback the Echo packets in the data plane versus consuming the processing power at the control plane with the sending of control packets.

Figure 100. BFD Echo Mode packet exchange



Benefits

- **Fast, Sub-second Failure Detection:** This is useful to maintain the integrity of the network for time-sensitive applications.
- **Faster Route Convergence:** The fast failure detection from BFD allows routing protocols to converge faster to increase network availability.
- **Low Overhead, Lightweight Protocol:** This minimizes the consumption of resources at the control plane and allows distribution of packet handling in the data plane.
- **Routing Protocol Independent:** BFD works with EIGRP, OSPF, IS-IS, and BGP (single-hop peers over Ethernet interfaces).

Hardware

Routers	• Cisco 7200 Series Router • Cisco 7301 Router

Considerations

The BFD implementation also supports full interoperability between Version 0 and Version 1 implementations. With this release, Cisco now supports the BFD Version 1 implementation. The Echo Mode is an adjunct to the Asynchronous mode; it is available only with Version 1.

Product Manager: Tanya Shastri, (tanyas@cisco.com)

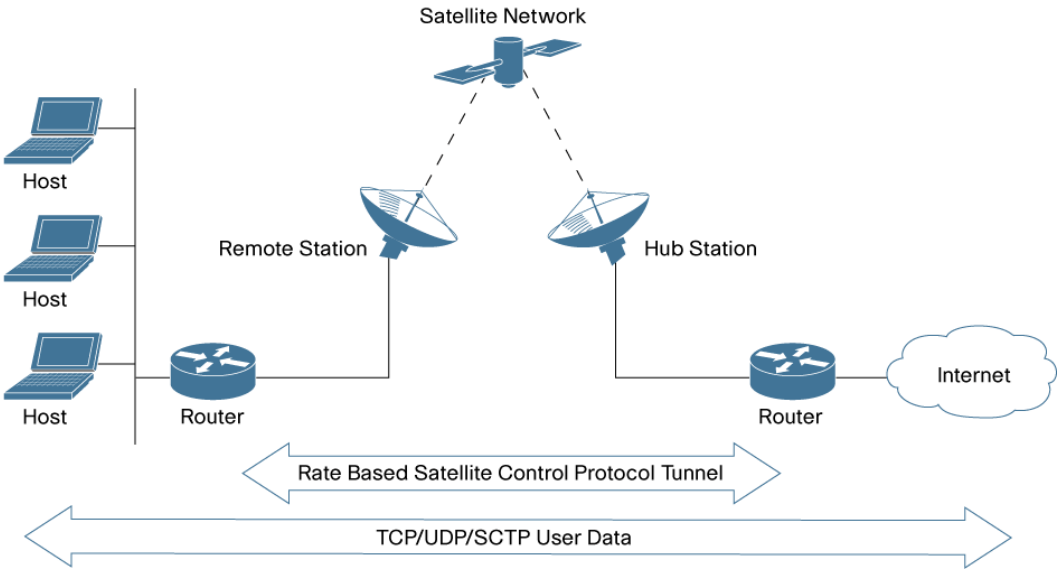
7.4.2) ACL-based Rate Based Satellite Control Protocol (RBSCP)

Rate Based Satellite Control Protocol (RBSCP) was designed for wireless or long-distance delay links with high error rates, such as satellite links. RBSCP has been designed to preserve the end-to-end model and provide performance improvements over a satellite link. Using tunnels, RBSCP allows two routers to control and monitor the sending rates of the satellite link, thereby increasing the bandwidth utilization. Lost packets are retransmitted over the satellite link by RBSCP preventing the end host TCP senders from going into slow start mode. RBSCP improves the performance of certain IP protocols, such as TCP and IP Security (IPsec), over satellite links without breaking the end-to-end model.

ACL-based support for RBSCP provides the ability to make RBSCP sub-features (such as TCP ACK splitting, TCP and Stream Control Transport Protocol (SCTP) window scaling) available on an access list basis that can be selectively applied to any output interface.

This feature reduces the tunneling and queuing overhead associated with RBSCP tunnels by allowing only ACL selected traffic to use RBSCP. Additional benefits include the ability to use TCP header compression and better QoS, since the TCP and SCTP headers are no longer hidden inside the RBSCP/IP headers.

Figure 101. RBSCP Topology



Benefits

- **Improved Performance:** By reducing the tunneling and queuing overhead associated with RBSCP tunnels, router performance is improved.
- **Improved QoS:** The ability to use TCP header compression allows better QoS, since the TCP and SCTP headers are no longer hidden inside the RBSCP/IP headers.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers

Product Management Contact: Tanya Shastri (tanyas@cisco.com)

7.4.3) Open Shortest Path First version 3 (OSPFv3) IPsec ESP Encryption and Authentication
In order to ensure that OSPF for IPv6 (OSPFv3) packets are not altered and re-sent to the router, causing the router to behave in a way not desired by its managers, OSPFv3 packets must be authenticated and/or encrypted. OSPFv3 requires the use of IPsec to enable authentication and/or encryption of routing exchanges. OSPFv3 relies on the IPv6 IPsec Authentication Header (AH) and Encapsulating Security Payload (ESP) to ensure integrity, authentication, and confidentiality of routing exchanges.

This functionality adds the support for:

- ESP authentication and encryption (including virtual links)
- AH support for virtual links

Note: AH was supported in prior releases—with this functionality, AH for virtual links is also supported.

Crypto images are required to use this functionality. This is because only the crypto images have the IPsec API needed for use with OSPFv3.

Benefits

- **Secures OSPFv3 Routing Exchanges:** Ensures the integrity, authenticity, and confidentiality of the OSPFv3 routing exchanges sent between routers.
- **Prevents DoS Attacks:** Enhanced and granular protection against DoS attacks targeting routing infrastructure routers.

Hardware

Routers	• Cisco 1700, 1800, 2691, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information:

The draft-ietf-ospf-ospfv3-auth-07 describes the means/mechanisms to provide authentication/encryption to OSPFv3 using IPv6 AH/ESP Extension Header.

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00801d660d.html - wp1154380

Product Management Contact: Chetan Khetani (cpk@cisco.com)

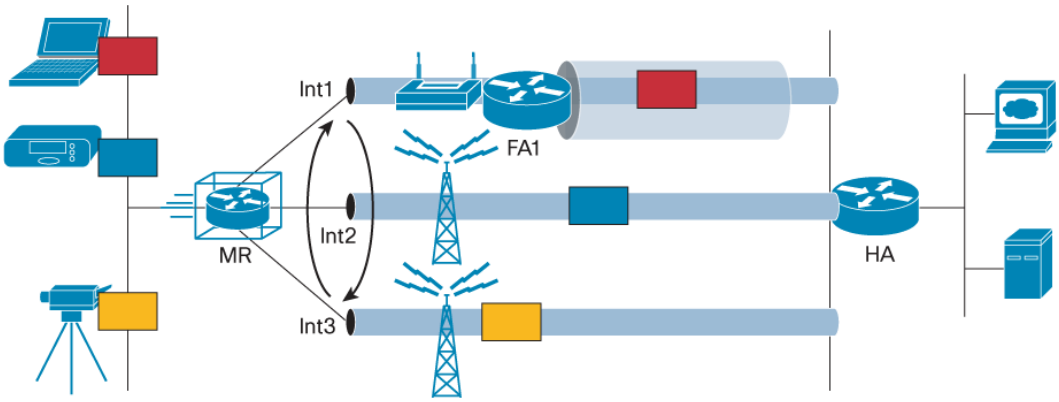
7.5) Mobility

7.5.1) Mobile IP—Mobile Router Multi-path Support
Cisco Mobile Router (MR), a Cisco IOS Software router running Cisco Mobile Network technology, currently supports seamless mobility via one mobile tunnel only at a given time. A MR chooses one of its roaming interfaces, such as WiFi, EVDO, or UMTS, based on the administratively configurable priority to establish a network connection. The Home Agent (HA), which is on the other side of the Mobile IP tunnel, also supports one tunnel connection only per mobile node or per mobile router. These restrictions prevent a MR from utilizing all of its interfaces even when the network connectivity through those interfaces is available. This, in turn, prevents users from utilizing all the possible bandwidth while they are on the road.

The Multi-path support for Mobile Router feature allows a MR and a HA to establish multiple Mobile IP tunnels over all available roaming interfaces. When this feature is enabled, the MR will try to register through all of its available roaming interfaces to the HA. Each registration is independent of the other registrations taking place on the other roaming interfaces. Once registered through the roaming interfaces, the mobile router will have multiple routes or multiple path to the HA—assuming the Mobile IP reverse tunnel feature is configured. The mobile traffic from or to the mobile network will be load balanced among the multiple routes based on the CEF load balancing algorithms, either per packet or per destination (default). In addition, this feature supports unequal load balancing. The unequal load balancing is weighted based on the bandwidth of the roaming interfaces. For example, if the bandwidth of one roaming interface is 100kbps and the bandwidth of the other roaming interface is 1 Mbps, the mobile traffic will be routed 10 times more through the 1Mbps link than through the 100kbps link.

This feature supports networks with or without foreign agent. Since the mobile router is registering independently on each of its roaming interfaces, it may also use a foreign agent to register on one interface and a collocated care-of address to register with the HA on a different interface.

Figure 102. Three Mobile IP tunnels are established between a Mobile Router (MR) and a Home Agent (HA) over 3 roaming interfaces. Traffic is load balanced across the three tunnels.



Benefits

- **Better Investment Protection:** Allow users to use existing and/or purchased wireless connections
- **Increased Bandwidth:** Allow users to combine multiple low speed connections together to obtain higher bandwidth for support of new services

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3200, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers, MWR, MWAM
Universal Gateways and Access Servers	• Cisco AS5000 Series

Considerations

This feature does not support multiple roaming interfaces terminated on the same Foreign Agent.

Product Management Contact: Richard Shao (rshao@cisco.com)

7.6) IP Services

7.6.1) Enhanced Object Tracking (EOT) Support for Carrier Delay

Enhanced Object Tracking (EOT) provides complete separation between the objects to be tracked and the action to be taken by a client when a tracked object changes. Thus, several clients such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) can register their interest with the tracking process, track the same object, and each take different action when the object changes. Each tracked object is identified by a unique number that is specified on the tracking Command-Line Interface (CLI). Client processes use this number to track a specific object.

In this release, the interface “Carrier Delay” parameter is now taken into account for reporting interface states into Enhanced Object Tracking (EOT). This allows taking “Carrier Delay” into account to report interface states in protocols. No change to the “Carrier Delay” configuration is required to activate the feature.

Benefits

- **Increases Network Availability:** Allows better tracking of objects for key router functionality like HSRP or GLBP to increase network availability, speed network recovery, and decrease network outages and their duration.
- **Allows Carrier Delay in EOT:** Carrier Delay is now taken into account with EOT, so the interface is not prematurely reported up or down.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers, MWR, MWAM
Universal Gateways and Access Servers	• Cisco AS5000 Series

Additional Information:

EOT Product Literature:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbeb.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

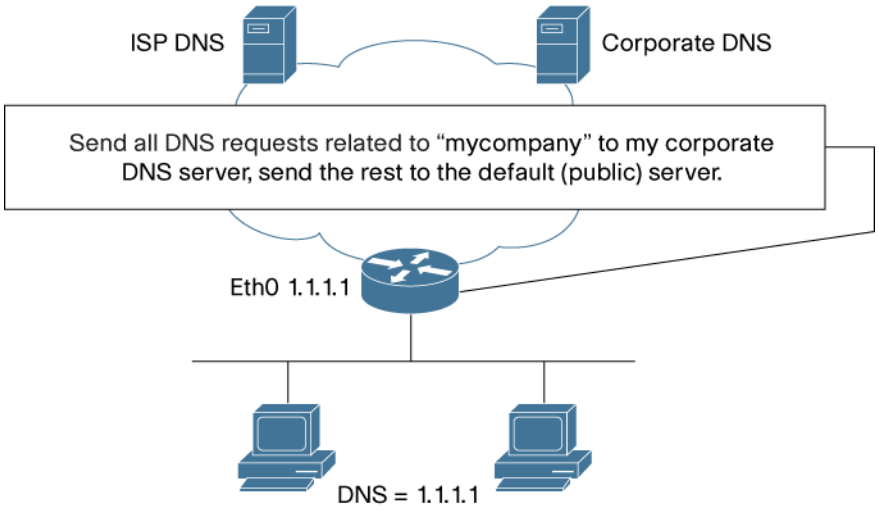
7.6.2) Domain Name Service—Split DNS

Domain Name System (DNS) is a standard that defines a domain naming procedure used in TCP/IP. A domain is a hierarchical separation of the network into groups and subgroups with domain names identifying the structure. The named groups consist of named objects, usually devices like IP hosts, and the subgroups are domains.

In this release, Split DNS is introduced as a mechanism to direct DNS queries to specific DNS servers based on different criterions when the router acts as a DNS forwarder or resolver. The concept of DNS view is also introduced to offer a list of criteria to select the DNS servers and specific DNS parameters associated with those criteria. DNS view parameters are applied to a DNS query if all the criteria match. Possible criteria are:

- Domain name pattern
- Source IP address of the query
- Virtual Route Forwarding (VRF)

Figure 103. Split DNS Topology



Benefits

- **Reduced DNS Server Utilization:** Allows selective use of corporate DNS servers and offloads these servers for non-corporate related traffic.
- **Allows Client-based DNS Resolution:** A variety of mechanisms are available to allow DNS clients to select DNS servers and queried parameters.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers, MWR, MWAM
Universal Gateways and Access Servers	• Cisco AS5000 Series

Additional Information:

VRF aware DNS:
http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008051d2af.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

7.7) High Availability

7.7.1) Hot Standby Router Protocol—HSRP Group Shutdown

The Hot Standby Router Protocol (HSRP) is a First-Hop Redundancy Protocol (FHRP) designed to allow for transparent fail-over of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

In this release, HSRP Group Shutdown allows for automatically disabling an entire HSRP group when a tracked object from Enhanced Object Tracking (EOT) declares the HSRP Group to be down. This avoids the sending of packets to an HSRP Group when it is not operational.

Benefits

- Increases Network Availability—Allows shutting down an HSRP group to avoid packet loss in an inactive HSRP group.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers, MWR, MWAM
Universal Gateways and Access Servers	• Cisco AS5000 Series

Additional Information:

HSRP Product Literature:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

8) Release 12.4(6)T Highlights

Table 26. Release 12.4(6)T Feature Highlights

8.1) Hardware Support	8.2) Cisco IOS Security	8.3) Voice	8.4) High Availability
8.1.1) G.SHDSL WAN Interface Card (WIC-1SHDSL-V3)	8.2.1) Cisco IOS Firewall Enhancements 8.2.2) Cisco IOS Web VPN 8.2.3) Scalability Enhancements for Dynamic Multipoint VPN with Next Hop Resolution Protocol-Cisco Express Forwarding 8.2.4) Complete Certificate Chain Validation in Cisco IOS Public Key Infrastructure 8.2.5) Enhanced Online Certificate Status Protocol in Cisco IOS Public Key Infrastructure 8.2.6) EasyVPN Password Aging via Authentication, Authorization and Accounting 8.2.7) EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client 8.2.8) Secure Multicast 8.2.9) Control Plane Logging 8.2.10) Management Plane Protection 8.2.11) Network Address Translation ARP Ping	8.3.1) Cisco Resource Reservation Protocol Agent for Call Admission Control 8.3.2) Local Voice Busyout and Advanced Local Voice Busyout Enhancements 8.3.3) Cisco Text Relay for Baudot Text Phones 8.3.4) Extended Session Initiation Protocol- Session Initiation Protocol Support on the Cisco Multiservice IP-to-IP Gateway 8.3.5) In-Service Updates to Gatekeeper Zone Prefix Configuration 8.3.6) Packet Mode Services on D Channel 8.3.7) Skinny Call Control Protocol Private Line Automatic Ringdown with DTMF Out Pulse Digits for FXS Analog Phones 8.3.8) Session Initiation Protocol Gateway Support for Busyout 8.3.9) Session Initiation Protocol Transport Layer Security (TLS) Support	8.4.1) Cisco Gateway Load Balancing Protocol for IPv6 8.4.2) Hot Standby Router Protocol—Multiple Group Optimization

8.5) Management Instrumentation	8.6) IP Routing	8.7) IP Services	8.8) VPN	8.9) Connectivity
8.5.1) Cisco IOS IP Service Level Agreements—Label Switched Path Health Monitor 8.5.2) Cisco IOS IP Service Level Agreements—ICMP Jitter Operation 8.5.3) Cisco IOS IP Service Level Agreements: Real Time Protocol-based Voice over IP Operation 8.5.4) Multiprotocol Label Switching Label Switched Path Ping and Label Switched Path Traceroute	8.6.1) Enhanced Interior Gateway Routing Protocol for IPv6 8.6.2) Routing Information Protocol Version 2: RFC 1724 MIB Extension 8.6.3) Open Shortest Path First Version 2 RFC 3623 Graceful Restart—Helper Mode	8.7.1) Dynamic Host Configuration Protocol Option 82—Per Interface Support	8.8.1) ANI Suppression During L2TP Set-Up for the Cisco AS5000 Series	8.9.1) Asynchronous Transfer Mode Oversubscription for DSL 8.9.2) Private VLAN Edge on Cisco 1800 Fixed Configuration Routers

8.1) Hardware Support

8.1.1) G.SHDSL WAN Interface Card (WIC-1SHDSL-V3)
The new G.SHDSL WAN interface card provides 1-port symmetric high-bit-rate DSL (SHDSL) connectivity to

a WAN. The new interface card is the latest G.SHDSL-based WIC for Cisco modular routers. It supersedes existing interfaces (part numbers WIC-1SHDSL and WIC-1SHDSL-V2) while maintaining feature parity with WIC-1SHDSL-V2.

The G.SHDSL WAN Interface Card is available in Cisco IOS Software Releases 12.4(5), 12.4(2)XA, and 12.4(6)T on Cisco access routers.

Figure 104. G.SHDSL WAN Interface Card (WIC-1SHDSL-V3)

Benefits

- High-speed, symmetrical WAN connectivity
- Lower monthly cost than traditional WAN circuits
- Single or dual-pair copper wires
- Provides businesses the necessary bandwidth for critical traffic
- Opportunities for integrating voice and data traffic on the same WAN link
- Service providers can bundle services and offer differentiated service levels agreements (SLAs)

Hardware

Routers	• Cisco 1721, 1751, 1760, 1841, 2600XM, 2691, 2801, 2811, 2821, 2851, 3725, 3745, 3825, and 3845 Routers

Product Number: WIC-1SHDSL-V3

Additional Information:
http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a00800921f0.html

Product Management Contact: Subbu Mahadevan (smahadev@cisco.com)

8.2) Cisco IOS Security

8.2.1) Cisco IOS Firewall Enhancements

Cisco IOS Firewall integrates stateful firewall and application inspection functionality as part of a complete set of threat defense features offered on Cisco routers. Routers with integrated firewalls enable cost-effective and easy-to-deploy security solutions at every access point in the network. A firewall combined with other integrated router security capabilities allows new classes of solutions to connect mobile workers, branch offices, telecommuters, partners and customers into the network.

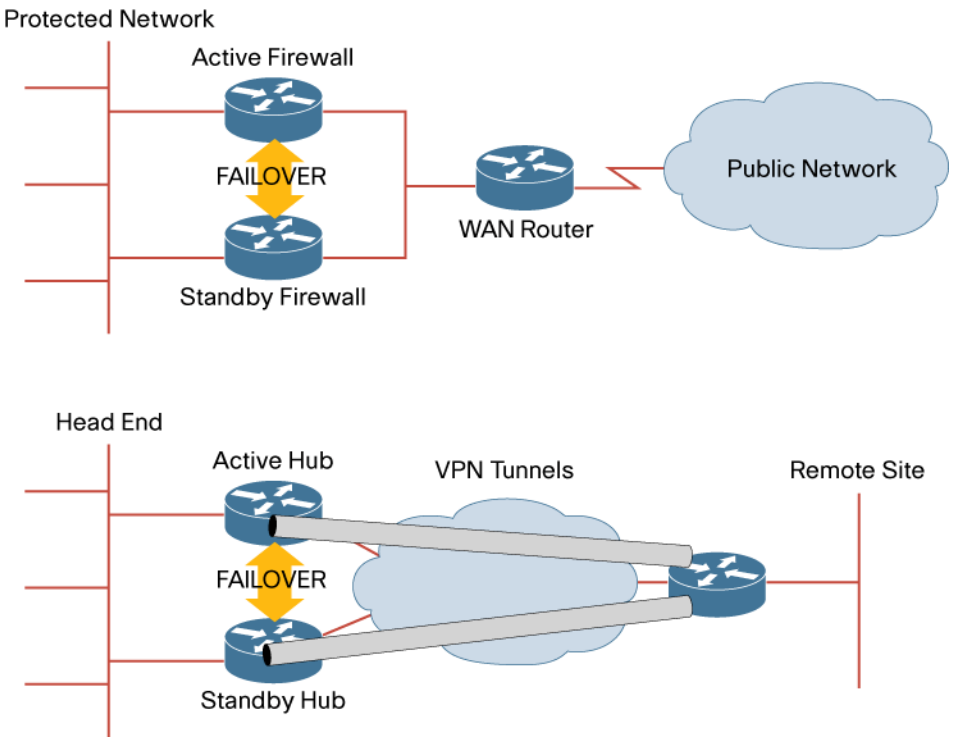
Release 12.4(6)T introduces a series of enhancement to Cisco IOS Firewall:

- Firewall Stateful Failover
- Zone-Based Policy Configuration
- Cisco Unified Firewall MIB

Firewall Stateful Failover

Firewall Stateful Failover enables Active/Standby failover between two routers for Firewall functionality. This functionality works in conjunction with Hot Standby Router Protocol (HSRP) on either LAN or VPN links to maintain Firewall session state, and to enable active connections to continue during a router or circuit failure. This enables a highly available Firewall solution that maximizes network uptime and security.

Figure 105. Topology for Firewall Stateful Failover for both LAN and VPN Applications.



Hardware

Routers	• Cisco 3700, 3800, and 7200 Series

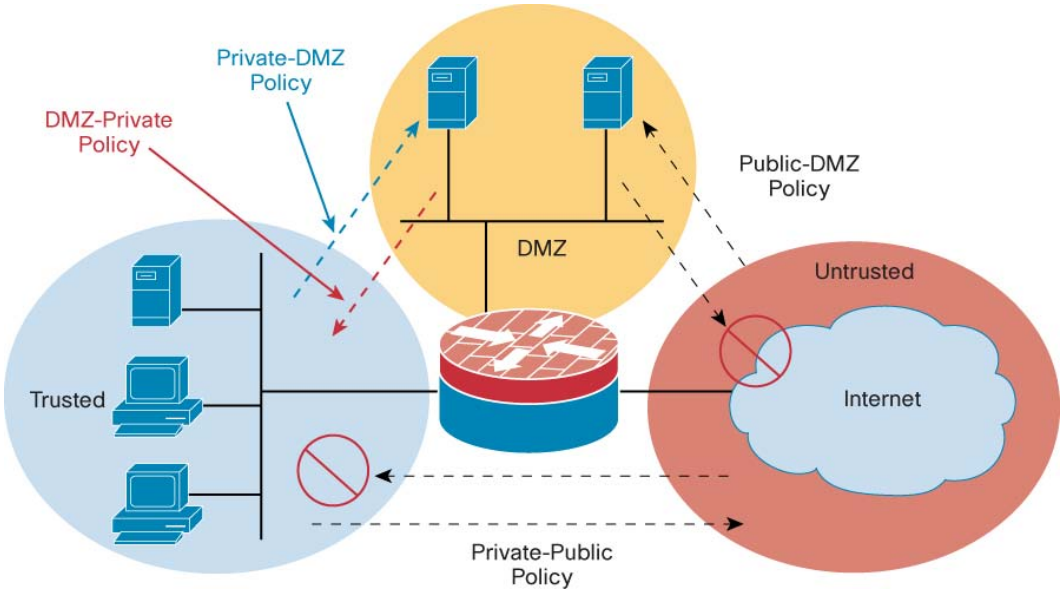
Zone-Based Policy Configuration

Improved firewall policy configuration means network administrators can more easily understand the effect of firewall policies on network traffic. This functionality allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones enables the application of Firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface. With this functionality, configuration is easier to understand, which enables:

1. Firewall policies that are configured on traffic moving between zones
2. Simplified troubleshooting, as inter-zone traffic can be used to test different firewall policies

Zone-to-zone policies can apply differing policies to different groups of hosts or networks based on ip address lists. This offers more granular application of security policies and allows easier integration of security policies with network management applications.

Figure 106. Zone-Based Policy Configuration



Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Cisco Unified Firewall MIB

The Cisco Unified Firewall MIB offers a unified SNMP standards based monitoring interface for functionality on all Cisco Firewall products: Cisco IOS Firewall, Cisco PIX, and Cisco Firewall Service Blades for Catalyst platforms. The Unified Firewall MIB offers statistics collection and monitoring for Stateful Packet Inspection, URL Filtering, and Application Inspection.

Benefits

- Highly available firewalls with maximum network uptime and security
- Simplified and more granular firewall policy application
- Easier integration of security policies with network management applications
- Cost-effective integrated firewall and security solutions with simplified deployment

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Product Management Contact: Jonathan Gohstand (jgohstan@cisco.com)

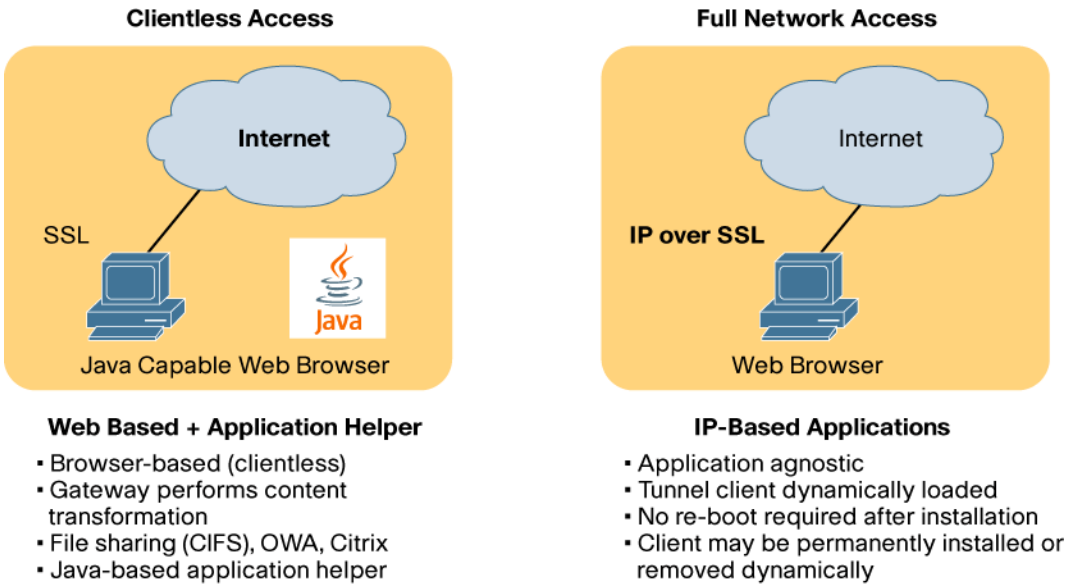
8.2.2) Cisco IOS Web VPN

Cisco IOS WebVPN is a Secure Socket Layer (SSL) based VPN solution that provides “clientless” remote-access by employing a web browser as the remote user’s VPN client. A web browser has already been installed on most personal computers, so no further application installation is required to securely access network resources. Cisco IOS WebVPN makes it easy to deploy remote access to internal applications on a single integrated network device. It delivers comprehensive endpoint and network security with Cisco Secure Desktop for endpoint security and integrated network security features like firewall, access controls, intrusion prevention, and application control. Cisco IOS WebVPN offers a clean, cost-effective SSL VPN solution capable of host assessment, malware protection, privacy and post-session clean-up.

WebVPN in Cisco IOS Software supports two functional modes:

- Clientless mode provides secure access to private web resources, and will provide access to web content. This is useful for accessing most content that would generally be accessed via a browser (ie: Internet, databases, or online tools).
- Network Access mode supports virtually any application with a persistent “LAN-like” connectivity via the Cisco SSL VPN Client that is dynamically and transparently loaded on the remote host.

Figure 107. WebVPN Solution Overview



Benefits

- Uses a standard web browser to access the corporate network without the installation of additional clients on the client machine
- SSL encryption native to browser provides transport security
- Accessible from non-corporate machines, such as airport kiosks
- Easy firewall/network traversal from any location
- Seamless wireless roaming
- Integrated network security features (ie: firewall, access controls, intrusion prevention, and application control)
- Clientless: standard HTML content transformation, native Citrix support, Java based application helper, and Windows file shares
- Security and Device Manager (SDM) provides a simple GUI based provisioning and management with step-by-step wizards for turn key deployment.
- Cisco Secure Desktop prevents digital leakage, protects user privacy, and integrates with desktop guest permissions, without complicated implementation or management
- Virtualization and VRF awareness: pool resources while masking the physical attributes and boundaries of the resources

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Considerations

If WebVPN needs to be enabled on the router that is running HTTP Secure Server, the administrator must configure an IP address for WebVPN using the “gateway-addr” keyword option of the “webvpn enable” command.

Complex Web content may not work with Clientless mode and therefore may require the use of Network Access mode.

Additional Information: http://www.cisco.com/go/webvpn/

Product Management Contact: Gary Sockrider (ask-stg-ios-pm@cisco.com)

8.2.3) Scalability Enhancements for Dynamic Multipoint VPN with Next Hop Resolution Protocol-Cisco Express Forwarding

DMVPN control protocol Next Hop Resolution Protocol (NHRP) RFC2332, and its interaction with Cisco Express Forwarding is optimized to allow:

1. **Route Summarization**

   In a DMVPN network, the hub is the central repository for routing information. All spokes send their routes to the hub and the hub redistributes these routes to all of the other spokes. Prior to these enhancements, all individual routes were required to learn from the spoke routers must be sent to all of the other spoke routers. Each spoke had to have full routing information about the networks behind all other spokes, in order for a spoke to build spoke-spoke dynamic tunnels. This enhancement eliminates this requirement and allows the hub router to summarize the routing information that it advertises to the spokes routers. It also maintains support for dynamic spoke-spoke tunnels.

   The Route summarization is enabled on the hub router to reduce the routing load on the hub router, and the routing table size on the spoke router. An additional benefit of route summarization is that the number of routes advertised decreases dramatically from a hub to a spoke.

2. **Increase in scalability of a DMVPN Spoke-Spoke**

   This increase in scalability occurs when multiple hub routers are enabled when using the Open Shortest Path First (OSPF) routing protocol. Prior to this feature in order to get the correct routes on the spoke routers to support dynamic spoke-spoke tunnels OSPF had to be use “broadcast” network mode. Because of this we couldn’t have more then two hub routers. This feature, allows OSPF point-multipoint network mode to be used on a DMVPN network which removes the restriction of not allowing more then two hubs, yet still allowing dynamic spoke-spoke tunnels. Note: Both before and after this feature the DMVPN network must be configured in the same OSPF area.

3. **Increase in scalability of a DMVPN Network**

   The increase in scalability of a DMVPN network, by relaxing the requirement that the hub routers be connected in a loop (daisy chain). The daisy chaining requirement was needed to forward NHRP protocol packets and some data packets between the hubs. This feature allows the forwarding of these packets between the hubs to be more direct, rather then having to travel around the complete chain of hub routers. For example a DMVPN network with 8 hubs would require that an NHRP resolution request/reply travel the complete 8 hub chain resulting in a total of 8 hops. With this feature you can configure a primary hub that is connected to all 8 secondary hubs, in which case an NHRP resolution reply/request would travel via the primary hub, 4 hops total, to get between any pair of secondary hubs. This also allows the creation of multi-level hierarchical hub-and-spoke DMVPN networks, which can better match the DMVPN network structure with the pattern of data flow.

Benefits

Previous Limitation	New Feature	**Benefits**
Large routing tables at the spokes can cause network instability	Route Summarization	Improve network and bandwidth utilization
Delays in setting up voice calls between spokes	Voice packets Cisco Express Forwarding switched via hub	Reduced latency during call setup
Complex interconnection of hubs to expand DMVPN Spoke-to-Spoke Networks Single point of failure	Simplified hub network design	Improved resiliency Failure of a single hub will not affect the rest of the DMVPN network

Hardware

Routers	• Cisco 800, 870, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series • Cisco 7301 Router

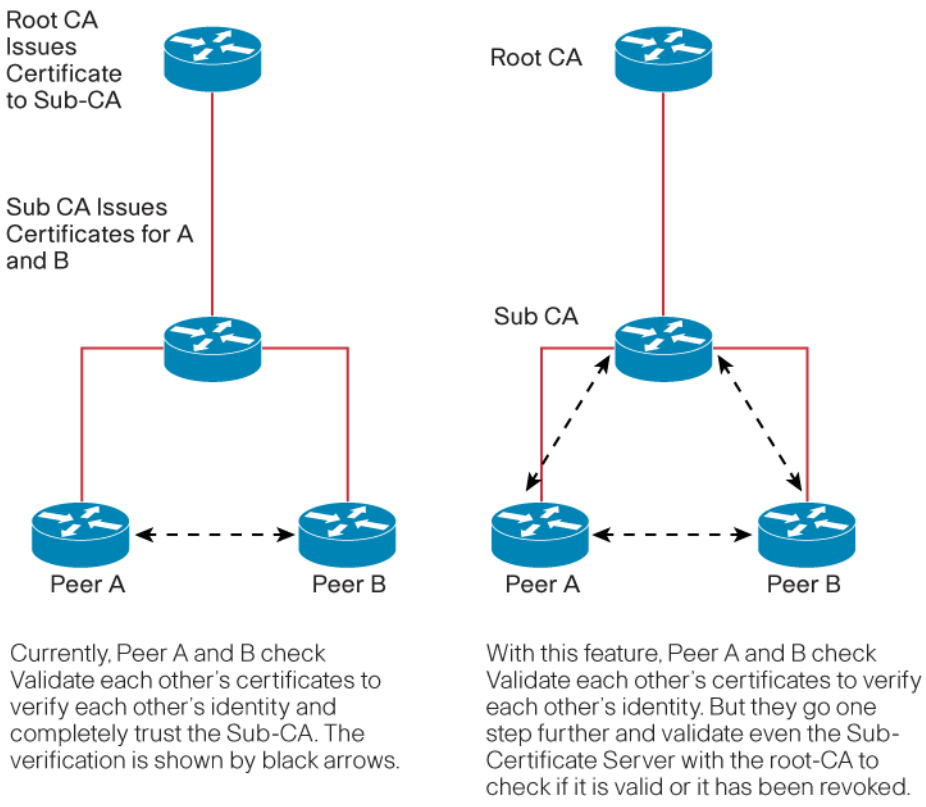
Product Management Contact: Siva Natarajan (ask-stg-ios-pm@cisco.com)

8.2.4) Complete Certificate Chain Validation in Cisco IOS Public Key Infrastructure

Cisco IOS Public Key Infrastructure (PKI) deployments currently validate the first trusted certificate. If the trustpoint that issued the certificate is a sub Certificate Authority (CA), it may be required to validate the certificate from the parent's trustpoint settings. The Complete Certificate Chain Validation enables full path processing via enhanced CLI.

For Example: If the trustpoint issuing the certificates to the two peers is a sub Certificate Authority, it may be necessary to verify its authenticity by contacting either the root CA server or some other trustpoint to see if it has been revoked or not for added security.

Figure 108. Complete Certificate Chain Validation in Cisco IOS PKI



Benefits

- Strengthens peer PKI credentials by verifying the authenticity of the sub Certificate Server that has issued PKI credentials

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

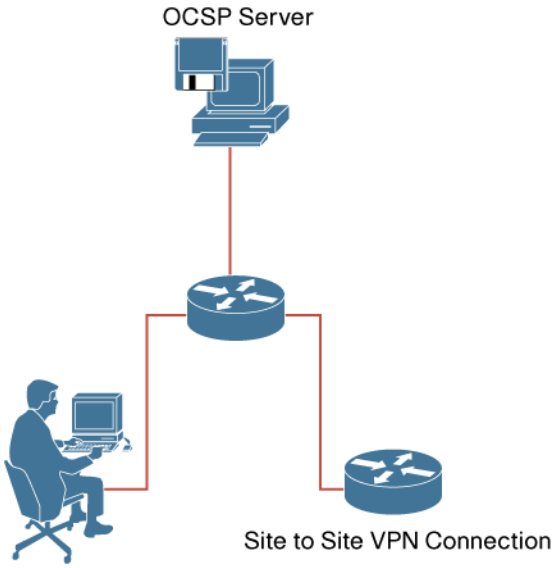
8.2.5) Enhanced Online Certificate Status Protocol in Cisco IOS Public Key Infrastructure

Conventional Public Key Infrastructure (PKI) deployments check the Certification Revocation Lists (CRLs) residing on the end host to validate a certificate. Online Certificate Status Protocol (OCSP) provides an alternative to CRLs that determine the status of a certificate. For example, when a user attempts to access a server, OCSP sends a request for certificate status information and responds back to the user on the status of the certificate. This overcomes the chief limitations of CRLs: it eliminates the need to download updates frequently. This also creates a more scalable infrastructure for determining the validity of certificates.

Other enhancements enable the recognition of different trust models, including Self-Signed Certificates and certificates signed by non root-CA, when branch offices maintain their own OCSP servers.

PKI Clients should be flexible enough to recognize these trust models for OCSP Servers where the certificate has been granted by authorities other than the root-CA server.

Figure 109. Enhanced Online Certificate Status Protocol in Cisco IOS PKI



Benefits

- Scalable alternative to CRLs
- Supports multiple OCSP servers in branch office scenarios in a Cisco IOS PKI network
- Flexibility in trust models of OCSP enable self signed certificates and certificates signed by CA Servers other than root

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

8.2.6) EasyVPN Password Aging via Authentication, Authorization and Accounting
EasyVPN environments currently initiate authentication by the software client/router connecting the end user. These Password Authentication Protocol (PAP)-based clients would send the username and password to the EasyVPN Server, which in turn would generate an Authentication, Authorization and Accounting (AAA) request to an authentication server (ie: Cisco ACS, Microsoft AD Server). If the password has expired, the authentication server would reply back with an authentication failure. The reason for the failure is not passed back to the user, so the user will not know that it was due to password expiration.

With EasyVPN Password Aging via Authentication, Authorization and Accounting, Authentication Servers can notify the client that the password has expired, while providing a generic way for the end user to change the password. This feature will work with the Cisco ACS as well as Microsoft AD server (which calls for support of the MSCHAPv1/v2 authentication support).

Benefits

- User has the opportunity to change expired passwords without administrator intervention
- Identifies the cause for authentication denial

Hardware

Routers	• 800, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

8.2.7) EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client
EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client enhances the Cisco IOS EasyVPN server to push firewall policies to Personal Firewall products integrated with the Cisco EasyVPN Software Client running on the client's computer. This functionality has been tested with personal firewalls (ie: Cisco Security Agent, Cisco Integrated Client Firewall software, and Zone Labs—ZoneAlarm®).

Configuration Policy Push (CPP) is not a replacement for a perimeter firewall; rather, it creates another layer of security in remote access VPN installations and aids the administration by allowing one to push specific firewall policies to the end hosts. A split tunnel at the client end enables access to corporate network, while at the same time, exposes the clients to attacks from the Internet. The objective of this feature is to provide additional security to the clients, so that the VPN Concentrator/EasyVPN Server can make a decision to allow/deny the IPsec tunnel, if the client does not have the required firewall policy.

The EasyVPN client initially proposes the firewall functionality it supports to the Server. Based on the firewall policy configured on the Server, it will either accept one of the policies proposed by the client, proceed with no client firewall support or terminate the tunnel setup. The firewall configuration policies are configured on the Server, and these will be sent to the client. The client enforces firewall policies.

Figure 110. EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client

Benefits

- Improves security against split tunneling, by enabling Cisco IOS EasyVPN Servers to configure Personal Firewalls on client machines
- EasyVPN Servers can choose to disallow clients that do not have the latest firewall configuration policies from joining the VPN Network

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

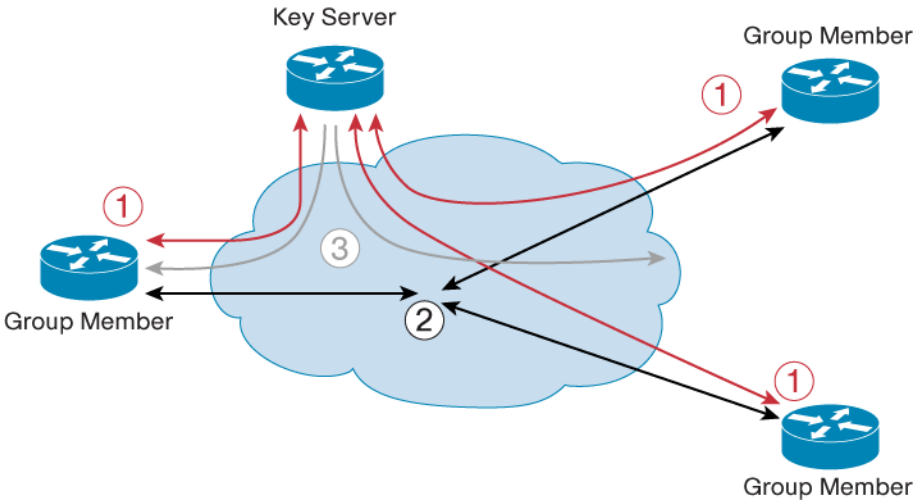
8.2.8) Secure Multicast

Secure Multicast is a set of features necessary to secure IP Multicast group traffic originating on, or flowing through, a Cisco IOS Software device. Secure Multicast combines the keying protocol Group Domain of Interpretation (GDOI) with IPsec encryption to provide users an efficient method to secure IP Multicast group traffic. It enables the router to apply encryption to non-tunneled (ie: “native”) IP multicast packets and eliminates the requirement to configure tunnels to protect multicast traffic.

Secure Multicast relies on the following two Internet standards:

GDOI is defined as the ISAKMP Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a “Group Controller/Key Server” (GCKS), which establishes security associations among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in the IETF by RFC3548. The topology shown in the figure below and the corresponding bullets explain how this protocol works:

Figure 111. Secure Multicast



Topology 1 illustrates the protocol flows necessary for group members to participate in a group:

1. Group members register with the key server. The key server authenticates and authorizes the group members, and downloads the IPsec policy and keys necessary for them to encrypt and decrypt IP multicast packets.
2. Group members exchange IP multicast packets encrypted with IPsec.
3. As needed, the key server pushes a re-key message to the group members. The re-key message contains new IPsec policy and keys to use when old IPsec Security Associations (SAs) expire. Re-key messages are sent in advance to SA expiration time to ensure that there are always valid group keys available.

Cisco IOS IPsec is a well known RFC (RFC 2401) that defines an architecture to provide various security services for traffic at the IP layer. IETF RFC 2401 describes the components and how they fit together with each other and into the IP environment.

A variety of IP multicast applications benefit from the encryption of native IP multicast packets. For a complete list of applications, visit http://www.cisco.com/go/multicast/.

Benefits

Previous Limitation	New Feature	**Benefits**
No native Multicast encryption	Standard and Flexible Framework implementing a Tuneless architecture	Framework offers unprecedented flexibility (e.g. supports Multicast and Unicast) Day 1 transparent interoperability between various core Cisco IOS technologies
No security for native multicast in Multicast VPN (mVPN) type architectures	Native Multicast encryption	Supports Multicast encryption in mVPN architectures
The value of the “Core” network mitigated Single point of failure	Leverage core for Multicast replication	New Architecture leverages the core and investment costs spent on building core

Hardware

Routers	• Cisco 800, 870, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Product Management Contact: Siva Natarajan (ask-stg-ios-pm@cisco.com)

8.2.9) Control Plane Logging

Control Plane Protection enables users to filter and rate-limit the packets going to the router's control plane, and discard malicious and/or error packets using features such as Control Plane Policing, port-filtering and queue-thresholding. The Control Plane Logging feature adds a way to allow logging of the packets dropped or permitted by these features.

Benefits

- The ability to log packets destined to a router's control-plane
- Enables identification of what is permitted or denied by the deployed Control Plane Protection policy
- Assists in developing and refining Control Plane Protection policies by identifying control-plane traffic

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 and 7301 Series Routers • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, and 2691 Routers

Additional Information:

- http://www.cisco.com/go/nfp
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/htcpp.htm

Product Management Contact: Dan Hamilton (ask-stg-ios-pm@cisco.com)

8.2.10) Management Plane Protection

Management Plane Protection (MPP) enables user to restrict the interfaces on which network management packets can enter a device. With this feature, network operators can designate one or more router interfaces as management interfaces. Device management traffic can enter a device through these management interfaces. After MPP is enabled, no interfaces except the designated management interfaces will accept network management traffic destined to the device.

Benefits

- Greater access control for managing a device than allowing management protocols on all interfaces
- Improved performance for data packets on non-management interfaces
- Simplifies the task of using per-interface ACLs to restrict management access to the device
- Fewer ACLs needed to restrict access to the device
- Management packet floods on switching and routing interfaces are prevented from reaching the CPU

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 and 7301 Series Routers • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, and 2691 Routers

Additional Information: http://www.cisco.com/go/nfp

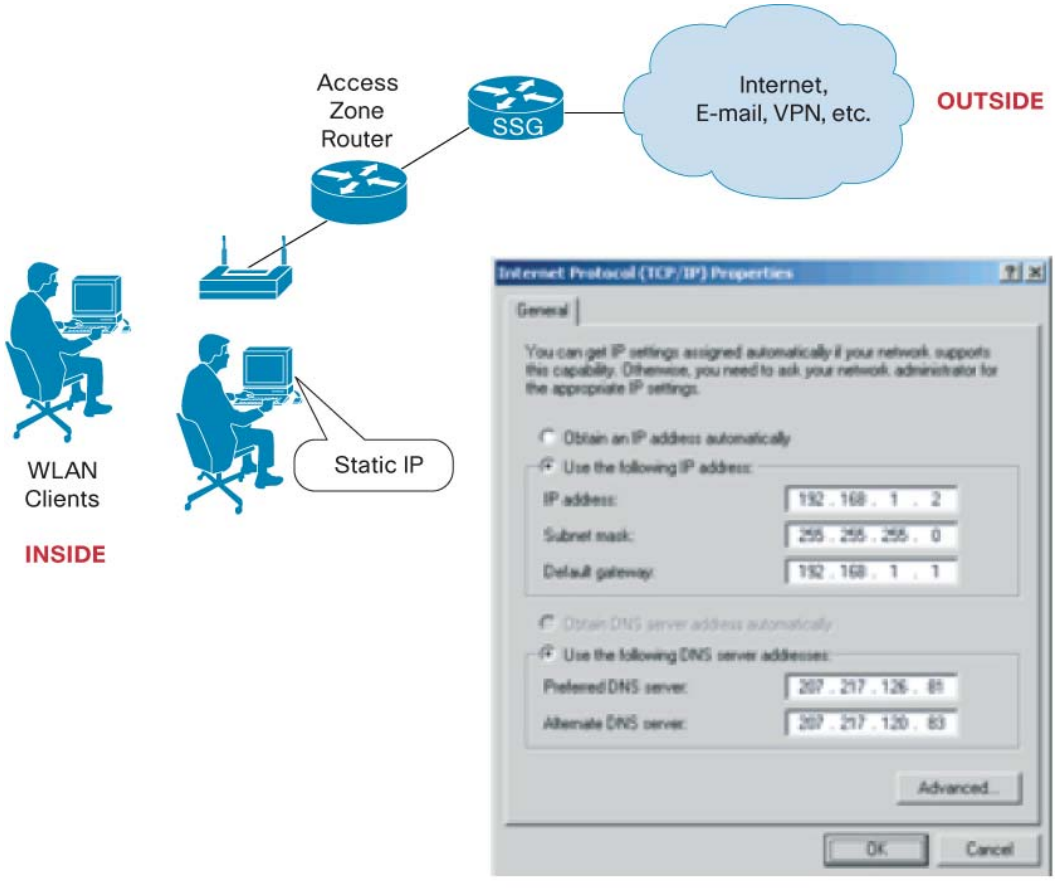
Product Management Contact: Dan Hamilton (ask-stg-ios-pm@cisco.com)

8.2.11) Network Address Translation ARP Ping

The existing WLAN-Network Address Translation (NAT) feature running at the Access Zone Routers (AZRs) allows users with Static IP address, who do not want to change their IP address, to continue using services of the public Wireless LAN provider. WLAN-NAT will create NAT entries for Static IP clients, and also provide them a routable address. NAT ARP Ping will address additional supports for the existing WLAN-NAT feature.

ARP Ping: With the current WLAN-NAT design, when the Static-IP client's NAT-entry times-out, the NAT entry and the secure-ARP entry associated to this client are deleted. An ACCOUNTING-STOP message will be sent to the Service Selection Gateway (SSG) and the Static-IP client's RADIUS object is removed. Re-authentication with the SSG is needed for the same client to again gain access to the services. With the new requirement, the NAT entry and the secure-ARP entry should not be deleted when the Static-IP client still exists in the network with its IP address for which it was authenticated. An ARP Ping is necessary to determine Static-IP client existences and to restart the NAT-entry timer.

Figure 112. NAT ARP Ping



Benefits

- The static IP configured laptop devices can work seamlessly with the wireless LAN infrastructure without changing the laptop settings.

Hardware

Routers	• Cisco 800, 17/1800, 2600XM, 2800, 3700, 3800, 7200, and AS5000 Series Routers • Cisco 7301 Router

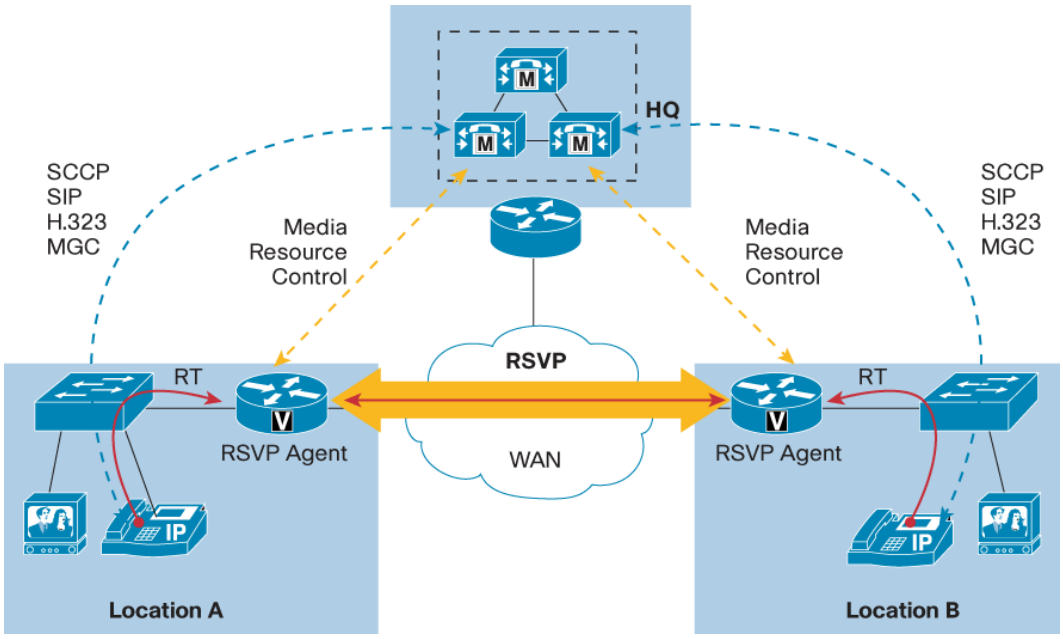
8.3) Voice

8.3.1) Cisco Resource Reservation Protocol Agent for Call Admission Control
Cisco Resource Reservation Protocol (RSVP) Agent for Call Admission Control (CAC) uses the network to deliver call admission control in conjunction with Cisco Unified CallManager deployments. RSVP Agent enables dynamic adjustment to changes in the network, supports complex network topologies, and enables unified voice, video, and data network designs.

CAC enables users to accept or reject a call based on bandwidth and policy considerations. RSVP, an IETF standards-based signaling protocol for reserving resources in the IP network, secures and reserves bandwidth across the WAN for calls accepted by the RSVP Agent. The resulting user experience is superior Quality of Service (QoS) and reliability for calls amid meshed network and multi-tiered networks.

Call set-up is initiated between the IP phone, IP videophone or gateway and Cisco Unified CallManager as shown in Figure 100. Cisco Unified CallManager classifies the call based on parameters such as application (voice or video) or Multilevel Precedence and Preemption (MLPP) and signals to the RSVP Agent in the access router. Bandwidth pools are pre-configured in the router on a per-application and per interface basis using the RSVP Application ID (RFC 2872). This allows VoIP and Video applications to use independent resources and avoid contention which could degrade Quality of Service (QoS). Using the classification provided by Cisco Unified CallManager, the RSVP Agent attempts to set-up a call within the appropriate bandwidth pool and across the WAN to a far-end RSVP Agent for the receiving party. If RSVP bandwidth is secured, the RSVP Agent signals back to Cisco Unified CallManager. Cisco Unified CallManager in turn signals to the IP phone, IP videophone or gateway and the call proceeds. If RSVP bandwidth can not be secured, the RSVP Agent signals back to Cisco Unified CallManager. Call handling policies are applied by Cisco Unified CallManager and the call is either disallowed or allowed to proceed but on a best efforts basis. Mid-call policies may also be applied for handling of changes to the media stream such as transfers during the course of a call.

Figure 113. Operation of RSVP Agent for CAC



Network design using the RSVP Agent allows voice and video calls to proceed as part of a single unified network together with data. This allows for support of meshed designs, multi-tiered designs, adjustment to dynamic link changes and redundant links. Hub and spoke limitations are removed. With a single design the cost for both infrastructure and management is reduced. Because CAC is managed and secured as a part of the network, there is no reliance on end-user IP devices. RSVP Agent functions independent of the call signaling protocol and hence SIP, SCCP, H.323 and MGCP are all supported.

Key Features and Benefits

- **Complex network topologies:** RSVP Agent provides CAC for complex and dynamically changing network topologies. Both the logical and physical network design for voice, video and data can now be the same. This simplifies deployments and reduces the cost for both infrastructure and management.
- **Locations capability:** RSVP Agent functionality may be enabled and disabled based on locations. This enables RSVP Agent to co-exist together with locations-based CAC and eases migration to RSVP Agent implementations. Locations capability also allows for a choice to not use the RSVP Agent for local calls that do not cross the WAN.
- **End-user device independent:** RSVP Agent is managed and secured as part of the network and does not rely on end-user devices to secure CAC. This eliminates concerns of end-point trust, and also preserves investment in existing IP phones.
- **Call signal independence:** RSVP Agent supports calls made using SIP, SCCP, H.323 and MGCP.
- **Application ID (RFC 2872):** RSVP Agent allows separate bandwidth pools to be established based on application. As a call is initiated Cisco Unified CallManager assigns the call an application ID and signals this to the router. The call is then placed using the appropriate bandwidth pool. This feature ensures that a single application (e.g. video) does not overwhelm the available reserved bandwidth.
- **Interface configuration:** RSVP bandwidth pools can be configured on a per interface level.

- **New call policy:** A choice of policies may be configured in Cisco Unified CallManager to require RSVP or in the event RSVP can not be secured to allow for best efforts. Separate policies may be configured for audio and video.
- **RSVP is not required on every hop:** The RSVP Agent secures a reservation across the WAN. Routers along the media path that support RSVP provide a bandwidth guarantee. Routers along the path that do not have RSVP enabled (e.g. in the network core) do not guarantee bandwidth but do pass the RSVP reservation. Hence, the RSVP Agent serves to control admittance to the network and secure bandwidth guarantees across those elements of the network where this is critical. Networks may be designed to implement RSVP at the edge and combine this with packet marking in the network core.
- **MLPP:** RSVP Agent works in conjunction with MLPP to allow high priority calls to take precedence and receive guaranteed bandwidth when needed.

Hardware

Routers	• Cisco 2600XM, 2800, 3700, and 3800 Series • Cisco 2691 Router

Considerations

Requires Cisco Unified CallManager 5.0

Standards Support

RFC 2872—Application and Sub Application Identity Policy Element for Use with RSVP

Product Manager: David Sauerhaft (dsauerha@cisco.com)

8.3.2) Local Voice Busyout and Advanced Local Voice Busyout Enhancements
The enhancements to Local Voice Busyout (LVBO) and Advanced Local Voice Busyout (AVBO) allow for the one to busyout based upon the registration status of an H.323 gateway to an H.323 gatekeeper, and the ability to busyout gracefully after an active call has been terminated on the voice-port. In addition, capability has been added to allow the busyout monitor gatekeeper command in the voice class busyout configuration mode for monitoring a large number of IP interfaces for voice.

This allows consistency of feature application under the voice-port or the voice class busyout configuration modes.

Customers monitoring a non-trivial number of local IP interfaces or remote IP interfaces using IP SLA probes often use the “voice class busyout” method of LVBO/AVBO configuration to simplify their work, especially if the same busyout criteria must be applied to several voice-ports. Providing consistency for the added busyout monitor gatekeeper CLI will simplify their ability to monitor a large number of these interfaces.

Benefits

- Reduces operational overhead by simplifying the configuration via the voice class busyout command line interface (CLI)
- Allows for the consistent application of voice busyout features

Hardware

Routers	• Cisco 2800 and 3800 Series

Considerations

- Busyout options can not be applied directly to the voice port if already configured under the voice class busyout configuration.

Additional Information:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba7.html

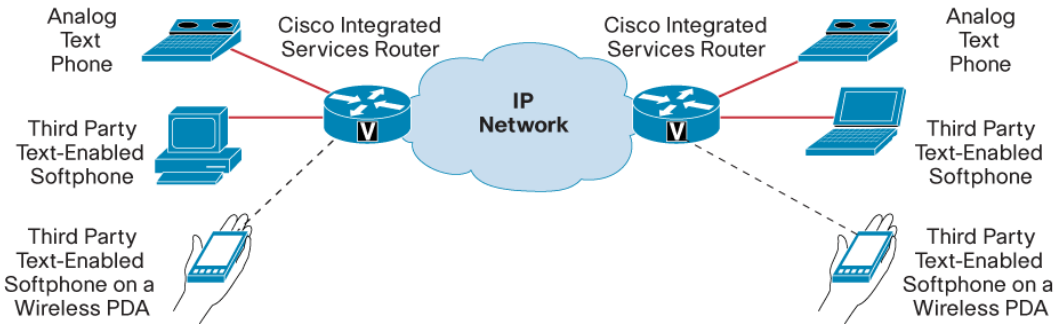
Product Management Contact: Sarat Khilnani (skhilnan@cisco.com)

8.3.3) Cisco Text Relay for Baudot Text Phones
Cisco Text Relay implements a mechanism for transporting Text Telephone (TTY) signals over Voice over IP (VoIP) calls in a highly reliable manner. Text Telephones (TTY), or Telecommunication Device for the Deaf (TDD), are specialized phones that enable people who are deaf, hard of hearing, or speech-impaired to communicate over TDM or IP networks by allowing them to type messages back and forth to one another instead of, or in augmentation of, talking and listening. Cisco Text Relay transports both TTY text characters and voice over the same channel, supporting both Voice Carry Over (VCO) and Hearing Carry Over (HCO).

The Cisco Text Relay for Baudot Text Phones feature supports both Baudot 45.45 and Baudot 50 bps standards-based TTY Phones. These TTY phones are commonly used in countries including the United States, Canada, Ireland, Australia, New Zealand, and South Africa.

Cisco Text Relay is gateway controlled, enabling it to work independently from the call agent. It can be configured on supported gateways for the SIP, H.323 and MGCP signaling protocols. Cisco Text Relay works in a wide range of VoIP environments, including those using Cisco CallManager, Cisco CallManager Express, Cisco SRS Telephony, Cisco SIP Proxy Server, Cisco Multimedia Conference Manager, Cisco BTS 10200 Softswitch, Cisco PGW 2200 Softswitch, and Cisco EGW 2200 Enterprise Gateway.

Figure 114. Cisco Text Relay for Baudot Text Phones



Benefits

- Supports the reliable transport of Baudot TTY calls over VoIP over any codec (G.711, G.729a, etc.)
- Highly resilient to network impairments such as packet loss
- Less than 0.05% Total Character Error Rate (TCER) with 10% packet loss
- Support for both Baudot 45.45 and 50 bps PSTN Text Phones
- Supports Hearing Carry Over (HCO) and Voice Carry Over (VCO)

Hardware

Routers	• Cisco 2600XM, 2691, 2800, 3600, 3700, and 3800 Series with one of the following modules: NM-HD-1V, NM-HD-2V, NM-HD-2VE, NM-HDV2, NM-HDV2-1T1/E1, NM-HDV2-2T1/E1, and EVM-HD-8FXS/DID (with all associated Extension Modules)
Additional Devices	• Cisco 2430 Integrated Access Device • Cisco VG224 Voice Gateway

Additional Information: http://www.cisco.com/go/accessibility

Product Management Contact: Steven White (whites@cisco.com)

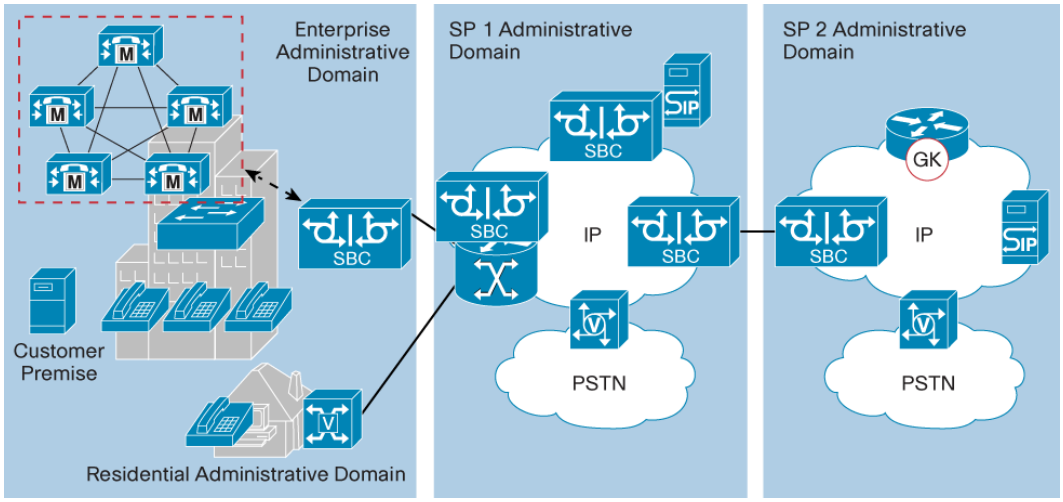
8.3.4) Extended Session Initiation Protocol—Session Initiation Protocol Support on the Cisco Multiservice IP-to-IP Gateway
This feature introduces Extended Session Initiation Protocol (SIP)-SIP functionality support on the Cisco Multiservice IP-to-IP Gateway. Basic SIP-SIP support was introduced in Release 12.4(4)T.

Extended SIP-SIP functionality support on the Cisco Multiservice IP-to-IP Gateway enhances Back-to-Back-User-Agent (B2BUA) functionality in conformance with RFC 3261 to interoperate with SIP User Agents (UAs) and includes the following enhancements to the Cisco Multiservice IP-to-IP Gateway feature suite:

- Delayed Media Call
- Fax passthrough
- Modem passthrough
- TCP to UDP interworking
- TCL scripts with SIP NOTIFY
- VoiceXML support on SIP-SIP calls
- Transport Layer Security (TLS) support
- ENUM support
- Lawful Intercept with SIP
- Interoperability with Cisco CallManager 5.0, Cisco PGW, Cisco SIP Proxy Server, Cisco BTS10200, Cisco DynamicSoft, Broadsoft and Sylantro

The Multiservice IP-to-IP Gateway is used by service provider, enterprise, and small and medium-sized organizations to interconnect SIP and H.323 voice and video networks. The IP-to-IP gateway provides organizations with all their Session Border Control (SBC) needs integrated into the network layer interoperating with many different network elements including voice gateways, IP phones, and call-control servers, in many different application environments, from advanced enterprise voice and/or video services with Cisco CallManager or Cisco CallManager Express, as well as simpler toll bypass and VoIP transit applications. The Cisco Multiservice IP-to-IP Gateway provides a network-to-network interface point for signaling interworking, media interworking, security, billing, and QoS and bandwidth management.

Figure 115. Extended SIP-SIP Support on the Cisco Multiservice IP-to-IP Gateway



Benefits

- SBC functionality integrated into Cisco IOS Software with Lawful Intercept and TDM to IP Gateway support
- B2BUA functionality in conformance with non-proprietary, open standards
- Added SIP functionality to the Cisco Multiservice IP-to-IP Gateway feature suite
- TCL and VXML applications on calls traversing the Cisco Multiservice IP-to-IP Gateway
- Testing and integration with Enterprise and Service Provider voice solutions

Hardware

Routers	• Cisco 2600XM, 2800, 3700, 3800, and 7200 Series • Cisco 2691 and 7301 Routers

Considerations

Cisco Multiservice IP-to-IP Gateway support for the Cisco 2800, 3800, 2800XM, 3700, and 7200VXR Series, and the Cisco 7301 Router requires a Cisco IOS Integrated Voice and Video Services software image.

Additional Information:
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/prod_literature.html

Product Management Contact: Jennifer Blatnik (jennyng@cisco.com)

8.3.5) In-Service Updates to Gatekeeper Zone Prefix Configuration
Enhancements to this Cisco IOS Software release make it possible to add, change, or delete a gatekeeper zone prefix while the gatekeeper is running and managing active E.164 registrations, increasing availability for H.323 VoIP networks. Previous versions of Cisco IOS Software required the user to disable the gatekeeper (shutdown), removing existing calls and registrations before gatekeeper zone prefix changes could be applied.

Benefits

- Reduces scheduled outages requirements for Gatekeeper maintenance
- Enables administrator to make changes without dropping existing calls

Hardware

Routers	• Cisco 2800, 3800, 2600XM, 3700, and 7200 Series • Cisco 7301 Router

Product Management Contact: Kathy Lewis (kalewis@cisco.com)

8.3.6) Packet Mode Services on D Channel

The Packet Mode Services on D Channel feature allows Japanese and European telephone switches to query Cisco routers for the availability of packet mode services on the ISDN D channel.

Benefits

- Complies with the Q.931 SAPI value 0 procedures for call setup
- Enables Cisco routers to interoperate with Japanese and European (NTT and NET3) telephone switches

Hardware

Routers	• Cisco 1801, 1802, 1803, 1811, and 1812 Routers

Product Management Contact: Harbans Kaur (harbkaur@cisco.com)

8.3.7) Skinny Call Control Protocol Private Line Automatic Ringdown with DTMF Out Pulse Digits for FXS Analog Phones

This feature introduces the following enhancements to SCCP controlled Foreign Exchange Station (FXS) analog ports:

- Private Line Automatic Ringdown (PLAR) for Cisco VG224 SCCP controlled FXS analog ports
- Private Line Automatic Ringdown (PLAR) with additional Dual Tone Multi-Frequency (DTMF) Out Pulse Digits for Cisco VG224 SCCP controlled FXS analog ports

SCCP PLAR for the Cisco VG224 allows PLAR as a Skinny Call Control Protocol (SCCP) signaling controlled port. If a caller goes off hook on an analog phone connected to the Cisco VG224, the phone will automatically ring a predefined extension or PSTN number. The Cisco VG224 port “dials” the predefined extension or PSTN number on behalf of the user. The PLAR number is configurable on a per port basis on the gateway. This feature also allows additional digits to be sent after predefined extension or PSTN called number is connected where the wait connect time, wait time after destination is connected, and digit interval, time interval between DTMF digits outpulsing, is configurable. The DTMF Out Pulse Digits allows for easy pre-integration with existing Interactive Voice Response (IVR) systems for users to quickly bypass or transmit predefined calling information. SCCP PLAR works with both Cisco CallManager and Cisco CallManager Express call control systems.

Figure 116. SCCP PLAR on Cisco VG224 with Cisco CallManager Express

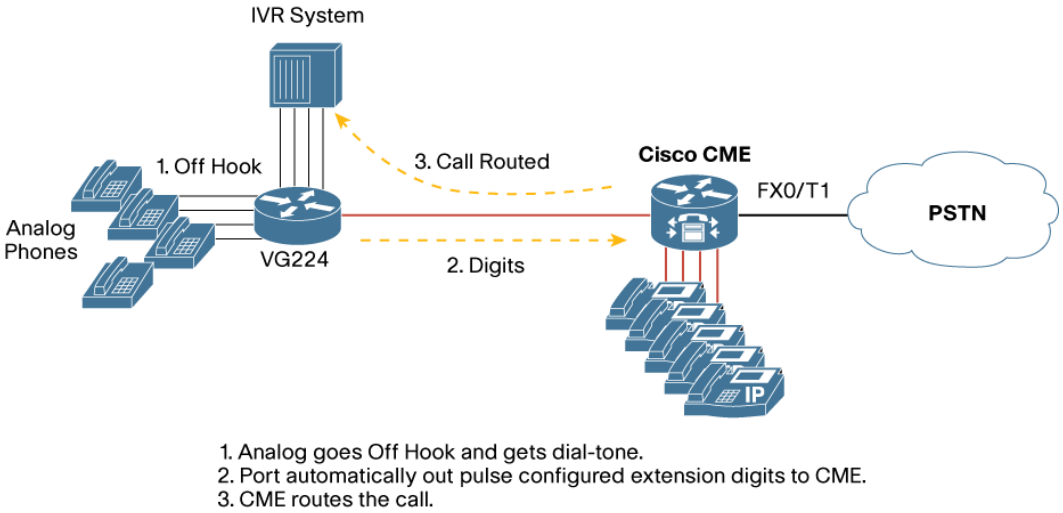
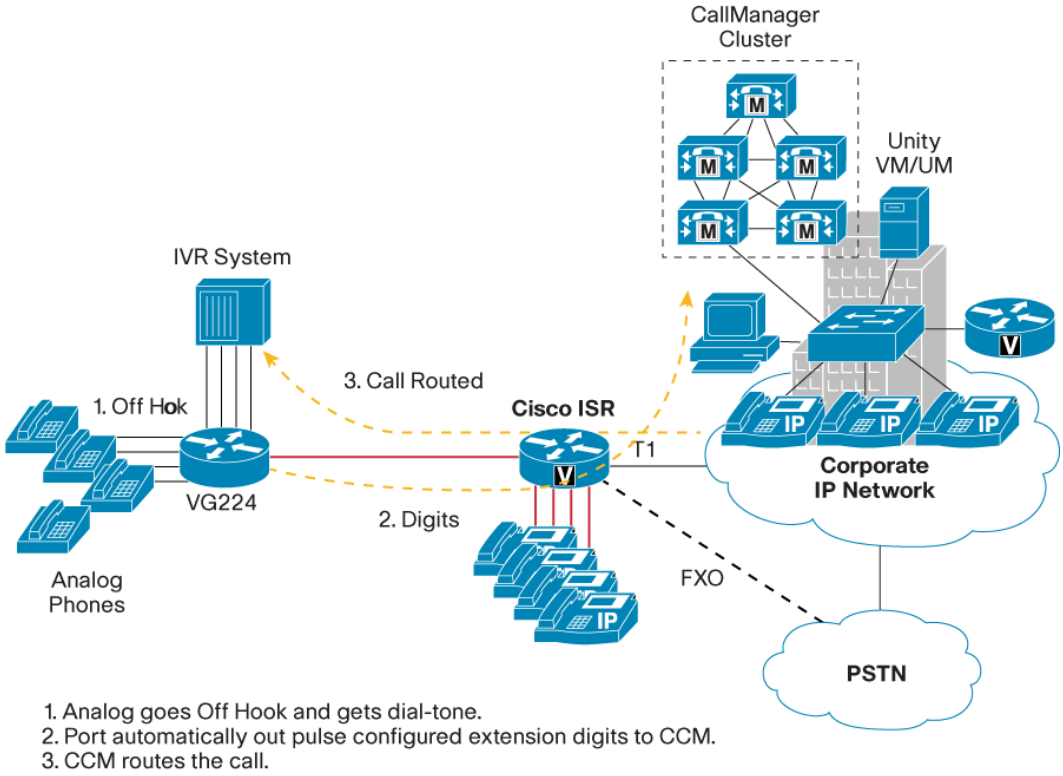


Figure 117. SCCP PLAR on Cisco VG224 with Cisco CallManager



Benefits

Feature	Benefit
Private Line Automatic Ring down for Cisco VG224 SCCP controlled FXS analog ports	Ability for an analog phone upon off hook to dial a predefined extension or PSTN number on behalf of user
Private Line Automatic Ring down with additional DTMF Out Pulse Digits for Cisco VG224 SCCP controlled FXS analog ports	Ability for an analog phone upon off hook to dial a predefined extension or PSTN on behalf of user and upon connection, continue to dial predefined digits

Hardware

Voice Gateway	• Cisco VG224 Voice Gateway

Considerations

The Cisco VG224 requires configuration for this feature to work.

Additional Information:

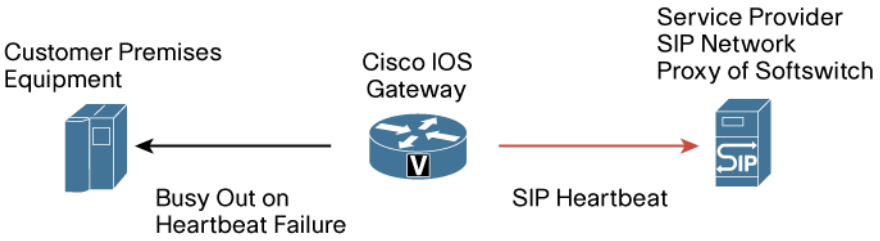
http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080483a76.html

Product Management Contact: Jennifer Blatnik (jennyng@cisco.com)

8.3.8) Session Initiation Protocol Gateway Support for Busyout

Session Initiation Protocol (SIP) Gateway Support for Busyout introduces a mechanism to monitor the SIP status of another user agent. At the SIP signaling level, a generic heartbeat mechanism now allows the gateway to monitor the status of SIP servers and provide the option of busying-out associated voice ports upon total heartbeat failure. When monitored servers' heartbeat responses fail, the configured voice ports present a seized/busied-out condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route. When a voice port is busied out, the gateway will resume the heartbeat mechanism and un-busy the associated voice ports upon receipt of a response. This functionality is different from existing Call Admission Control (CAC) mechanisms (such as AVBO) in that it works on a SIP level and does not require any proprietary capabilities on the remote SIP server (such as IP SLA responders as in Cisco's existing AVBO solution.). This feature will work over Channel Associated Signaling (CAS), Primary Rate Interface (PRI) and Foreign Exchange Station (FXS).

Figure 118. SIP Gateway Support for Busyout



Benefits

- Quick selection of an alternate route in the event of SIP server failures
- Prevents unnecessary call drops
- Customer defined timers for when the network is active as well as when there is a network failure
- Provides for significant customer flexibility in defining their network monitoring
- Does not require any proprietary capabilities on the remote SIP server (such as Service Assurance Agent [SAA] responders as in Cisco's existing AVBO solution).

Hardware

Routers	• Cisco 1800, 2400, 2600XM, 2800, 3800, and 7200 Series • Cisco 1751, 1760, 3660, 3725, and 3745 Routers
Universal Gateways and Access Servers	• Cisco AS5350, AS5400, and AS5850 Universal Gateways

Product Management Contact: Steve Levy (stlevy@cisco.com)

8.3.9) Session Initiation Protocol Transport Layer Security (TLS) Support

This feature implements transport layer security (TLS protocol) on TCP transport for Cisco IOS SIP gateways. The feature is an addition to the core TLS implementation in Cisco IOS and leverages the existing gateway's support of the Public Key Infrastructure (PKI) (for certificate management) and OPSSL-TLS APIs in order to provide the necessary func¬tionality. The use of PKI on Cisco IOS requires that the clock on the SIP gateway be synchronized with the network time to ensure proper validation of certificates.

This feature provides security for device authentication and data encryption of SIP signaling information at the Transport layer of the OSI model. The authentication of the SIP user at the application level would still be done using Digest Authentication.

The feature provides the following security functionality for gateway SIP calls:

- Mutual Authentication—To overcome Identity Theft whereby the intruder gains illegitimate access by posing as a trusted SIP endpoint or the server, a two way device authentication (by both client and the server) by exchange of gateway's certificate signed by the trusted Certificate Authority is performed.
- Signaling Data Encryption—To overcome the Eavesdropping (intruder sniffing) and Man-in-the-Middle attacks (intruder interrupting the dialog or modifying the signaling data), the following is performed:
  - Negotiation of a dynamically generated symmetric key and cipher algorithms through TLS handshake
  - SIP signaling data encryption/decryption using the exchanged symmetric key.

Benefits

- Ensures the security and integrity of SIP signaling to and from the Cisco IOS gateways.
- This includes helping combat:
- Denial of Service Attacks
- Identity Theft
- Eavesdropping

Hardware

Routers	• Cisco 1800, 2400, 2600XM, 2800, 3800, and 7200 Series • Cisco 1751, 1760, 3660, 3725, and 3745 Routers
Universal Gateways and Access Servers	• Cisco AS5350, AS5400, and AS5850 Universal Gateways

Additional Information:

- RFC2246: The TLS protocol version 1.0
- RFC3261: Session Initiation Protocol

Product Management Contact: Steve Levy (stlevy@cisco.com)

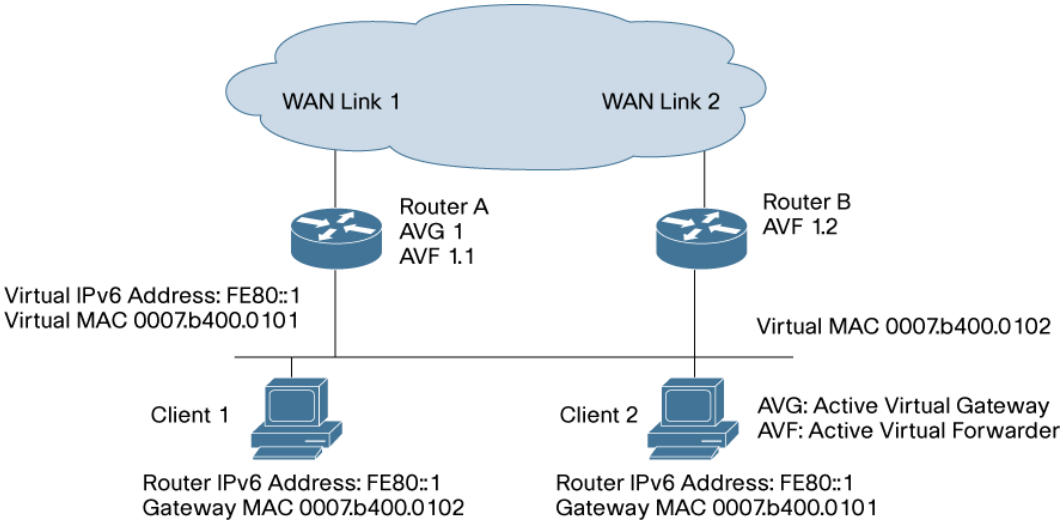
8.4) High Availability

8.4.1) Cisco Gateway Load Balancing Protocol for IPv6

Gateway Load Balancing Protocol (GLBP) for IPv6 protects data traffic from a failed router or circuit, while allowing packet load sharing between groups of redundant routers. GLBP differentiates itself from Virtual Router Redundancy Protocol (VRRP) in that GLBP offers the ability to concurrently use more than one gateway, significantly reducing the cost of a First Hop Routing solution.

Multiple first hop routers on the LAN combine to offer a single virtual first hop IPv6 router while sharing the IPv6 packet forwarding load. GLBP performs a similar, but not identical, function for the user as HSRPv6. HSRPv6 protocol allows multiple routers to participate in a virtual router group configured with a virtual IPv6 address. One member is elected to be the active router to forward packets sent to the virtual IPv6 address for the group. These standby routers have unused bandwidth that the protocol is not using. GLBP provides load balancing over multiple routers (gateways) using a single virtual IPv6 address and multiple virtual MAC addresses. Each host receives the same virtual IPv6 address using standard IPv6 ND (Neighbor Discovery) procedures, and all routers in the virtual router group participate in forwarding packets.

Figure 119. Cisco GLBP for IPv6



Benefits

- Increases network availability by providing protection against router failures.
- Provides network redundancy and load sharing for IPv6 networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3200, 3700, 3800, and 7200 Series • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760, 2691, 3660, and 7301 Routers
Universal Gateways and Access Servers	• Cisco AS5000 Series

Considerations

There is no “default gateway” concept in IPv6. The router’s address is learned through Router Advertisement [RA]. On a LAN where a number of routers form a GLBP group, should a router not be configured for GLBP, there would be a risk to see two different RAs reaching the hosts. An RA

would be generated by the GLBP virtual gateway and another by the router out of the GLBP group. Hosts would then load balance the packets between the mis-configured router and the GLBP virtual gateway. To prevent this, Cisco recommends setting up the Default Router Selection feature, which was introduced in Cisco IOS Software Release 12.4(2)T. Setting-up RA priority to “high” on GLBP routers would allow the GLBP routers to be preferred.

Additional Information:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html

Product Management Contact:

- Benoit Lourdelet (blourdel@cisco.com)
- Patrick Grossetete (pgrosset@cisco.com)

6.4.2) Hot Standby Router Protocol—Multiple Group Optimization
There is a direct relationship to the increase in sub-interfaces per physical interface and the corresponding HSRP Group configuration required. The negotiation and maintenance of multiple HSRP groups can have a detrimental impact on network traffic and CPU utilization.

This feature optimizes the number of HSRP messages sent out of a physical interface when multiple HSRP groups are configured on sub-interfaces.

Only one HSRP group is required on a physical interface for the purpose of electing Active and Standby routers. This group is known as the ‘master’ group. The HSRP group state of the client groups follows that of the master group, (i.e. the client groups do not participate in any sort of router election mechanism.)

Benefits

- Increased scalability for HSRP groups on a physical interface
- Reduces operational overhead through simplified configuration

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3200, 3700, 3800, and 7200 Series • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760, 2691, 3660, and, 7301 Routers
Universal Gateways and Access Servers	• Cisco AS5000 Series

Additional Information:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.5) Management Instrumentation

6.5.1) Cisco IOS IP Service Level Agreements—Label Switched Path Health Monitor
Cisco IOS IP Service Level Agreements (SLAs)

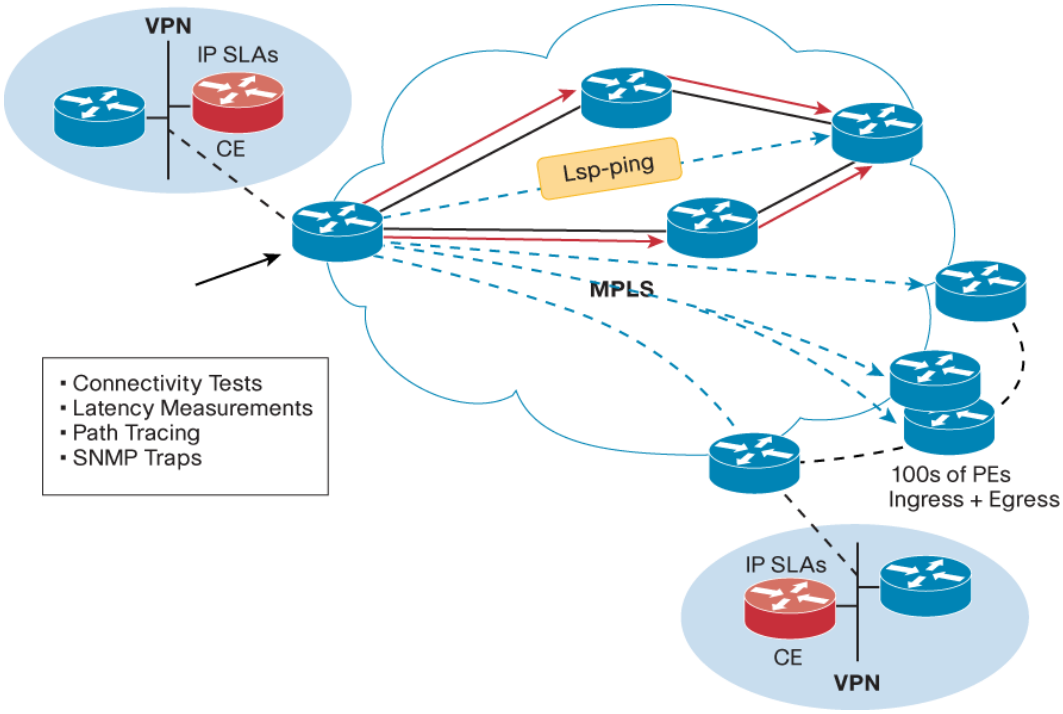
Customers demand guaranteed, reliable network services for business-critical applications and services. Cisco IOS IP SLAs is a capability embedded in Cisco IOS Software, which allows Cisco customers to increase productivity, lower operational costs, and reduce the frequency of network

outages. IP and SLAs are converging and extending IP performance monitoring to be application aware makes this functionality critical for new IP network applications such as Voice over IP (VoIP), Audio and Video, MPLS VPNs and other critical applications. Cisco IOS IP SLAs measures end-to-end and can perform network assessments, verify Quality of Service (QoS) and ease deployment of new services, and assist administrators with network troubleshooting. Cisco IOS IP SLAs uses unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

Cisco IOS IP SLAs—Label Switched Path Health Monitor

The Cisco IOS IP SLAs Label Switched Path (LSP) Health Monitor feature provides the capability to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) VPNs. The feature is useful for determining network availability or testing network connectivity between Provider Edge (PE) routers in an MPLS VPN. This feature will automatically monitor LSPs and notify network operations in the event of forwarding or connectivity issue and reduce problem resolution time. Once configured, the LSP Health Monitor will create and delete IP SLAs LSP ping or LSP traceroute operations based on network topology. LSP ping's diagnostic capability, combined with SNMP traps, can be used to indicate any path issues for network operators.

Figure 120. Cisco IOS IP SLAs—LSP Health Monitor



Benefits

- Layer 3 MPLS VPN edge to edge connectivity testing to reduce MPLS network operational expense and improve problem resolution times by:
- SLAs monitoring
  - Network performance monitoring
  - IP Service network health readiness or assessment tests
  - Edge-to-edge network availability monitoring

- Business-critical applications performance monitoring
- Reducing Mean Time To Repair (MTTR) while troubleshooting network outages

Hardware

Routers	• Cisco 3600, 3700, 3800, and 7000 Series

Additional Information:

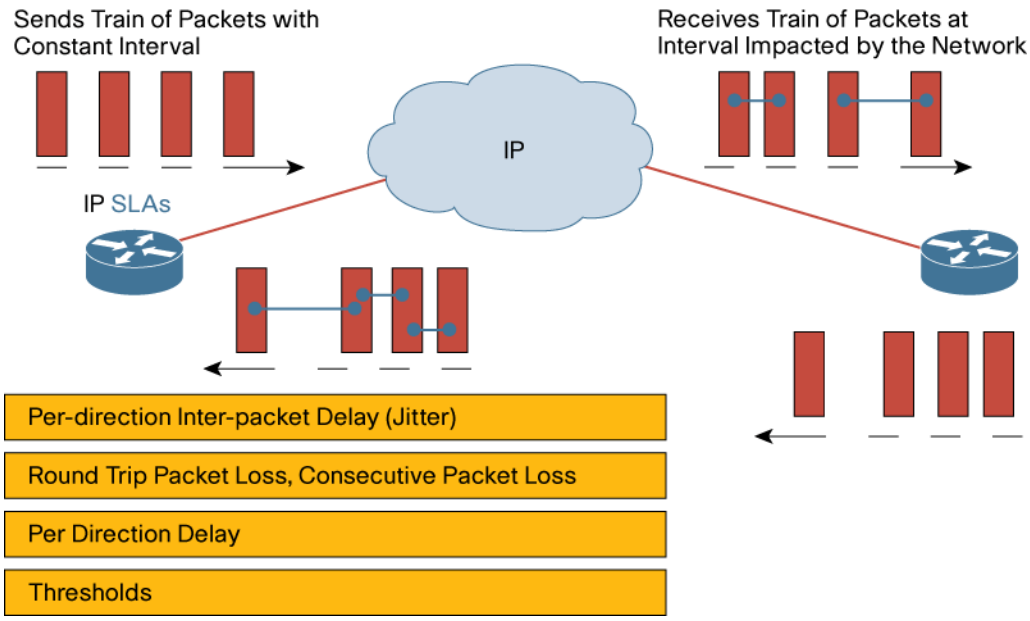
- http://www.cisco.com/go/ipsla
- http://www.cisco.com/en/US/products/ps6566/products_feature_guide09186a0080528450.html

Product Management Contact: Tom Zingale (tomz@cisco.com)

6.5.2) Cisco IOS IP Service Level Agreements—ICMP Jitter Operation

Cisco IOS IP SLAs uses unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements. This feature allows IP SLAs to send a series of ICMP packets to any endpoint and measure jitter, packet loss, latency and consecutive packet loss. The feature is extremely useful for performance monitoring, troubleshooting, and connectivity tests verifying end to end network operation. The ICMP jitter operation is similar to the IP SLAs UDP jitter operation but does not require a Cisco endpoint.

Figure 121. Cisco IOS IP SLAs—ICMP Jitter Operation



Benefits

- Measures performance characteristics to any endpoint (Cisco or non-Cisco)
- Extends the functionality provided by IP SLAs
- SLAs monitoring
  - Network performance monitoring
  - IP Service network health readiness or assessment

Hardware

Routers	• Cisco 3600, 3700, 3800, and 7000 Series

Considerations

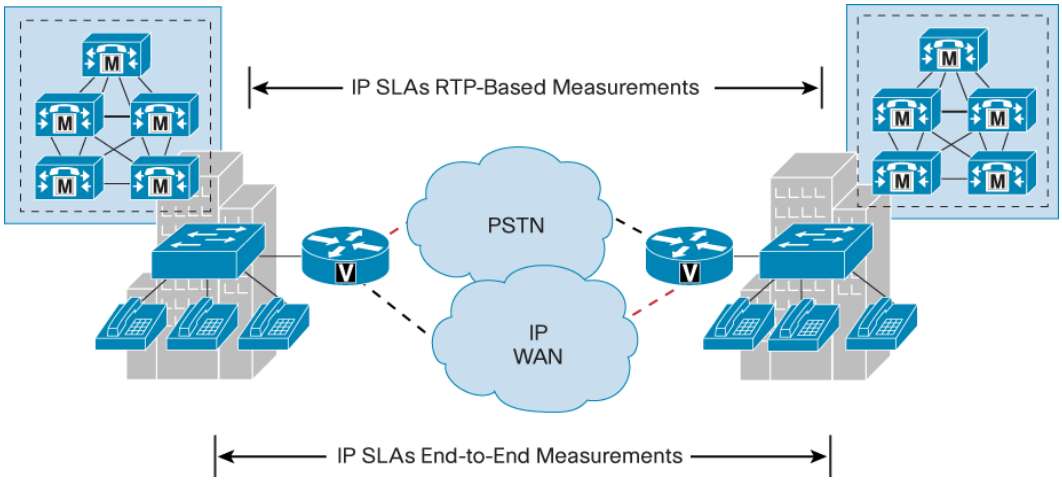
- Not available in the IP Base Cisco IOS package

Additional Information: http://www.cisco.com/go/ipsla

Product Management Contact: Tom Zingale (tomz@cisco.com)

6.5.3) Cisco IOS IP Service Level Agreements: Real Time Protocol-based Voice over IP Operation
This feature enhances Cisco IOS IP Service Level Agreements (SLAs) by including a capability to create a Voice over IP (VoIP) active test call using Real Time Protocol (RTP). This feature requires Digital Signal Processor (DSP) hardware within the device receiving the IP SLAs RTP stream. An RTP stream is generated and the voice gateway hardware (DSP) then processes the call and measures voice over IP statistics including: voice quality, jitter, frame loss, latency, acoustical round trip time and others. The voice quality scores produced include Mean Opinion Score-Conversional Quality (MOS-CQ), Mean Opinion Score—Listening Quality (MOS-LQ) and R-Factor.

Figure 122. Cisco IOS IP SLAs: RTP-based VoIP Operation



Benefits

- Measures performance characteristics for VoIP calls using RTP
- Calculates voice quality scores using voice gateway DSP hardware
- Extends the functionality provided by IP SLAs
- Adds to the already strong VoIP monitoring capabilities
- Performance Visibility for VoIP, Video, business-critical applications, MPLS, and VPN networks

Hardware

Routers	• Cisco 3600, 3700, 3800, and 7000 Series

Considerations

- Not available in the IP Base Cisco IOS package
- Requires DSP based Voice Module

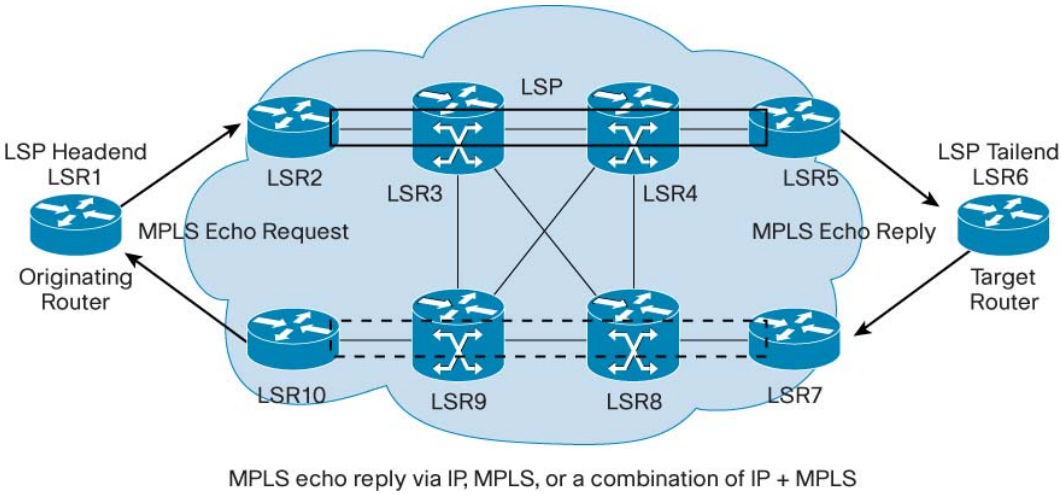
Additional Information: http://www.cisco.com/go/ipsla

Product Management Contact: Tom Zingale, tomz@cisco.com

6.5.4) Multiprotocol Label Switching Label Switched Path Ping and Label Switched Path Traceroute Internet Control Message Protocol (ICMP) ping and traceroute are often used to help diagnose the root cause when a forwarding failure occurs. However, they are not well suited for identifying LSP failures because an ICMP packet can be forwarded via IP to the destination when an LSP breakage occurs.

The Multiprotocol Label Switching (MPLS) Embedded Management-LSP Ping for Label Distribution Protocol (LDP) Forwarding Equivalence Classes (FECs) feature is a new capability that is better suited for identifying LSP breakages. This solution is based on the IETF specification for Detecting MPLS Data Plane Failures based on draft-ietf-mpls-lsp-ping-11.txt.

Figure 123. MPLS Embedded Management—MPLS LSP Ping and LSP Traceroute



Benefits

- MPLS LSP Ping and Traceroute helps with fault detection and isolation. **Benefits** include:
- Detecting MPLS traffic black holes or misrouting
- MPLS forwarding plane fault isolation
- Verify the forwarding plane (LSPs) against the control plane (IGP/LDP)
- MTU detection of the MPLS LSPs

Hardware

Routers	• Cisco 850, 870, 1800, 2800, and 3800 Series • Cisco 7200 Series

Additional Information:
http://www.cisco.com/en/US/products/ps6605/products_ios_protocol_group_home.html

Product Management Contact: Ripin Checker (rchecker@cisco.com)

6.6) IP Routing

6.6.1) Enhanced Interior Gateway Routing Protocol for IPv6

Enhanced Interior Gateway Routing Protocol (EIGRP) is a unique Cisco innovation valued for its ease of deployment, fast convergence times, minimal routing traffic overhead, and scalability. EIGRP for IPv6 allows fast, seamless IPv6 integration for IPv4 EIGRP users in the Enterprise, public sector (defense, government), and wireless applications by extending EIGRP to support next generation IPv6 infrastructure and services.

Network administrators looking at their IPv4 networks currently face a variety of challenges:

- **IPv4 Address Space Depletion:** Due to the 32 bit limit of IPv4, the availability of Class A, B & C Internet addresses, and the ever growing size of networks, the IPv4 address space available for use is rapidly being consumed and limited in its ability to scale to the requirements of next generation infrastructure requirements.
- **Mobile Wireless:** With the ongoing convergence of video/voice & data on Mobile Wireless devices, there is a rapidly growing demand for IP address space from these mobile devices that exceeds the capabilities of current IPv4 networks.
- **Mobile Networks:** New applications such as mobile networks using mobile platforms such as automobiles, ships, trains, and planes adds to the pressure on IPv4 address space.
- **Public Sector:** Many parts of the US Government have created memos (DoD memo June 2003, OMB Memo M-05-22), task forces (Commerce Department task force on IPv6), and recommendations (GAO-05-471) to transition from IPv4 to IPv6 based networking solutions by 2008.
- **Higher Education/Research Networks:** These networks are pushing the limits of networking technology and applications. As such, they require networking equipment and protocols that can extend beyond the boundaries of existing IPv4 based solutions.

All of these factors are pushing IPv6 as a next generation infrastructure technology capable of overcoming the limitations of IPv4 and allowing for the delivery of next generation services such as mobile wireless.

In order to make the transition from IPv4 to IPv6, there are two important issues that need to be considered:

- **Supportability of IPv4 and IPv6:** The migration to IPv6 will be a gradual one and administrators will require the flexibility to keep both their IPv4 users and IPv6 users on the same network infrastructure at the same time. Hence, the network needs to be able to support both IPv4 and IPv6.
- **EIGRP for IPv4:** EIGRP is an area of continual innovation by Cisco with support for such functionality as:
  - Nonstop Forwarding (NSF) with Stateful Switchover (SSO)
  - Stub Routing; MPLS VPN PE-CE with Site of Origin (SoO)
  - Route Redistribution Limiting and Max-Prefix Limits
  - SNMP MIBs
  - Enhanced Route Map support

The strong protocol support and ongoing innovation for EIGRP leads to the following major customer benefits:

- **Ease of Use:** EIGRP is simple to learn, configure, and deploy compared to other major Interior Gateway Protocols (IGPs). This a major source of time saving for EIGRP customers.
- **Scalability:** EIGRP contains functionality that allows it be suitable and scalable for deployment in multiple scenarios including hub and spoke, broadcast domains, and meshed architectures.
- **Sub-Second Convergence:** Backup routes are pre-computed and instantaneously used in case of failure.
- **High Availability:** Provides comprehensive support for High Availability improves the reliability of network and minimizes downtime.
- **Investment Protection:** Since EIGRP is widely available across Cisco platforms suitable for both Enterprises and Service Providers, it provides a significant degree of capital investment protection for customers needing different routers to meet their networking needs.

As a result of these benefits, over 52% of Cisco Enterprise networks in a wide range of industries, such as Financial Services, Energy and Utilities, Manufacturing, Health Care, Public Sector/ Government/ Defense, Retail, Transportation, and Hospitality, use EIGRP as their interior routing protocol in their IPv4 implementations. For these customers, migration to IPv6 requires a clear path and strategy to preserve the benefits from their existing EIGRP for IPv4.

To solve the issue of integrating IPv6 into EIGRP based IPv4 networks, Cisco is offering support for EIGRP for IPv6. This functionality will allow an EIGRP IPv4 customer, as shown in Figure 111, to integrate EIGRP for IPv6 support into their network infrastructure, as shown in Figure 112. The old IPv4 network was only capable of handling IPv4 users with IPv4 address prefixes. The new network can handle both IPv4 users as well as IPv6 users with IPv6 prefixes. This is possible since the single EIGRP IPv4 routing table in the old network has been supplemented with an EIGRP IPv6 routing table in the new network. In this manner, the IPv4 and IPv6 networks operate in a dual stack or ‘ships in the night’ mode. The new network offers users a seamless integration of their IPv4 and IPv6 networks while allowing them to retain all the benefits of using EIGRP.

Figure 124. Routing Domain Based Upon EIGRP for IPv4

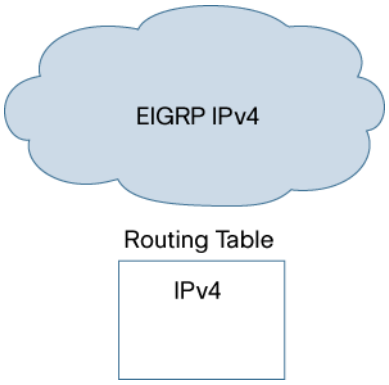
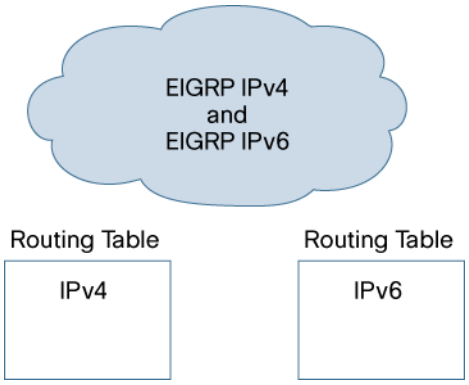


Figure 125. Routing Domain Integrating EIGRP Based IPv4 and IPv6



Benefits

- Extends key EIGRP benefits, including ease of use, fast convergence times, minimal routing traffic overhead, and scalability, to IPv6 environments.
- Fast, seamless IPv6 Integration: Allows existing EIGRP IPv4 customers to integrate IPv6 based upon EIGRP into their network. This is important for applications in enterprises, public sector (government/defense), and wireless networks.
- Delivery of IPv6 Services: Enables the creation of next-generation IPv6 infrastructure to deliver services such as Mobile Wireless or Mobile Networks.

Hardware

Routers	• • Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router •

Product Manager: Chetan Khetani (cpk@cisco.com)

6.6.2) Routing Information Protocol Version 2: RFC 1724 MIB Extension

This functionality provides the MIBs for Routing Information Protocol (RIP) version 2 as defined in RFC 1724 - RIP Version 2 MIB Extension. This is a read-only MIB.

Benefits

- Effective monitoring of the RIP routing protocol through the table objects
- Object support includes Global Counters, Interface Status Table and the Interface Configuration Table

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Considerations

- The optional peer table defined in RFC 1724, Section 5.3 is not supported.

Product Management Contact: Chetan Khetani (cpk@cisco.com)

6.6.3) Open Shortest Path First Version 2 RFC 3623 Graceful Restart—Helper Mode

Open Shortest Path First (OSPF) Nonstop Forwarding (NSF) Awareness or helper mode as per RFC 3623 Graceful OSPF Restart, allows routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. The local router may not be performing NSF; its awareness of NSF allows the integrity and accuracy of the routing table and the link state database on the neighboring NSF-capable router to be maintained during the switchover process.

Benefits

- OSPF RFC 3623 Nonstop Forwarding (NSF) Awareness feature allows routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets.
- This function does not require the local router to be NSF-capable
- The NSF-awareness feature is enabled by default, not requiring additional configuration

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Product Management Contact: Chetan Khetani (cpk@cisco.com)

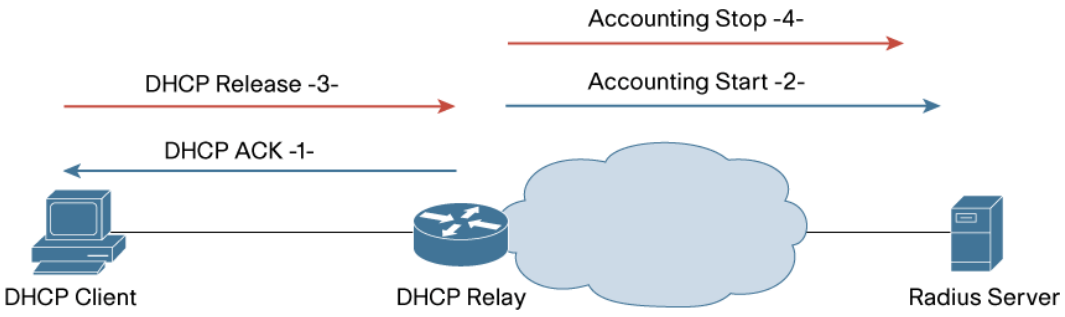
6.7) IP Services

6.7.1) Dynamic Host Configuration Protocol Option 82—Per Interface Support

Automatic DHCP address allocation is typically based on an IP address, whether it is the gateway IP address or the incoming interface IP address. Mainly, in ISP networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the Relay Agent Information Option, the Cisco IOS Relay Agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. It is also possible to manipulate or check the content of an already present Option 82 content.

Addressing the ISP needs, the above mentioned capability can now be configured at an interface level, dramatically increasing the versatility of the solution. Typically it enables the aggregation of several DHCP services with different Option 82 management policies on the same router.

Figure 126. DHCP Option 82—Per Interface Support



Benefits

- Allows for better router resource utilization by aggregating several service types on the same router.

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3200, 3700, 3800, and 7200, Series • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, 2691, 3660, and 7301 Routers
Universal Gateways and Access Servers	• Cisco AS5000 Series

Additional Information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/hipdhcpr.htm - wp1078842

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

6.8) VPN

6.8.1) ANI Suppression During L2TP Set-Up for the Cisco AS5000 Series
This feature enables suppression of all or part of the calling number field in the L2TP setup process for the Cisco AS5400 Series Universal Voice Gateways. This functionality is supported by using a Radius profile. There are no new CLI being added as part of this feature.

This is important functionality for Service Providers since certain countries mandate that wholesale dial providers do not disclose the calling party number information to the ISP they serve.

Benefits

Service providers can disclose or withhold the calling party number information for their customers.

Hardware

Cisco Universal Voice Gateways	• Cisco AS5400XM, AS5400HPX, AS5400, and AS5350

Product Management Contact: Dax Choksi (dchoksi@cisco.com)

6.9) Connectivity

6.9.1) Asynchronous Transfer Mode Oversubscription for DSL
Asynchronous Transfer Model (ATM) oversubscription enables multiple VBR-rt, VBR-nrt, and UBR+ PVCs to be configured with a sum of their individual sustainable cell rates (SCRs) exceeding the physical lines bandwidth.

Resource limitations on Cisco xDSL interfaces may require limiting the maximum amount of oversubscription allowable. This can be accomplished by utilizing the atm oversubscribe factor command.

Benefits

- Enables the configuration of multiple PVCs for a higher total sustained cell rate (SCR)
- Enables PVCs with higher SCRs to take advantage of available bandwidth
- Uses a simple command syntax atm oversubscribe

Hardware

Routers	• Cisco 2600XM Series • Cisco 1841, 2691, 2801, 2811, 2821, 2851, 3725, 3745, 3825, and 3845 Routers

Additional Information:

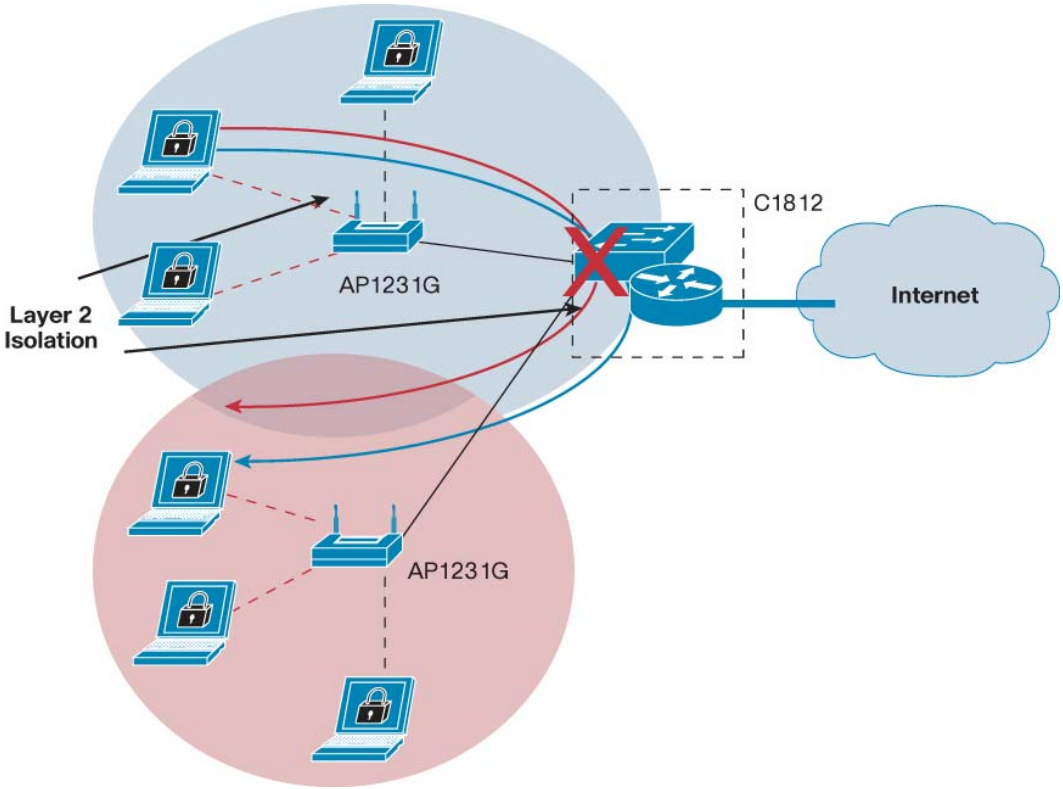
http://www.cisco.com/en/US/products/ps6706/prod_release_note09186a0080527f26.html - wp249006

Product Management Contact: Subbu Mahadevan (smahadev@cisco.com)

6.9.2) Private VLAN Edge on Cisco 1800 Fixed Configuration Routers

The Private VLAN Edge feature allows one to block switched traffic between two ports on the same VLAN. Traffic must be routed to pass from one port to another. This enables support for multiple VLANs with Layer 2 isolation to exist within a single subnet. A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port in the same device. Traffic can not be forwarded between protected ports at Layer 2, all traffic passing between protected ports must be forwarded through a Layer 3 device.

Figure 127. Private VLAN Edge on Cisco 1800 Fixed Configuration Routers



Benefits

- Provides isolation of traffic across switch ports in a device
- Limits the size of broadcast domains

Hardware

Routers	• Cisco 1801, 1802, 1803, 1811, and 1812 Routers

Additional Information:

http://www.cisco.com/en/US/tech/tk389/tk814/tk841/tsd_technology_support_sub-protocol_home.html

Product Management Contact: Harbans Kaur (harbkaur@cisco.com)

9) Release 12.4(4)T Highlights

Table 27. Release 12.4(4)T Feature Highlights

9.1) Hardware	9.2) Cisco IOS Security	9.3) Voice	9.4) High Availability
9.1.1) Cisco 1801, 1802, and 1803 Integrated Services Routers 9.1.2) Multi-Processor Forwarding for Broadband LAC, LNS, and PTA 9.1.3) ADSL2/ADSL2+ Support for Integrated Service Routers (ISRs)	9.2.1) Flexible Packet Matching 9.2.2) Application Firewall for Instant Message Traffic Enforcement 9.2.3) VRF-Aware Domain Name System 9.2.4) Easy VPN Phase 6 9.2.5) Control Plane Protection 9.2.6) VRF-Aware IPsec MIB 9.2.7) IPv6 Support for Site-Site IPsec VPN 9.2.8) Dynamic Multipoint VPN Quality of Service Support	9.3.1) Cisco IOS IP Service Level Agreements for VoIP with Real Time Protocol 9.3.2) Secure Communication between IP-STE and PSTN STE Endpoints 9.3.3) Interoperability Enhancements to the Cisco Multiservice IP-IP Gateway 9.3.4) Identify Alternate Endpoint Call Attempts in RADIUS Call Accounting Records 9.3.5) Cisco Modem Relay 9.3.6) Session Initiation Protocol: CLI for Passing Calling Name when Privacy Exists 9.3.7) Fax Relay Support for SG3 Fax Machines at G3 Speeds 9.3.8) SIP-SIP Basic Support on the Cisco Multiservice IP-to-IP Gateway 9.3.9) Cisco CallManager Express 3.4 9.3.10) Survivable Remote Site Telephony Version 3.4 Support with Release 12.4(4)T	9.4.1) Cisco Hot Standby Router Protocol for IPv6 9.4.2) NetFlow Reliable Export via Stream Control Transport Protocol

9.5) Management Instrumentation	9.6) Quality of Service	9.7) Broadband	9.8) IP Routing
9.5.1) NetFlow Top Talkers CLI	9.6.1) Skype Classification via NBAR Packet Description Language Modules 9.6.2) Direct Connect Packet Description Language Modules Native Implementation	9.7.1) Multicast User Authentication and Profile Support 9.7.2) Point-to-Point Protocol over Ethernet Circuit ID Tag Processing	9.8.1) Bidirectional Forwarding Detection Support 9.8.2) Border Gateway Protocol Route-Map Continue Support for Outbound Policy 9.8.3) Border Gateway Protocol Selective Next-Hop Route Filtering

9.1) Hardware

9.1.1) Cisco 1801, 1802, and 1803 Integrated Services Routers

Cisco 1800 Fixed-Configuration Integrated Services Routers are the next evolution of the award-winning Cisco 1700 Series access routers. The Cisco 1800 Series fixed-configuration routers are designed for secured broadband access, Metro Ethernet, and wireless connectivity. They also help businesses reduce costs by enabling deployment of a single device to provide multiple services typically performed by separate devices.

The Cisco 1801, 1802, and 1803 Integrated Services Routers provide:

- Secure broadband access with concurrent services for branch and small offices
- ADSL2/ADSL2+ (G.992.4/G.992.5) support on Cisco 1801/1802 using Cisco IOS Software Release 12.4(4)T and later releases.

- Integrated ISDN Basic Rate Interface (BRI), or Ethernet backup port for redundant WAN links
- LAN Switching with optional inline POE
- Secure wireless LAN for simultaneous 802.11a and 802.11b/g operation with use of multiple antennas
- Advanced security including:
  - Stateful Inspection Firewall
  - IPsec VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES])
  - Dynamic Multipoint VPN (DMVPN) and Easy VPN
  - Intrusion Prevention System (IPS)
  - Antivirus support through Network Admission Control (NAC) and enforcement of secure access policies

Cisco 1801, 1802, and 1803 routers provide high-speed DSL broadband access through asymmetric DSL (ADSL) over basic telephone service (Cisco 1801), ADSL over ISDN (Cisco 1802), or Symmetrical High-Data-Rate DSL (G.SHDSL) (Cisco 1803) while helping to ensure reliable networking with integrated ISDN S/T BRI backup. The Cisco 1801, 1802, and 1803 routers combine the cost **Benefits** of DSL service with the advanced routing capability required for business use of the Internet.

Figure 128. Cisco 1801, 1802, and 1803 Integrated Services Routers

Benefits

- High-speed processor delivers exceptional processing power for applications and concurrent security and wireless services.
- Offers flexibility to connect to various types of DSL broadband including ADSL2/ADSL2+ for the Cisco 1801/1802 (Ethernet access is via 1811/1812. 1801,2,3 offer Ethernet on LAN side and xDSL on the wan connectivity side). Additional capability includes the ability to deploy redundant WAN connections for failover protections and load balancing.
- Detects harmful network activity and generates alarms to warn of threats and intrusion attempts. New IPS signatures can be dynamically loaded.
- Provides simultaneous operation at multiple Wi-Fi frequencies including 2.4 GHz and 5 GHz. Enterprise advanced management and configuration capabilities are offered through a Web-based GUI.

Hardware

Routers	• Cisco 1801, 1802 and 1803 Series Routers

Additional Information:

http://www.cisco.com/en/US/products/ps5853/products_data_sheet0900aecd8028a95f.html

Product Management Contact: Bala Nagesh (bnagesh@cisco.com)

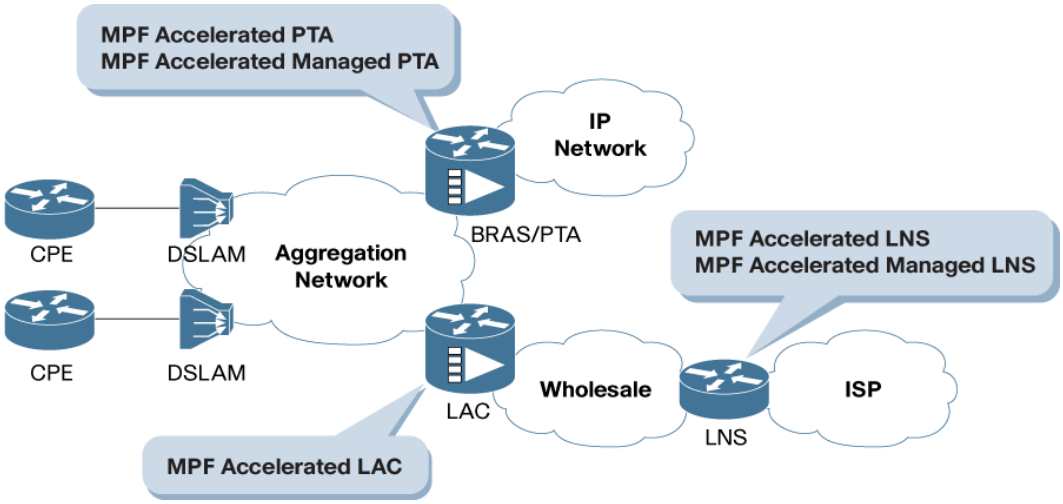
9.1.2) Multi-Processor Forwarding for Broadband LAC, LNS, and PTA

Multi-Processor Forwarding (MPF) for Broadband L2TP Access Concentrator (LAC), L2TP Network Server (LNS), and PPP Termination and Aggregation (PTA) significantly improves broadband feature performance by accelerating features with a fast-forwarding method of switching packets on the second CPU of the Cisco 7301 and Cisco 7200 VXR Routers. MPF for Broadband LAC, LNS, and PTA significantly improves performance by at least two times that of typical Cisco 7301 or Cisco 7200 VXR Routers without any hardware changes.

MPF for Broadband LAC, LNS, and PTA is accomplished using a second CPU running fast-forwarding software to switch packets. Standard Cisco IOS Software features use a single CPU for both control plane and data functionality. MPF has moved the data plane traffic to the second CPU, on which LAC features, LNS and PTA applications are processed at an accelerated rate, thus improving the performance of these broadband features. The MPF microcode running in the second CPU forwards traffic at approximately twice the forwarding performance of standard Cisco IOS Software. MPF can run all basic LAC, LNS, and PTA functionality with minimal impact to configuration and to Cisco IOS Software Release 12.4T functionality. Standard Cisco IOS Software processes certain non-MPF features, which are not accelerated.

The **Benefits** of improved network performance are important due to the rapid increase in broadband users. Existing customers who deploy an LNS network can gain performance without adding additional hardware into their network. Service providers can offer services to more subscribers while maintaining their current network topology.

Figure 129. MPF for Broadband LAC, LNS, and PTA



Benefits

- Hardware acceleration of Broadband traffic
- Improved network performance and user scalability for Broadband LAC, LNS, and PTA applications
- No forklift upgrades for improved network performance

Hardware

Routers	• Cisco 7206VXR and 7301 Series Routers

Considerations

The NPE-G1 engine is required for the Cisco 7200 VXR Router. LAC, LNS, and PTA functionality for both the Cisco 7301 and Cisco 7200 VXR Routers is supported only on native Gigabit Ethernet (GE) ports.

No port adapter traffic is accelerated by the second CPU. Any traffic from these port adapters will be forwarded using just the first CPU. Cisco recommends that users migrate any existing port adapter traffic to the native GE ports in order to fully leverage the MPF accelerated features.

Product Management Contact: Dilshad Mohamed (dmohamed@cisco.com)

9.1.3) ADSL2/ADSL2+ Support for Integrated Service Routers (ISRs)
ADSL2/ADSL2+ functionality, based upon the ITU G.992.4/G.992.5 standards, is provided on the Integrated Service Router (ISR) product line via software support and a Hardware Interface Card (HWIC). ADSL2/ADSL2+ are next generation ADSL technologies capable of providing increased bandwidth (up to 24 Mbps downstream and 1Mbps upstream) for Data/Voice/Video applications in Service Provider Triple Play service offerings. The Cisco 857/876/877 and Cisco 1801/1802 Fixed Configuration ISRs will support the ADSL2/ADSL2+ standard via the Cisco IOS 12.4(4)T release. The Cisco 1841, 2800, and 3800 ISRs will offer this same support through a single-port, single-wide HWIC for use in these modular platforms. The HWICs will support ADSL over POTS (Annex A) and ADSL over ISDN (Annex B) standards via two different cards: the HWIC-1ADSL for 1-port ADSLoPOTS HWIC; and, the HWIC-1ADSLi for 1-port ADSLoISDN HWIC.

Figure 130. 1-Port HWIC for Cisco 1841/2800/3800 ISRs

Benefits

- ADSL2/ADSL2+ standard support for ISRs
- Higher data throughput (up to 24 Mbps downstream and 1 Mbps upstream) for Data/Voice/Video Triple Play service offerings
- Multiple form factors to fit the needs of Service Providers and Small Medium Branch Office applications

Hardware

Routers	• Cisco 857/876/877, Cisco 1801/1802/1841 and Cisco 2800/3800 Series Routers

Product Management Contact:

- Subbu Mahadevan (smahadev@cisco.com)
- Bala Nagesh (bnagesh@cisco.com)
- Sanjay Kumar (sanjayku@cisco.com)

9.2) Cisco IOS Security

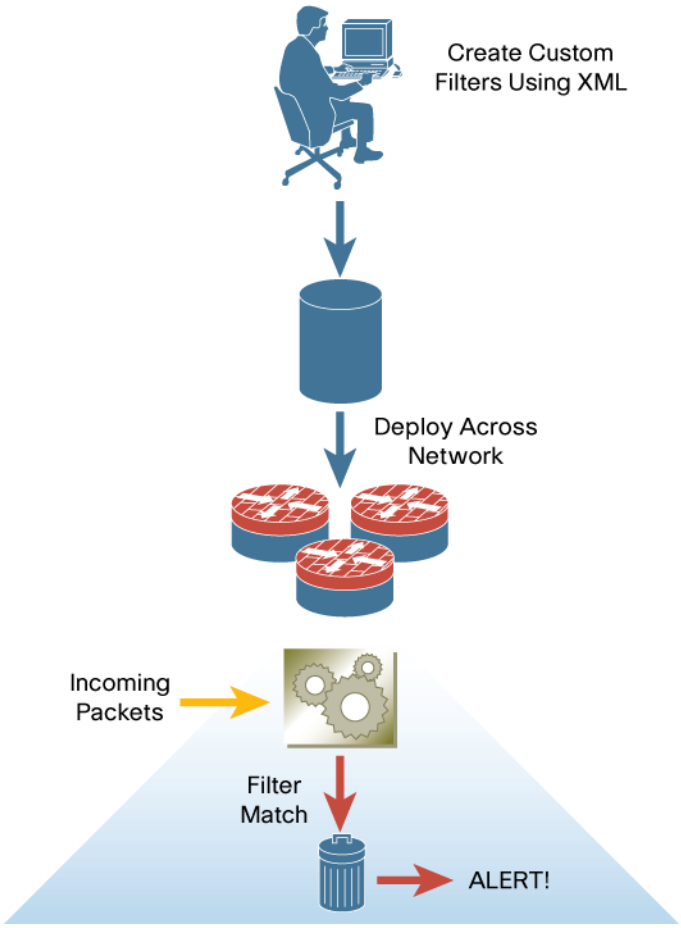
9.2.1) Flexible Packet Matching

Flexible Packet Matching (FPM) is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM further extends the network traffic class definition capability to include new CLI syntax to offset into a user-defined protocol header and, furthermore, into the data portion of the packet.

FPM is the next-generation Access Control List (ACL) technology that provides rapid first line of defense against malicious traffic at the entry point into the network. It features powerful custom pattern matching deep within packet header or payload, minimizing inadvertent blocking of legitimate business traffic.

FPM provides network security administrators with powerful tools to identify miscreant traffic as it enters the network, and to immediately drop and/or keep a log for audit purposes. Administrators can specify custom match patterns at multiple offsets within the packet. FPM includes ready-made definitions for standard protocols via Protocol Header Definition Files (PHDF), which simplify deployment. Customers can also customize and add extensions to PHDFs at device run time.

Figure 131. Cisco IOS FPM



Benefits

FPM enables users to create their own stateless packet classification criteria and to define policies with multiple actions (ie: drop, log or send ICMP unreachable) to immediately block new viruses, worms, and attacks. Essentially, FPM provides the means to inspect packets for characteristics regardless of the header fields involved. It provides a flexible Layer 2 through Layer 7 stateless classification mechanism.

Hardware

Routers	• Cisco 871 Series, 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 3700, 3800, 7200 and 7301 Series Routers

Considerations

This feature will only be available in Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

Additional Information: http://www.cisco.com/go/fpm/

Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.2) Application Firewall for Instant Message Traffic Enforcement

Application Firewall for Instant Messenger Traffic Enforcement reduces exposure to potential vulnerabilities from instant messenger clients. It offers flexible policy enforcement by allowing administrators to restrict user access to specific instant messenger services, such as text chat, voice or video chat, and file transfer, and ensures judicious use of network resources.

For example, Instant Messenger Traffic Enforcement can easily implement a policy that allows that text-chat capability in instant messenger, but denies access to additional services such as voice or video chat and file transfer. Additionally, audit-trail capability allows customers to monitor the volume of instant messenger traffic for specific users.

Benefits

- Can limit instant messenger usage within a network by enforcing instant messenger policy in a granular manner, thereby ensuring judicious use of network resources
- Reduces exposure to vulnerabilities from instant messenger clients

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3700, 3800, 7200 and 7301 Series Routers

Considerations

The feature will only be available in the Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

Additional Information: http://www.cisco.com/go/firewall/

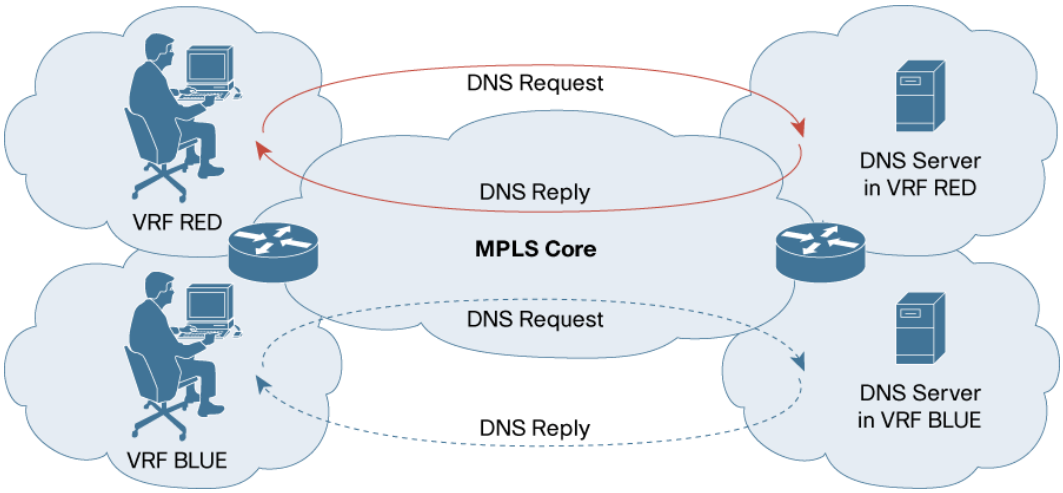
Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.3) VRF-Aware Domain Name System

The Domain Name System (DNS) translates the names of network nodes into IP addresses on the Internet. The current Cisco IOS DNS feature assumes that all name lookups should be directed to preconfigured DNS servers in the global IP address space.

Virtual Routing and Forwarding (VRF)-aware DNS extends this functionality in the context of Multiprotocol Label Switching (MPLS) VPNs by allowing users to direct DNS queries within a given VRF to their respective DNS server within that VRF.

Figure 132. VRF-Aware DNS



Benefits

Facilitates SSL-based VPN deployments in corporate remote access networks, as an alternative to existing IPsec-based VPNs

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 2600 (2600XM, 2691), 3600 (3631, 3660), 3700, 3800, 7200, 7301, and AS5000 Series Routers

Additional Information

Configuring DNS on Cisco Routers:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800c525f.shtml

Product Management Contact: Mark Denny (mdenny@cisco.com)

9.2.4) Easy VPN Phase 6

- **Auto Configuration Update:** Allows users to push configuration changes to any number of Cisco IOS Easy VPN hardware clients.
- **Dial Backup Reactivate Primary Peer:** Easy VPN client continues the IKE SA setup attempt with primary server even after failover. Once the primary becomes available, the connection is re-established and the secondary is dropped.
- **Easy VPN Remote Dual Tunnel Support:** Allows two tunnels to be built from one remote device connecting to different head-end devices.
- **Easy VPN Syslog Enhancements:** Provides enhanced logs indicating detailed reasons for session establishment failures.

Benefits

- **Auto Configuration Update:** Provides zero touch provisioning of any feature, including voice and routing.
- Easy VPN can stop worms or attacks by enabling Access Control Lists (ACLs), Firewall, Cisco IOS Intrusion Prevention System (IPS), and Quality of Service (QoS). Easy VPN client cannot join the VPN unless it applies the configuration change.

- **Dial Backup Reactivate Primary Peer:** Maintains optimum connection at all times, and does not require use of dynamic routing protocol.
- **Easy VPN Remote Dual Tunnel Support:** Supports segregation of application traffic such as voice and data to disparate locations.
- **Easy VPN Syslog Enhancements:** Important events like authentication failure and its cause are logged, to make it easy to troubleshoot VPN client connectivity failures.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Considerations

Auto Configuration Update: Release 12.4(4)T or higher must run on the router headend device

Additional Information: http://www.cisco.com/go/ipsec/

Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.5) Control Plane Protection
Control Plane Protection (CPPr) protects a router's control and management planes, ensuring routing stability, availability, and packet delivery.

Network infrastructure attacks are becoming increasingly common, highlighting the need for infrastructure protection. Denial of Services (DoS) attacks are one kind of infrastructure attack which targets a router's control plane processor. The route processor is critical to network operation and any service disruption of the control plane traffic can lead to network outages that affect business operations. Cisco's Network Foundation Protection provides the tools, technologies and services to counter these and similar threats directed towards the heart of the system, the processor. Control Plane Policing (CoPP) introduced the concept of early rate-limiting aggregate and protocol specific control plane traffic. Control Plane Protection (CPPr) extends this control plane protection functionality by providing enhanced and granular control against DoS attacks.

Benefits

- Enhanced and granular protection against DoS attacks targeting infrastructure routers
- Better platform reliability and availability

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 3700, 3800, 7200 and 7301 Series Routers

Additional Information (URLs): http://www.cisco.com/go/nfp/

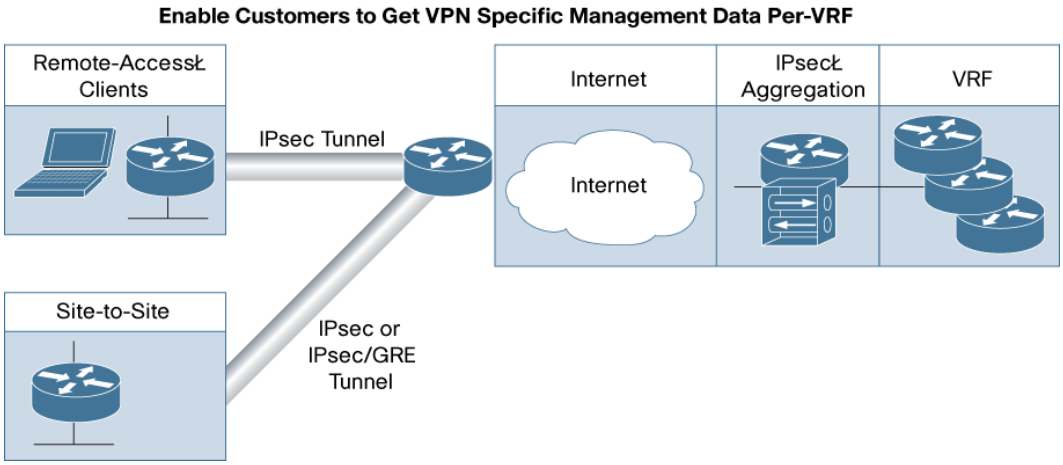
Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.6) VRF-Aware IPsec MIB
Virtual Routing and Forwarding (VRF)-Aware IPsec introduced IPsec tunnel mapping to Multiprotocol Label Switching (MPLS) VPNs. With this capability, users can map IPsec tunnels to VRF instances using single public-facing IP addresses.

VRF-Aware IPsec MIB enables customers to collect and utilize per-VPN specific management data for ongoing operational needs. The granular components of this feature includes VPN Management

data support for both site-site and remote-access deployments. The feature can be applied in the context of an IPsec, IPsec+GRE, and Virtual Tunnel Interface tunnel.

Figure 133. VRF-Aware IPsec MIB



Benefits

- Improved manageability for users who deploy VRF-Aware IPsec
- Enhanced value and flexibility: the tunnel agnostic nature of this feature reaffirms the flexibility in VPN solution choices, from a manageability perspective

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information (URLs): http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.7) IPv6 Support for Site-Site IPsec VPN

IPv6 is the next-generation network layer internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. The primary objective for IPv6 is to increase Internet global address space to accommodate the rapidly increasing numbers of users and applications that require unique global IP addresses.

Cisco IOS IPsec functionality provides network data encryption at the IP packet level, offering a robust, standards-based security solution. It provides data authentication and anti-replay services, in addition to data confidentiality services. IPsec is the only way to implement secure VPNs. Customers can combine IPsec with other Cisco IOS Software functionality to build scalable, robust, and secure Quality of Service-aware VPNs.

IPv6 support for Site-to-Site IPsec VPNs enables businesses to use advanced encryption between router-router communications on an IPv6 network. IPv6 IPsec VPN supports tunnel mode for site-to-site IPsec protection of IPv6 traffic. The feature can use IPv6 IPsec encapsulation to protect both IPv6 unicast and multicast traffic. The supported features include:

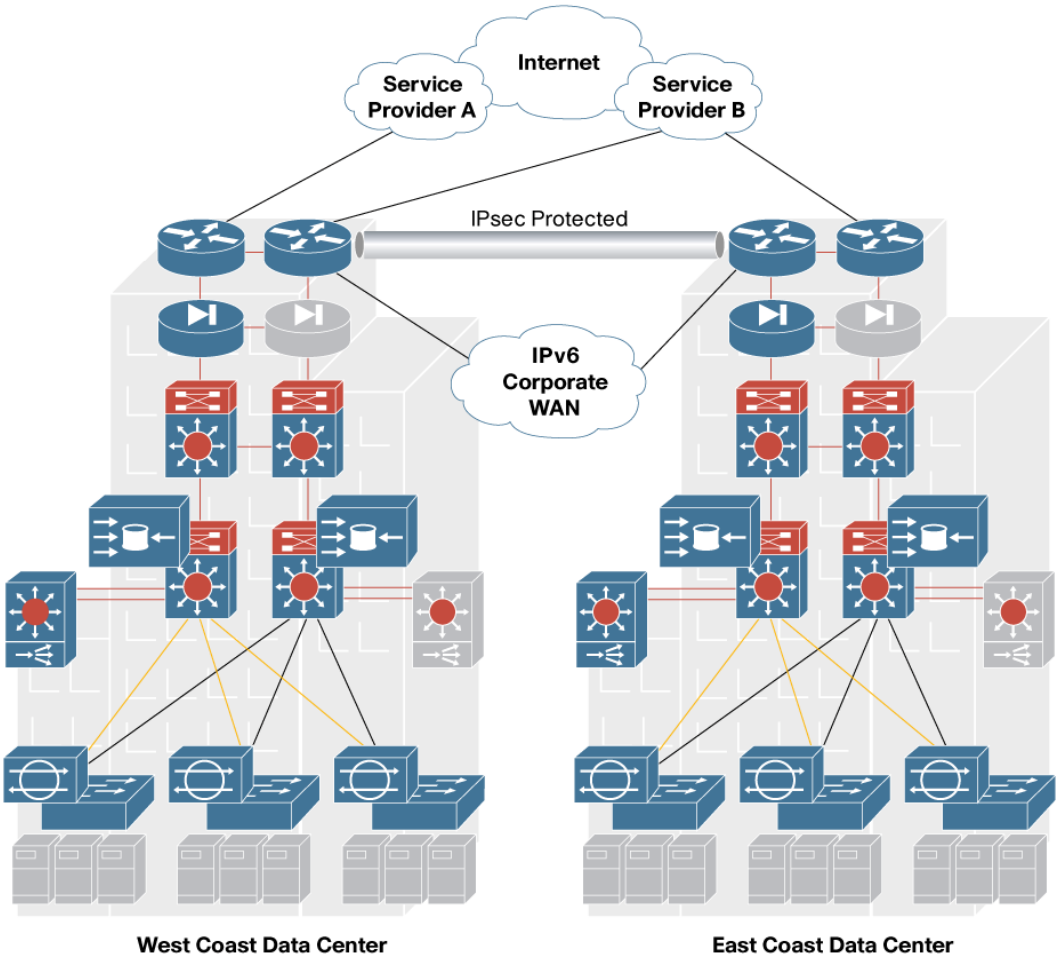
- Native IPv6 IPsec support: native IPv6 ipsec support for site-site deployments
- Tunnel Mode IPv6 IPsec encapsulation: tunnel mode introduces a one-to-one relationship between tunnels and sites with a dedicated logical interface

- Cross-vendor interoperability: flexibility to work with third party vendors under certain conditions.

Figure 134. IPv6 Support for Site-Site IPsec VPN

Enable Businesses to use Advanced Encryption Between Router-Router on an IPv6 Network

IPv6 Features	Customer Benefits
Native IPv6 Support ▪ Support Site-Site Deployments	▪ Flexibility between v4 or v6 networks
Tunnel Mode IPv6 IPsec Encapsulation ▪ 1:1 relationship between tunnels and Ł sites with a dedicated logical interface	▪ Supports both Unicast and Multicast traffic
Cisco Vendor Interoperability ▪ Can work with other vendor who Ł can support setting IP Proxy any any	▪ Cross vendor interoperability



Benefits

- Native IPv6 IPsec support: flexibility for customers to choose between secure IPv4 and IPv6 traffic
- Tunnel mode IPv6 IPsec encapsulation: flexibility for customers to run different traffic types, including unicast and multicast

- Cross vendor Interoperability: ability to work in an heterogeneous environment

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information: http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

9.2.8) Dynamic Multipoint VPN Quality of Service Support

Dynamic Multipoint VPN (DMVPN) Quality of Service (QoS) Support improves interoperation between IPsec and QoS technologies, in order to address different deployment models in Cisco VPN solutions.

The initial phase of Enhanced QoS Support for DMVPN introduces the following features:

- **Per-SA shaping on main interface:** Enables DMVPN customers to shape remote sites on the main interface. The Per-SA shaping on the main physical interface leverages the existing queuing implementation and ties the policy definitions of the remote under the main interface. Support for traffic shaping to ensure that the an enterprise accessing its service provider can meter all its traffic and send it out at a constant rate such that all its traffic passes through the service provider's policing functions.
- **Low Latency Queuing (LLQ) before Crypto Engine:** Introduces a single PQ for all egress and ingress packets. It enables per-tunnel LLQ classification and policing.
- **Enhancements to Queuing before Crypto Engine:** Helps classify packets into fair-queue such that there is one queue per tunnel based on Security Association.
- Enhancements include fair-queue system to provide per-SA fairness when crypto engine is congested, allocating Pak priority queues before crypto engine etc.
- **Prioritization of Routing Updates:** Routing updates occurring in the DMVPN network are prioritized by allocating a separate Queue.

Feature	Solution Addressed
Traffic Shaping for Spoke Overrun	Partial
Prioritization of Routing Updates	Yes
Scalability	Max 255 Spokes

Benefits

- Enhanced support for V3PN application in DMVPN networks
- Improved support for convergence of dynamic routing protocols
- Initial phase of Enhanced Quality of Service Support for Dynamic Multipoint VPN is the foundation that enables new network service offerings by service providers

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information: http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

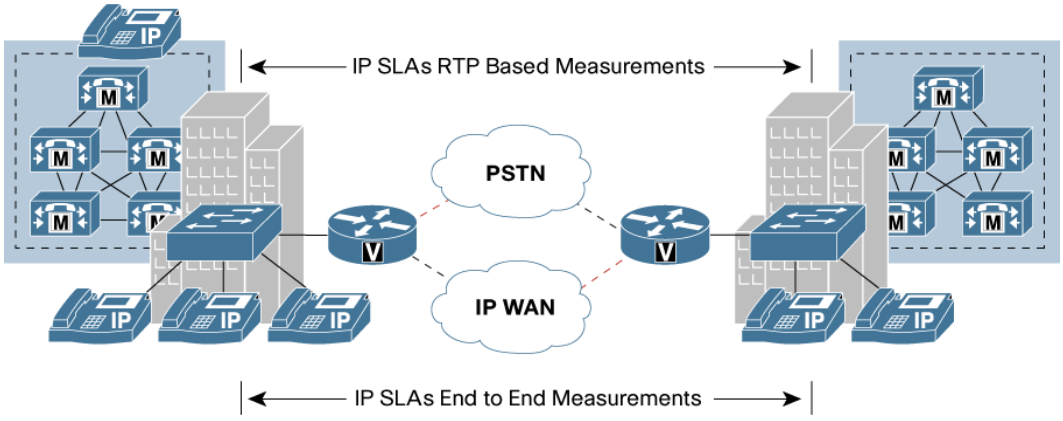
9.3) Voice

9.3.1) Cisco IOS IP Service Level Agreements for VoIP with Real Time Protocol

Customers demand guaranteed, reliable network services for business-critical applications and services. Cisco IOS IP Service Level Agreements (SLAs) is a capability embedded Cisco IOS Software, which allows Cisco customers to increase productivity, lower operational costs, and reduce the frequency of network outages. The convergence of IP and SLAs, and the extension of IP performance monitoring to become application-aware is critical for new IP network applications (ie: VoIP, audio and video, VPN). Cisco IOS IP SLAs measures end-to-end and can perform network assessments, verify Quality of Service (QoS) and ease deployment of new services, and assist administrators with network troubleshooting. Cisco IOS IP SLAs uses unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

This feature enhances Cisco IOS IP SLAs further by including a capability to create a VoIP active test call using Real Time Protocol (RTP). This feature requires DSP hardware within the device receiving the IP SLAs RTP stream. An RTP stream is generated and the voice gateway hardware (DSP) then processes the call and measures voice over IP statistics including: voice quality, jitter, frame loss, latency, acoustical round trip time and others. The voice quality scores produced include MOS-CQ, MOS-LQ, and R-Factor.

Figure 135. Cisco IOS IP SLAs RTP VoIP Operation



Benefits

- Measures performance characteristics for VoIP calls using RTP
- Calculates voice quality scores using voice gateway DSP hardware
- Extends the functionality provided by Cisco IOS IP SLAs
- Adds to the already strong VoIP monitoring capabilities
  - Performance visibility for VoIP, video, business critical applications, MPLS and VPN networks
  - SLAs monitoring
  - Network performance monitoring
  - IP Service network health readiness or assessment
  - Edge-to-edge network availability monitoring

- Business-critical applications performance monitoring
- Troubleshooting network operation

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3200, 3600 (3631, 3660), 3700, 3800, 7200, 7301, and AS5000 Series Routers

Considerations

Not available in the IP Base package.

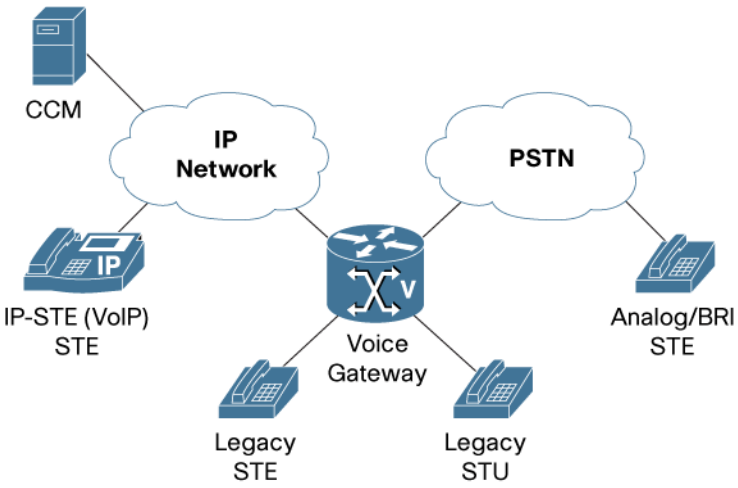
Additional Information: http://www.cisco.com/go/ipsla

Product Management Contact: Tom Zingale (tomz@cisco.com)

9.3.2) Secure Communication between IP-STE and PSTN STE Endpoints
This feature allows Analog & BRI Secure Terminal Equipment (STE) to communicate with VoIP STEs using v.150.1 Modem Relay.

STE and Secure Telephone Units STU are capable of encrypting voice and data streams with government-proprietary algorithms. To provide support for legacy STE, STU, and newer IP-STE, Cisco gateways must be able to pass calls to and from analog/BRI STE connected to Public Switched Telephone Network (PSTN)/Time Division Multiplexing (TDM) voice networks, in addition to supporting voice and data in secure and non-secure modes within the IP network. This feature provides the missing link between passing calls to/from analog/BRI STEs and VoIP STEs by adding support on the line side for v.150.1 Modem relay on Cisco gateways.

Figure 136. Secure Communication between IP-STE Endpoint and PSTN STE Endpoints



Hardware

Routers	• Cisco 2600 (2600XM, 2691), 3700, and 3800 Series Routers
Additional Devices	• Cisco VG200 Series Gateways

Product Management Contact: Stephen Childs, stchilds@cisco.com

9.3.3) Interoperability Enhancements to the Cisco Multiservice IP-IP Gateway
This feature introduces the following enhancements to the Cisco Multiservice IP-IP Gateway feature suite:

- Convenient IP-to-IP Gateway interoperability
- IP-to-IP Gateway image consolidation
- Tool Command Language Interactive Voice Response 2.0 (TCL IVR 2.0) in an IP-Only Environment

The Multiservice IP-to-IP Gateway facilitates easy and cost effective connectivity between independent VoIP service provider networks. Some in the industry call IP-to-IP Gateways “border elements” or “session border controllers”. The IP-to-IP Gateway provides a network-to-network interface point for billing, security, Cisco Call Manager interconnectivity, call admission control and signaling interworking. It will perform most of the same functions of a PSTN-to-IP gateway, but will join two VoIP call legs. Media packets can either flow through the gateway and hide the networks from each other, or flow around the IP-to-IP Gateway if network security is not of primary importance.

Benefits

Feature	Benefit Description
Convenient IP-to-IP Gateway Interoperability	Interoperability with the Cisco ATA-188 Analog Telephone Adaptor and with Microsoft NetMeeting.
IP-to-IP Gateway Image Consolidation	Allows the IP-to-IP Gateway feature set to run concurrently on the same Cisco router with TDM-to-IP voice gateway features.
TCL IVR 2.0 in an IP-Only Environment	Provides the ability to create scripted interactive voice response applications for IP endpoints. Support also includes media playout and digit collection.

Hardware

Routers	• 2600 (2600XM, 2691), 2800, 3660, 3700, 3800, 7200, 7301

Considerations

IP-to-IP Gateway and Gatekeeper support for the Cisco 2801 Integrated Services Router Requires Cisco IOS Enterprise Plus/H323 MCM or CISCO IOS Integrated Voice and Video Services software images.

Additional Information:
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/prod_literature.html

Product Management Contact: Kathy Lewis (kalewis@cisco.com)

9.3.4) Identify Alternate Endpoint Call Attempts in RADIUS Call Accounting Records
The Cisco IOS Gatekeeper provides the ability to send an ordered list of alternate endpoints in response to a call admission request (ARQ) from a calling endpoint. The alternate endpoint list identifies alternate routes to the called destination.

When this feature is enabled, the gateway call accounting record will indicate the IP address of each alternate endpoint tried, the order in which the alternate endpoints were tried, and the cause value associated with each call attempt.

Benefits

Provides information useful for tracking down and troubleshooting call routing related issues.

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3700, 3800, and AS5000 Series Routers

Product Management Contact: Kathy Lewis (kalewis@cisco.com)

9.3.5) Cisco Modem Relay
Cisco Modem Relay implements non-negotiated, bearer switched modem relay on select gateways, enabling V.34 modem traffic to be reliably transported.

This non-negotiated, bearer switched mode does not involve capability negotiation during the call setup time. Instead it is enabled directly on the gateway by way of Command Line Interface (CLI) and the media change from voice mode to modem relay mode occurs after modem tones are detected. This mode change is initiated by gateways directly over the existing bearer voice RTP stream.

Benefits

- Can be used with any call agent, including the PGW 2200, BTS 10200, Cisco Call Manager and Cisco Call Manager Express (CME).
- Works with any supported signaling protocol, including H.323, Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP).

Hardware

Routers	• Cisco 2600 (2600XM, 2691), 2800, 3600 (3631, 3660),3700 and 3800 Series Routers
Additional Devices	• Cisco VG200 Series Gateways

Considerations

V.34/V.34bis Support Only

Cisco Modem Relay, as with the “Modem Relay Support on VoIP Platforms” (12.2[11]T), supports only V.34 and V.34bis modulations. It does not directly support V.90, V.92 and other modem modulations. Note, however, almost all V.90 and V.92 modems also support V.34 and will train down to V.34 as required. Thus, V.90 and V.92 modems are effectively supported by Cisco Modem Relay at slower speeds and without V.92 features such as Modem on Hold. Slower modems such as point of sale and credit card modems (V.22, etc.) are not supported by Cisco Modem Relay. Modem Passthrough is recommended in these cases.

Product Management Contact: Steven White (whites@cisco.com)

9.3.6) Session Initiation Protocol: CLI for Passing Calling Name when Privacy Exists
This feature provides the following three Command Line Interface (CLI) options on a voice gateway that will make handling of caller ID information contained within Session Initiation Protocol (SIP) messages more flexible:

1. Ability to manage caller ID information when privacy exists. This allows the customer to indicate if the Caller ID should or should not be passed through the SIP network when privacy is indicated on the PSTN signaling interface.

2. Ability to manage the Display Name field when no Display Name exists. This allows the customer to indicate in the Display Name part of the SIP Uniform Resource Identifier (URI) to be left empty or provide the calling number when no calling name is present from the PSTN.
3. Ability to allow caller ID information to be passed to an ISDN network as 'network provided' versus 'user provided.' To be 'network provided' simply indicates to the ISDN network that the network termination device is within the Service Provider's premise whereas to be "user provided" means the network termination device is within the customer premise.

Benefits

Provides more robust Caller ID capabilities used for application screening, billing settlements and other related Caller ID services.

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2800, 3600 (3631, 3660), 3700, 3800, 7200 and AS5000 Series Routers

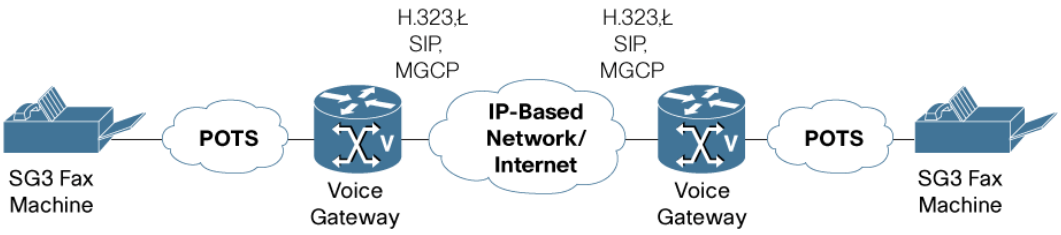
Product Management Contact: Steve Levy (stlevy@cisco.com)

9.3.7) Fax Relay Support for SG3 Fax Machines at G3 Speeds

Fax Relay Support for SG3 Fax Machines at G3 Speeds is a fax machine spoofing feature on select gateways used to force Super Group 3 (SG3) fax machines to automatically fallback to Group 3 (G3) speeds.

The Fax Relay Support for SG3 Fax Machines at G3 Speeds feature works with H.323, SIP and MGCP signaling protocols.

Figure 137. Fax Relay Support for SG3 Fax Machines at G3 Speeds



Benefits

Enables faxes to be sent between two SG3 fax machines capable of sending over 33.6 kbps over T.38 Fax Relay at supported G3 speeds (<= 14.4 kbps).

Hardware

Routers	• Cisco 2600 (2600XM, 2691), 2800, 3600 (3631, 3660), 3700, and 3800 Series Routers
Additional Devices	• IAD2400, VG200

Considerations

In order for SG3 fax machines to work using Cisco Fax Relay Support for SG3 Fax Machines at G3 speeds, the SG3 capability on at least one of the SG3 fax machines must be disabled. Most SG3 fax machines support some mechanism for disabling SG3.

Product Management Contact: Steven White (whites@cisco.com)

9.3.8) SIP-SIP Basic Support on the Cisco Multiservice IP-to-IP Gateway
This feature introduces SIP-SIP basic functionality support on the Cisco Multiservice IP-to-IP Gateway.

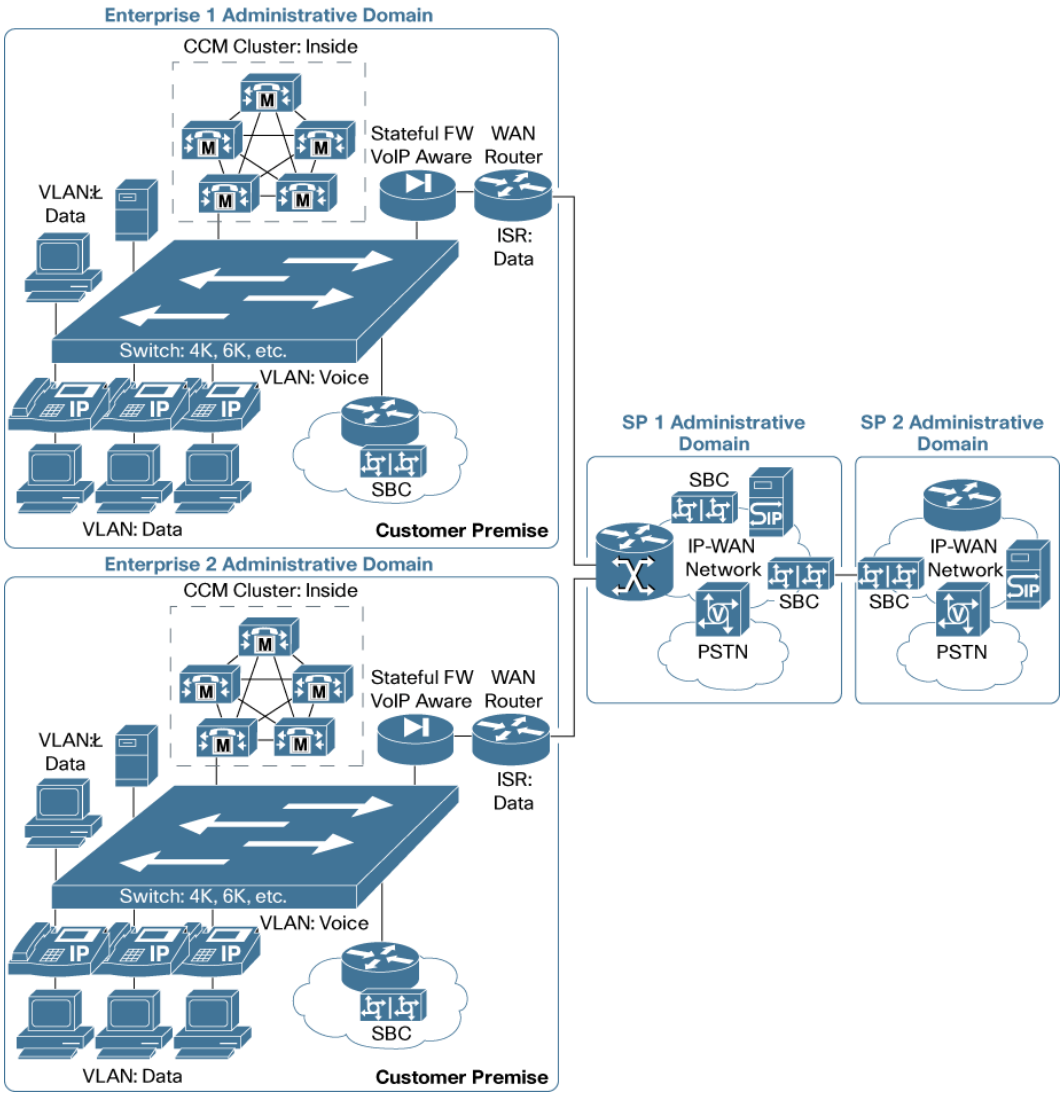
SIP-SIP basic functionality support on the Cisco Multiservice IP-to-IP Gateway provides Back-to-Back-User-Agent (B2BUA) functionality in conformance with RFC 3261 to interoperate with Session Initiation Protocol (SIP) User Agents (UAs) and includes the following enhancements to the Cisco Multiservice IP-to-IP Gateway feature suite:

- Voice calls (B2BUA)—Termination and Re-origination of Signaling and Media
- Early Media Call
- Network Topology hiding
- Codecs
  - G711ulaw,G711alaw
  - G279r8: ar8, br8, abr8
  - G.723: 5.3, 6.3, ar53, ar63
  - G.726: r16,r24, r32
  - G.728
- Codec Filtering
- Media Flow-Through
- Dual-tone Multi-frequency (DTMF)
  - RFC2833-to-RFC2833
  - SIP-Notify-to-SIP-Notify
- Fax
  - T.38
  - Cisco Fax Relay
- Transport
  - TCP
  - UDP
- Call Admission Control (CAC)
  - RSVP
  - Max-connections
- Quality of Service (QoS)
  - IP Precedence
  - DSCP
- Call Detail Records
- Tool Command Langauge (TCL) scripts with SIP RFC2833
- Rotary mode with similar codecs

The Multiservice IP-to-IP Gateway is used by service provider, enterprise, and small and medium-sized organizations to interconnect SIP and H.323 voice and video networks. The IP-to-IP gateway provides organizations with all their Session Border Control (SBC) needs integrated into the network layer interoperating with many different network elements including voice gateways, IP phones, and call-control servers, in many different application environments, from advanced

enterprise voice and/or video services with Cisco CallManager or Cisco CallManager Express, as well as simpler toll bypass and VoIP transit applications. The Cisco Multiservice IP-to-IP Gateway provides a network-to-network interface point for signaling interworking, media interworking, security, billing, and QoS and bandwidth management.

Figure 138. SIP-SIP Basic Support on the Cisco Multiservice IP-to-IP Gateway



Benefits

- B2BUA functionality in conformance with non-proprietary, open standards
- Added SIP functionality to the Cisco Multiservice IP-to-IP Gateway feature suite

Hardware

Routers	• Cisco 2600 (2600XM, 2691), 2800, 3700, 3800, 7200 and 7301 Series Routers

Considerations

IP-to-IP Gateway support for the Integrated Services Routers (ISR)—Cisco 2800 and 3800 Series or Cisco 2600XM, 3700, 7200VXR and 7301 Routers requires Cisco IOS Integrated Voice and

Video Services software images. For ordering information, refer to the Cisco Multiservice IP-to-IP Gateway datasheet.

Additional Information:
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/prod_literature.html

Product Management Contact: Jennifer Blatnik (jennyng@cisco.com)

9.3.9) Cisco CallManager Express 3.4
Cisco CallManager Express v3.4 with 12.4(4)T is enhanced with a SIP bulk registration capability, SIP phone/line side support and new fault monitoring capacity with a new CME SNMP MIB.

The bulk registration capability simplifies higher level SIP proxy registrations for enterprise and managed service deployments. New SIP line support is delivered with a SIP Back-To-Back-User Agent (B2BUA) and provides IETF RFC 3261 compliant support for IP Phones using the SIP protocol. Previously supported CME IP Phone features using SCCP are fully preserved.

The following features are now supported for IP Phones using SIP.

- Provisioning of Cisco IP Phone models using a SIP load: 7905G, 7912G, 7940G, and 7960G via Cisco IOS Software
- Register with digest authentication
- Basic call
- Transfer blind/attended
- Caller ID and name
- Forward busy/no answer/all/unreachable
- Hunt groups: sequential, parallel, combo
- CDR
- Distinctive ring receiving
- Transcoding
- Class of restriction
- Out-going call screening
- Analog phones (via ATA and VG224)
- Bulk registration w/digest authentic

In a SIP voice network features are also delivered by the phone. Features available using Cisco IP Phones using a SIP firmware load include:

- Hold/resume
- Call waiting w/caller ID
- Redial and Speed dial
- MWI (visual and audio)
- 3-way conference
- Intercom

CME previously provided a robust SIP trunking capability. CME v3.4 enhances this with the addition of a SIP bulk registration with digest authentication feature for security. Using this feature

CME SIP and SCCP phones utilizing SIP trunking can be registered to a higher level SIP proxy server. This simplifies enterprise and managed service CME deployments.

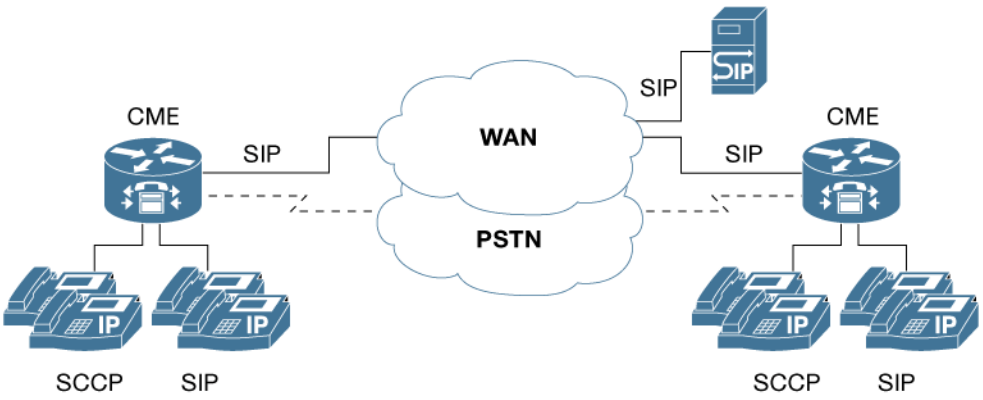
Also with CME v3.4 customers have enhanced capacity for fault reporting using SNMP. A new MIB (CISCO-CCME-MIB) has been defined which can provide fault reporting events to both Cisco or third party network management consoles.

The new CME fault reporting MIB includes:

- Traps (with Severity and Reason)
  - CCME catastrophic failures
  - Key Phone and Ephone Registration failures
  - Threshold based un-registration
  - CCME Inactive/Active state
  - Max-conf exceeded, In/out of Night Service mode
  - MoH live feed failure
- Active Monitoring
  - CME running version number
  - Number of phones registered/unregistered/auto-registered, not configured
  - DN State
  - Total Number of CME active calls
  - MoH Source
  - Phone load information
  - Phone types and button association
- Display Configuration for Troubleshooting
  - CME global parameters for ephone/ephone-dn
  - Transfer/DialPlan Pattern

CME is a solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. This solution enables the large portfolio of Cisco access and integrated services routers to deliver a robust set of features commonly used by small and medium business, enterprise branch, and service providers, thereby enabling deployment of a cost-effective highly reliable IP Communications solution for the small office and branch.

Figure 139. Cisco CallManager Express 3.4



Benefits

- CME provides call processing in the Integrated Access Router.
- CME integrates with voice mail solutions such as Cisco Unity Express and Cisco Unity.
- CME v3.4 enables bulk registration of SCCP and SIP phones to a higher level proxy server.
- CME v3.4 delivers a rich SIP trunking capability accessible to both SCCP and/or SIP phones.
- CME v3.4 provides a choice of using either feature rich SCCP or standards based SIP protocol on the station side.
- CME v3.4 provides enhanced capacity for fault reporting using a new SNMP MIB.

Hardware

Routers	• Cisco 2600XM, 2691, 2800, 3700, 3800 Series Routers
Additional Devices	• Cisco IAD2430 Integrated Access Device

Considerations

Limitations:

- IP Phones using SIP deliver less features than IP Phones using SCCP in this release.
- Call interaction between IP Phones using SIP and SCCP is limited to basic calling features only.
- When SIP phones are registered to CME, only SIP trunking between sites may be used. With SCCP phones H.323 or SIP trunking is available.
- Fault reporting is available for SCCP features only. SIP phone features are not available in the new CME MIB.

Additional Information: http://www.cisco.com/go/ccme

Product Management Contact: access-ccme-cue@cisco.com

9.3.10) Survivable Remote Site Telephony Version 3.4 Support with Release 12.4(4)T

Cisco Survivable Remote Site Telephony (SRST) version 3.4 Support with Release 12.4(4)T is enhanced with the new SRST SIP Back-To-Back-User Agent (B2BUA) and fault monitoring with a new SRST SNMP MIB.

The new B2BUA provides IETF RFC 3261 compliant support for IP Phones using SIP. Previously supported SRST IP Phone features using SCCP are fully preserved.

The following features are now supported in SRST mode for SIP phones.

- Register
- Basic call
- Inbound/outbound PSTN calls
- Caller ID and name
- Transfer blind/attended
- Class of restriction
- Forward busy/no answer/all
- Distinctive ring receiving

- After hours call blocking
- Analog phones (via ATA and VG224)

In a SIP voice network features are also delivered by the phone. Features available using Cisco IP phones using a SIP firmware load include:

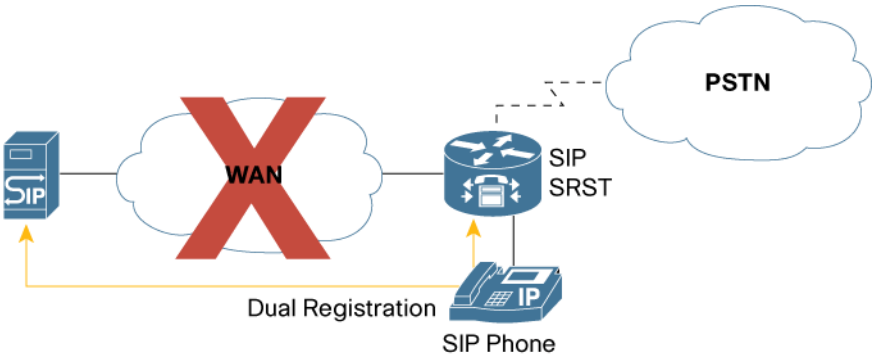
- Hold/resume
- Call waiting w/caller ID
- Redial and Speed dial
- MWI (visual and audio)
- 3-way conference
- Intercom

SRST v3.4 also gives customers new capacity for fault reporting using SNMP. A new MIB (CISCO-SRST-MIB) has been defined which can provide fault reporting events to both Cisco or third party network management consoles.

- The new SRST fault reporting MIB includes:
  - Traps (with Severity and Reason)
  - SRST catastrophic failures
  - Registration failures
  - Threshold based un-registration
  - SRST Inactive/Active states
  - Max-conf exceeded
- Active Monitoring
  - SRST state
  - Number of SCCP and SIP SRST endpoints
  - Duration of SRST state
  - Total number of SRST Calls
- Display Configuration for Troubleshooting
  - SRST global parameters for ephone/ephone-dn
  - SIP SRST configured parameters
  - Transfer/DialPlan Pattern, Alias, COR

SRST is a feature-rich call control application resident in branch routers that provides redundancy in the case of a WAN failure.

Figure 140. SRST version 3.4 Support with Release 12.4(4)T



Benefits

- SRST provides redundancy of call processing features in the event of a loss of the connection to the primary call processing agent.
- SRST integrates with Cisco Unity Express.
- SRST v3.4 adds call processing services for SIP Phones.
- SRST v3.4 provides enhanced capacity for fault reporting using new SNMP MIB.

Hardware

Routers	• Cisco 2600XM, 2691, 2800, 3700, 3800 Series Routers

Considerations

Limitations:

- IP Phones using SIP deliver less features then IP Phones using SCCP in this release.
- Call interaction between IP Phones using SIP and SCCP is limited to basic calling features only.
- To take advantage of SRST phones must dual register with the primary call agent as well as with the SRST enabled router.
- When SIP phones are registered to CME only SIP trunking between sites may be used. With SCCP phones H.323 or SIP trunking is available.
- SIP SRST support is limited to 480 phones maximum with SIP phones.

Additional Information: http://www.cisco.com/go/srst

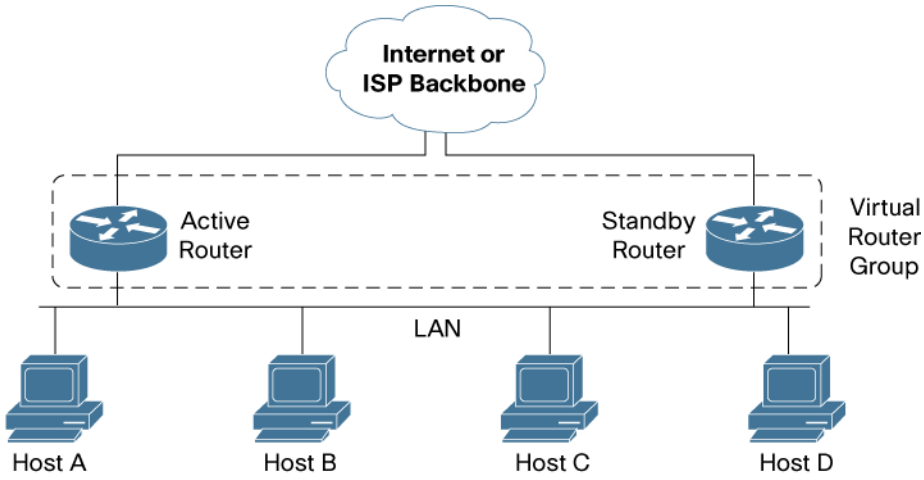
Product Management Contact: access-ccme-cue@cisco.com

9.4) High Availability

9.4.1) Cisco Hot Standby Router Protocol for IPv6

Cisco Hot Standby Router Protocol (HSRP) for IPv6 provides a fast switchover to an alternate default router than can be obtained using standard IPv6 Neighbor Discovery (ND) procedures. Using HSRP for IPv6, a backup router can take over for a failed default router within seconds using HSRP default parameters, or less than one second if millisecond HSRP timers are used. This is accomplished without any interaction with the hosts, and a minimum amount of HSRP traffic.

Figure 141. Cisco HSRP for IPv6



Benefits

- Increases network availability by providing protection against router failures.
- Provides network redundancy for IPv6 networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3200, 3600 (3631, 3660), 3700, 3800, 7200, 7301, and AS5000 Series Routers

Considerations

There is no “default gateway” concept in IPv6. The router address is learned through Router Advertisement (RA). On a LAN where a number of routers form an HSRP group, should a router not be configured for HSRP, there would be a risk to see two different RAs reaching the hosts. An RA would be generated by the HSRP virtual gateway and another by the router out of the HSRP group. Hosts would then load balance the packets between the misconfigured router and the HSRP virtual gateway. To prevent this, Cisco recommends setting up the Default Router Selection feature introduced in Release 12.4(2)T. Setting-up RA priority to “high” on HSRP routers would allow the HSRP routers to be preferred.

Additional Information:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html

Product Management Contact: Benoit Lourdelet (blourdel@cisco.com)

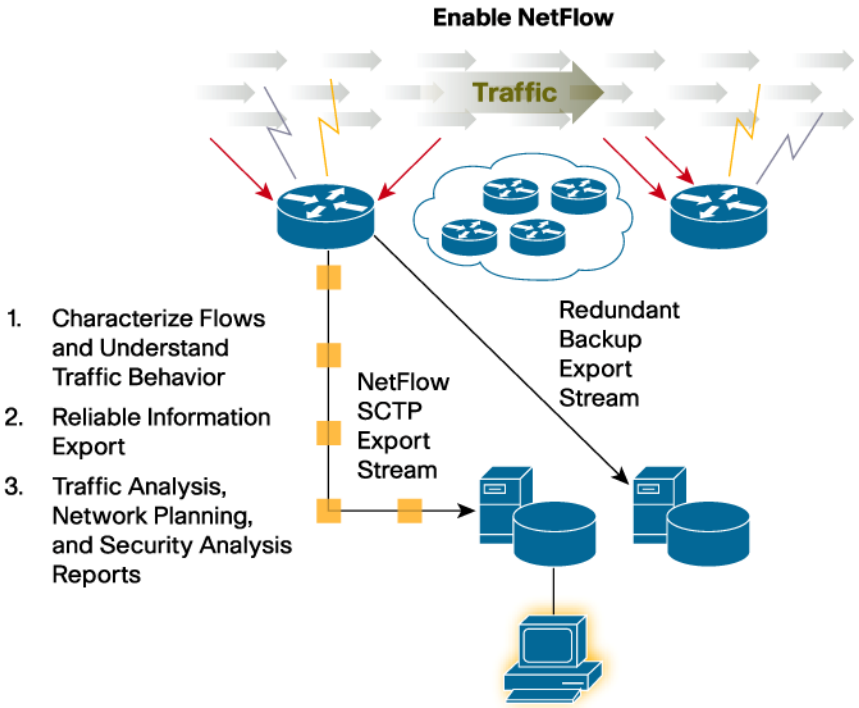
9.4.2) NetFlow Reliable Export via Stream Control Transport Protocol

Understanding who is using the network and for how long, what protocols and applications are being utilized and where the network data is flowing is a necessity for today’s IP networks managers. IP network managers rely on exported NetFlow data for a variety of purposes, including understanding network telemetry, to audit network health, security monitoring, capacity planning, billing, departmental charge back and troubleshooting.

NetFlow data is traditionally exported to a NetFlow collector where reports are generated. Historically NetFlow export information has been very scalable and efficient when sent over the

unreliable UDP protocol. In this release a new reliable export mechanism is introduced: Stream Control Transport Protocol (SCTP) is now available for NetFlow export data. SCTP allows congestion aware and reliable export of NetFlow data to the NetFlow collector. SCTP export is also highly available with redundant backup export streams for automated failover when a NetFlow collector is unavailable.

Figure 142. NetFlow SCTP Export Stream



Benefits

- Reliable and congestion aware NetFlow export
- High reliability with redundant export streams for NetFlow information
- Useful for accounting and billing data

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3700, 3800 and 7200 Series Routers

Additional Information: http://www.cisco.com/go/netflow

Product Management Contact: Tom Zingale (tomz@cisco.com)

9.5) Management Instrumentation

9.5.1) NetFlow Top Talkers CLI

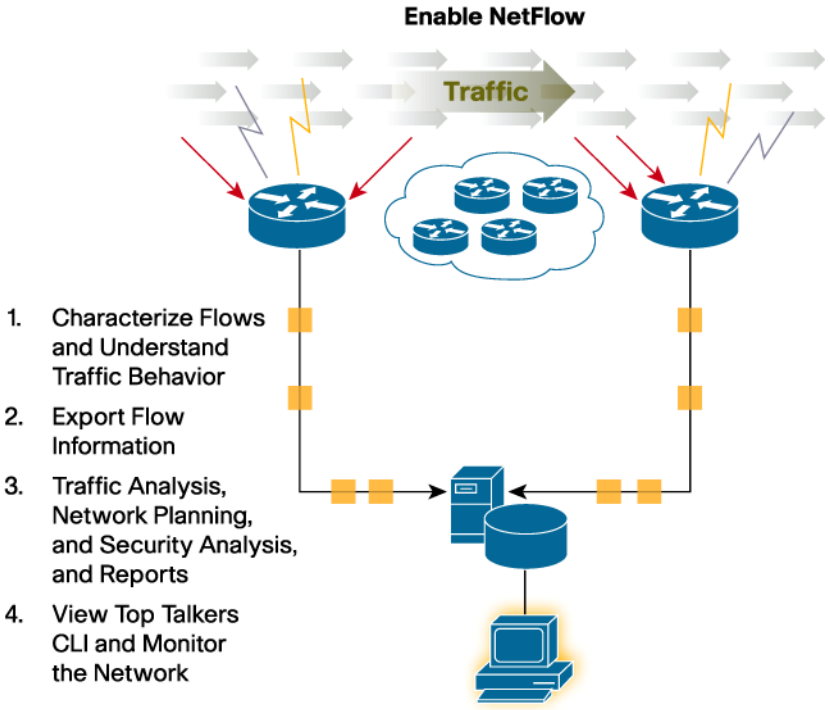
Understanding who is using the network and for how long, what protocols and applications are being utilized and where the network data is flowing is a necessity for today's IP networks managers. IP network managers rely on exported NetFlow data for a variety of purposes, including

understanding network telemetry, to audit network health, security monitoring, capacity planning, billing, departmental charge back and troubleshooting.

NetFlow Top Talkers CLI is a new flexible and extensible method to search the NetFlow cache for information. It can be used for troubleshooting or security monitoring when directly connected to a Cisco device. Some example uses of the new NetFlow Top Talkers CLI include:

- Show the top protocols currently flowing through the router
- Show the 10 IP addresses which are sending the most packets
- Show the 5 destination addresses which are routing the most traffic from a specific source network
- Show the 50 VLAN's which we're sending the least bytes
- Show the top 20 sources of 1-packet flows

Figure 143. NetFlow Top Talkers CLI



Benefits

- Real time network monitoring and trouble shooting capability in Cisco IOS Software
- Flexible and extensible method to monitor top talkers and search the NetFlow cache

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700, 1800, 2600, 2800, 3700, 3800 and 7200 Series Routers

Additional Information: http://www.cisco.com/go/netflow

Product Management Contact: Tom Zingale (tomz@cisco.com)

9.6) Quality of Service

9.6.1) Skype Classification via NBAR Packet Description Language Modules
Skype is a popular VoIP telephony service that allows users to speak, send instant messages, and/or send files to one another via the Internet.

This functionality provides the ability to recognize Skype application traffic in Cisco IOS Software. The NBAR PDLM for Skype classification is integrated into Cisco IOS Software. There will not be a downloadable PDLM for Skype because of infrastructure changes required to accommodate Skype application classification.

Benefits

- Discover Skype application traffic
- Use Cisco IOS QoS marking to assign priority for Skype voice and application traffic

Hardware

Routers	• Cisco 800, 1700, 2600, 3600, 3700, 7200, 7300 and 7500 Series Routers

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

9.6.2) Direct Connect Packet Description Language Modules Native Implementation
Direct Connect is a popular Peer-to-Peer (P2P) software application that facilitates audio, video, and image file-sharing between clients. The Direct Connect application provides complete distributed file-searching and file-sharing with other peers running the Direct Connect application.

This PDLM adds support for Direct Connect application recognition in Cisco IOS Software. An NBAR PDLM for Direct Connect is also available for use on earlier versions of Cisco IOS software.

Benefits

- Recognize, classify, and monitor Direct Connect traffic
- Enables users to assign priority for, and handling, of Direct Connect traffic

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3700, 3800, 7200 and 7301 Series Routers

Additional Information:

- NeoModus Direct Connect: http://en.wikipedia.org/wiki/NeoModus_Direct_Connect
- NBAR Packet Description Language Modules: http://www.cisco.com/pcgi-bin/tablebuild.pl/pdlm

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

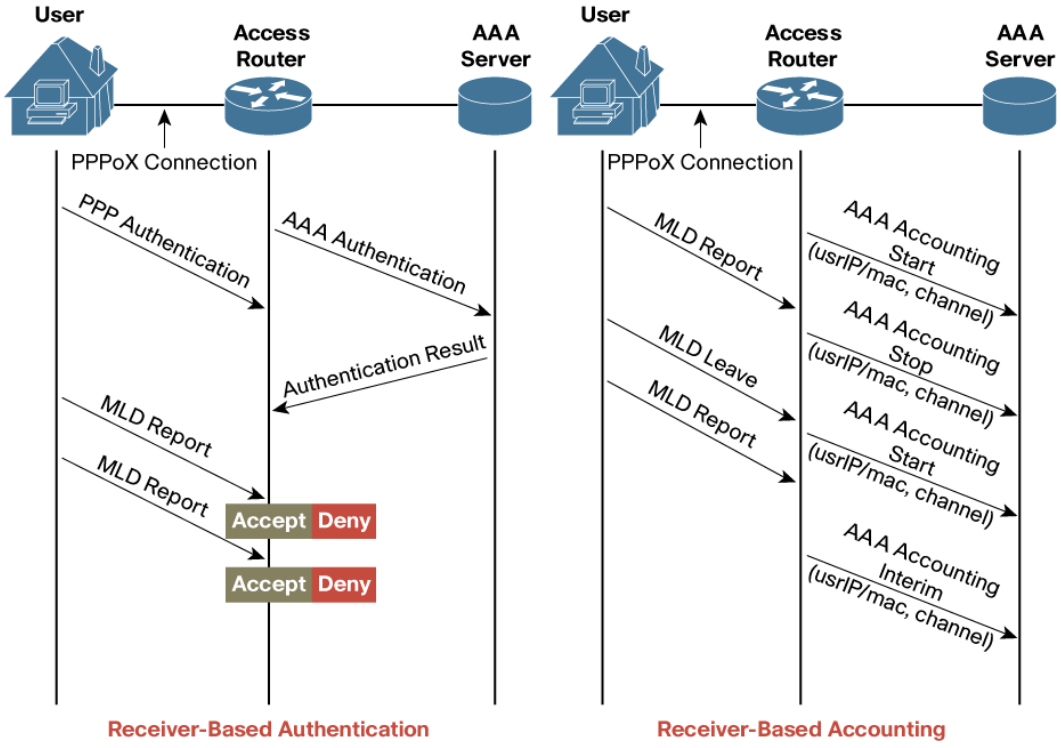
9.7) Broadband

9.7.1) Multicast User Authentication and Profile Support
Multicast User Authentication and Profile support is a new method of controlling and tracking multicast sources and receivers. Typical techniques used to control and track sources and receivers were tedious, cumbersome, and overly complex. Dedicated resources were required to manage and apply access-lists on every edge router in a multicast enabled network. This technique

was prone to human error and did not scale well for large networks with thousands of interested multicast sources and receivers.

Multicast User Authentication and Profile support leverages existing Cisco IOS Authentication, Authorization, and Accounting (AAA) features, as well as the Multicast Listener Discovery (MLD) mechanisms in Cisco IOS Software, to address these issues. It provides a centralized authentication and accounting framework for multicast users in large networks.

Figure 144. Multicast User Authentication and Profile Support



Benefits

- Improved manageability
- Scalable policies that can be pushed down to edge routers based on AAA profiles centrally stored on an AAA Server
- Reduced human error
- Leverages AAA, the widely recognized and adopted open Internet standard

Hardware

Routers	• Cisco 7200 Series

Considerations

The first phase of the Multicast User Authentication and Profile support feature will allow the control and tracking of multicast receivers, and will support only IPv6 multicast environments.

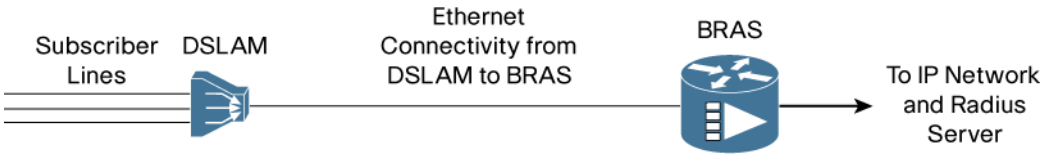
Product Management Contact: Michael Lin (mhelin@cisco.com)

9.7.2) Point-to-Point Protocol over Ethernet Circuit ID Tag Processing

The Point-to-Point Protocol over Ethernet (PPPoE) Circuit ID Tag Processing functionality, based upon the PPP Tag standard specified in draft DSL Forum 2004-071, allows Broadband Remote Access Servers (BRAS) to perform Subscriber Line Identification of DSL users when using DSLAMs with Ethernet uplinks. For Broadband environments with Ethernet connectivity between the DSLAM and BRAS, the standard practice (in ATM DSLAM environments) of mapping the subscriber line identification via an ATM VC does not work.

The DSL forum document 2004-071 focuses on the problem of transferring subscriber line identification from the DSLAM to the BRAS and eventually to AAA/Radius/DHCP servers. The addition of a PPP Tag to standard PPP packets is the mechanism used at the DSLAM to identify the subscriber line. The BRAS then needs to handle this PPP Tag with PPP Tag Intermediate Agent functionality which can transfer the subscriber line information from the PPP Tag to the appropriate places for the AAA/Radius servers. This subscriber line information is important for troubleshooting, authentication, and accounting issues in Broadband DSL networks.

Figure 145. DSL Broadband Network with Ethernet Connectivity between DSLAM and BRAS



Benefits

- Provides mechanism for subscriber line identification for Ethernet based DSLAMs
- Based upon DSL Forum draft standard 2004-071
- Simplifies troubleshooting, authentication, and accounting in Broadband DSL networks

Hardware

Routers	• Cisco 7200 and 7301 Series Routers

Product Management Contact: Michael Lin (mhelin@cisco.com)

9.8) IP Routing

9.8.1) Bidirectional Forwarding Detection Support

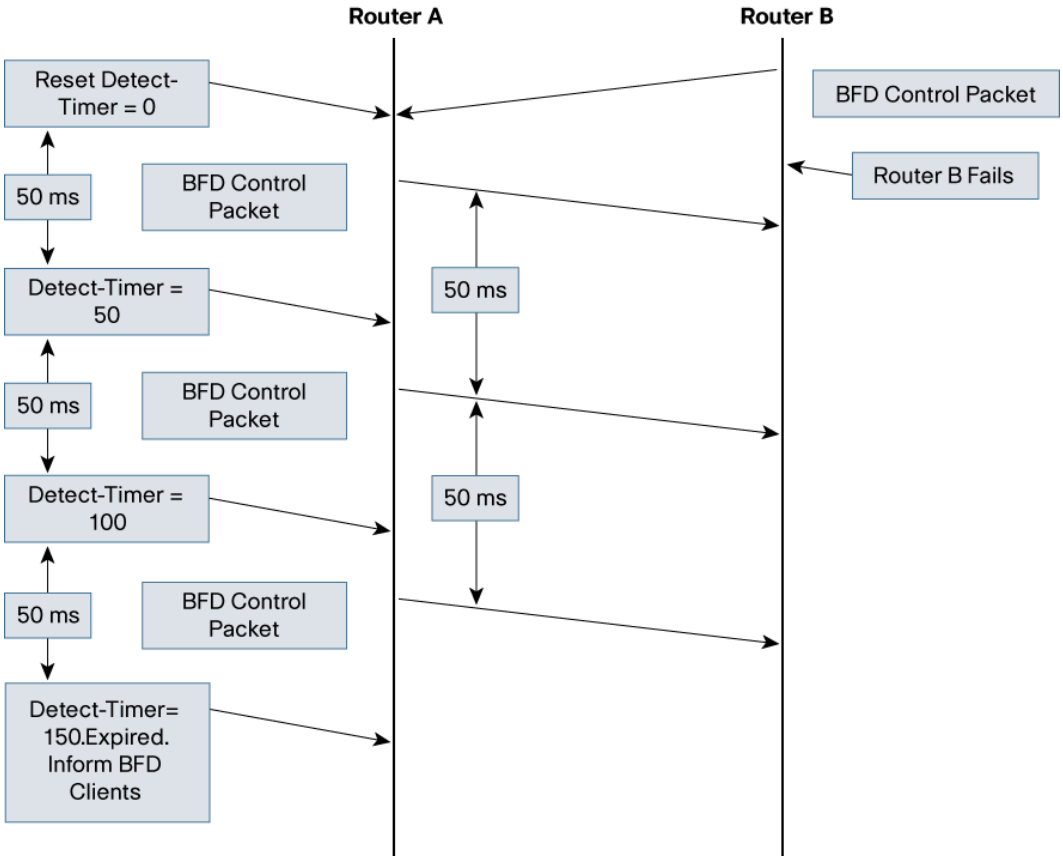
Bi-directional Forwarding Detection (BFD) provides rapid failure detection times between forwarding engines, while maintaining low overhead. It also provides a single, standardized method of link/device/protocol failure detection at any protocol layer and over any media.

The convergence of business-critical applications onto a common IP infrastructure in enterprise and service provider networks is becoming more common. Given the criticality of the data, these networks are typically constructed with a high degree of redundancy. While such redundancy is desirable, its effectiveness is dependant upon the ability of individual network devices to quickly detect failures and reroute traffic to an alternate path.

This detection is usually accomplished via hardware detection mechanisms. However, the signals from these mechanisms are not always conveyed directly to the upper protocol layers. When the hardware mechanisms do not exist (ie: Ethernet) or when the signaling does not reach the upper protocol layers, the protocols must rely on their much slower strategies to detect failures. The

detection times in existing protocols are typically greater than one second, and sometimes much longer. For some applications, this is too long to be useful.

Figure 146. BDF Support



In this example, Router A detects Router B failure within 150 msec after missing 3 BFD control packets from the Router B. The BFD on the Router A, then, informs its clients (such as OSPF routing protocol process) about the failure.

Benefits

- Facilitates faster network convergence due to faster failure detection of link/neighbor
- Allows for media independent link-failure detection
- Enables easier network profiling and planning

Hardware

Routers	• Cisco 7200 and 7301 Series Routers

Considerations

- The first phase release of the BFD supports EIGRP, OSPF, ISIS, and BGP single-hop peers over Ethernet interfaces.
- BFD is not supported over OSPF virtual links or sham links, as the current specification for BFD usage on IP links limits BFD to one-hop adjacencies.
- Care should be taken while configuring BFD timers. Consider CPU utilization, link speed, and speed of light constraints before setting low values.

- BFD is not intended as a protocol to detect CRC errors or packet loss between two adjacent routers.

Product Management Contact: Pepe Garcia (pepe@cisco.com)

9.8.2) Border Gateway Protocol Route-Map Continue Support for Outbound Policy

Border Gateway Protocol (BGP) Route-Map Continue Support for Outbound Policy introduces the continue clause to BGP route-map configuration for outbound policies in addition to the already supported inbound policies.

The continue clause provides more programmable policy configuration and route filtering. It introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow you to configure and organize more modular policy definitions to reduce the number of policy configurations that are repeated within the same route map.

Benefits

- Continue clauses provide a programmable method to organize and control the flow of a route map. Route-map configuration was linear before this feature was introduced.
- Continue clauses allow you to modularize network policy configuration so that repeated inbound or outbound policy definitions can be reduced within the same route-map.

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3600 (3631, 3660), 3700, 3800, 7200 and 7301 Series Routers

Considerations

- Continue clauses are supported for both inbound and outbound route maps.
- Continue clauses can only go to a higher route-map entry (higher sequence number) and cannot go to a lower route-map entry.

Product Management Contact: Pepe Garcia (pepe@cisco.com)

9.8.3) Border Gateway Protocol Selective Next-Hop Route Filtering

Border Gateway Protocol (BGP) Selective Next-Hop Route Filtering allows customers to configure the length of a prefix covering a BGP next-hop. The next-hop to a BGP prefix may be covered by different routing protocols and different routes/prefixes in the routing table. If a route is not available (ie: not in the RIB) then the BGP prefix is marked unreachable.

This enhancement allows customers to restrict the prefix length (via a route-map) or the protocol-source (ie: IGP, BGP, etc.) used to validate a next-hop route in the routing table. If the route is less specific (ie: a /24 instead of a /30) or is learned via some protocol (ie: BGP), then the next-hop will be considered unreachable.

Benefits

Customers have more granular control on the BGP next-hop resolution process.

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3600 (3631, 3660), 3700, 3800, 7200 and 7301 Series Routers

Considerations

The route-map used to implement the selective next-hop route filtering supports only “match ip address” and “match source-protocol”. No other “match” statements are evaluated and no “set” statements are applied.

Product Management Contact: Pepe Garcia (pepe@cisco.com)

10) Release 12.4(2)T Feature Technology Highlights

Table 28. Release 12.4(2)T Hardware and Feature Highlights

10.1) Hardware	10.2) Cisco IOS Security	10.3) Voice	10.4) Cisco IOS Infrastructure	10.5) Access Technology
10.1.1) Cisco 850 Series Integrated Services Routers 10.1.2) Cisco 870 Series Integrated Services Routers 10.1.3) Cisco 1800 Series Integrated Services Routers—Fixed Configuration Models 10.1.4) Cisco High-Speed Intra Chassis Module Interconnect 10.1.5) Inline Power Auto Negotiation	10.2.1) Cisco Router and Security Device Manager 2.1.2 10.2.2) Transparent Cisco IOS Intrusion Prevention System 10.2.3) Easy VPN Dynamic Virtual Tunnel Interfaces 10.2.4) Other Easy VPN Enhancements 10.2.5) Certificate Authority Key Rollover 10.2.6) Configurable Certificate Storage Location 10.2.7) Network Address Translation Optimize Media Path for Session Initiation Protocol Traffic 10.2.8) Zeroization	10.3.1) Session Initiation Protocol Support of Resource Priority Header and Reason Header 10.3.2) Session Initiation Protocol: User Agent MIB 10.3.3) Configurable Hostname in Locally Generated Session Initiation Protocol Headers 10.3.4) Secure Communication between IP-STE Endpoint and STE Endpoint 10.3.5) Land Mobile Radio over IP Enhancement 10.3.6) Media Gateway Control Protocol Controlled Backhaul of Basic Rate Interface Signaling 10.3.7) Skinny Client Control Protocol Analog (FXS) Ports Supplementary Feature Support for Cisco VG 224 10.3.8) E1 R2 Collect Call Blocking	10.4.1) Cisco IOS Embedded Event Manager Version 2.2	10.5.1) Authentication, Authorization, and Accounting CLI Stop Record Enhancement 10.5.2) Calling Number Suppression for Layer 2 Tunnel Protocol Setup 10.5.3) Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support 10.5.4) Service Selection Gateway—Configurable Maximum Number of Allowed Subscribers 10.5.5) Service Selection Gateway Support of WISPr RADIUS Attributes 10.5.6) Routed Bridge Encapsulation Client Side Encapsulation with Quality of Service 10.5.7) Define Interface Policy-Map AV Pairs Authentication, Authorization, and Accounting

10.6) Management Instrumentation	10.7) Quality of Service	10.8) IP Multicast	10.9) IP Routing	10.10) IP Services
10.6.1) Cisco IOS IP Service Level Agreements Random Scheduler 10.6.2) NetFlow Top Talker CLI—Phase 2 10.6.3) Advanced Encryption Standard and Triple-Data Encryption Standard Algorithm Encryption Support for SNMPv3	10.7.1) BitTorrent Packet Description Language Modules Native Implementation 10.7.2) Citrix ICA Published Applications Native Implementation 10.7.3) Multiple Matches Per Port 10.7.4) Modular Quality of Service CLI Policy Map Support on Configured Virtual Circuit Range Asynchronous Transfer Mode	10.8.1) Multicast Listener Discovery Group Limits 10.8.2) IPv6 Boot Strap Router—Ability to Configure Rendezvous Point Mapping 10.8.3) IPv6 Source Specific Multicast Mapping 10.8.4) Multicast Source Discovery Protocol MD5 Password Authentication	10.9.1) Application-Aware Routing: Policy Based RoutingEight9 10.9.2) TCP Show Extension 10.9.3) Internet Control Message Protocol Unreachable Rate Limiting User Feedback 10.9.4) “Clear IP Traffic” CLI	10.10.1) IPv6 Access Control List Extensions for Mobile IPv6 10.10.2) IPv6 Default Router Preference 10.10.3) Foreign Agent Local Route Optimization

10.1) Hardware

10.1.1) Cisco 850 Series Integrated Services Routers

The Cisco 850 Series Integrated Services Routers support broadband cable and Asymmetric DSL (ADSL) over analog telephone lines connections. Designed for very small offices, the routers provide secure WAN connectivity with optional integrated wireless LAN connectivity in a single device. Easy setup allows the Cisco 850 Series to be deployed at small remote offices and small businesses, and remote management features enable IT managers and service providers to provide better support at remote sites.

Figure 147. Cisco 851 Integrated Services Router

Benefits

- Provides secure access when connecting to the Internet or connecting small offices to a central site.
- High-speed LAN ports connect multiple devices to the small office network.
- Offers a secure broadband router and access point for WLANs in a single device.
- Out-of-band management with an external modem through the auxiliary port allows IT managers to remotely manage routers at small office sites.
- Cisco Configuration Express Service supports factory-loaded configurations in high-volume deployments.
- Support for the Cisco CNS 2100 Series Intelligence Engine enables plug-and-play installations with centralized configuration management.

Additional Information: Cisco 850 Series Integrated Services Routers Data Sheet

Product Management Contact: Hari Harikrishnan (harikris@cisco.com)

10.1.2) Cisco 870 Series Integrated Services Routers

The Cisco 870 Series extends the high performance, secure concurrent services, including Firewall, VPNs, and wireless LANs, at broadband speeds to small offices. Easy deployment and centralized management features enable the Cisco 870 Series to be deployed in small office or teleworker sites as part of an Enterprise network, used by small to medium business customers for secure WAN & Wireless LAN connectivity or used by Service Providers to offer business class broadband & Wireless LAN services.

Figure 148. Cisco 871 Integrated Services Router

Benefits

- The performance in a Cisco 870 Series router allows customers to take advantage of broadband network speeds while running secure, concurrent data, voice, and video services.
- Integrated Stateful Inspection Firewall for network perimeter security, high-speed IPsec 3DES and AES encryption for data privacy over the Internet, IPS, and antivirus support through NAC to enforce security policy in a larger enterprise or service provider network.
- Broadband router with secure WLAN in a single device.
- Allows multiple devices to be connected in a small office, with the ability to designate a port as network DMZ.
- Using smart wizards and task-based tutorials, Cisco SDM helps resellers and customers quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Software command-line interface (CLI).
- Cisco Configuration Express Service supports factory-loaded configurations for high-volume deployments.

Additional Information: Cisco 870 Series Integrated Services Routers Data Sheet

Product Management Contact: Hari Harikrishnan (harikris@cisco.com)

10.1.3) Cisco 1800 Series Integrated Services Routers—Fixed Configuration Models

Cisco 1800 Series are the next evolution of the award-winning Cisco 1700 Series modular access routers. The Cisco 1800 Series fixed-configuration routers are designed for secure broadband, Metro Ethernet, and wireless connectivity. They also help businesses reduce costs by enabling deployment of a single device to provide multiple services (integrated router with redundant link, LAN switch, firewall, VPN, IPS, wireless technology, and quality of service [QoS]) typically performed by separate devices.

Figure 149. Cisco 1800 Series Fixed-Configuration Routers

Benefits

- High-speed processor delivers exceptional processing power for applications and concurrent security and wireless services.
- Offers flexibility to connect to various types of DSL broadband or cable access or Ethernet access. Additional capability to deploy redundant WAN connections for failover protections and load balancing.
- Stateful firewall with URL filtering protects the network from unauthorized user access. URL filtering prevents inappropriate Websites from being accessed and downloading of offensive content.
- Detects harmful network activity and generates alarms to warn of threats and intrusion attempts. New IPS signatures can be dynamically loaded.
- Provides simultaneous operation at multiple Wi-Fi frequencies including 2.4 GHz and 5 GHz. Enterprise advanced management and configuration capabilities are offered through a Web-based GUI.

Additional Information: Cisco 1800 Series Integrated Services Routers—Fixed Configuration Models Data Sheet

Product Management Contact: Dwayne Thaele (dthaele@cisco.com)

10.1.4) Cisco High-Speed Intra Chassis Module Interconnect

This document provides sample configurations for the Cisco High-Speed Intrachassis Module Interconnect (HIMI). HIMI provides a dedicated, point-to-point interconnection between NME-to-NME or from NME to the onboard Gigabit Ethernet SFP port. HIMI is a Layer 2 channel that scales up to 1 Gbps.

Note: HIMI will only be available to Enhanced Network Modules (NMEs). Currently, Cisco EtherSwitch service modules are the only NMEs that support HIMI besides the router onboard Gigabit Ethernet SFP port (port 0/0) on Cisco 3825 routers and Cisco 3845 routers.

Note: HIMI supports a maximum of two NMEs per platform.

Benefits

- Allows modules to connect to each other or to the onboard SFP without accessing the router CPU.
- Allows extension of a Layer 2 environment between switching.

Hardware

Routers	• Cisco 3800 Series Routers

Considerations

The Cisco 3825 router supports EtherSwitch service module slots 1 and 2. The Cisco 3845 router supports EtherSwitch service module slots 2 and 4.

Product Management Contact: Kevin Sullivan (kevsulli@cisco.com)

10.1.5) Inline Power Auto Negotiation

Cisco devices are capable of automatically negotiating inline power levels with an IEEE 802.3af capable power device or pre IEEE Cisco device using a Cisco Discovery Protocol (CDP) extension. This feature extends the support of automatic negotiation of inline power levels to the HWIC-D-9ESW and HWIC-4ESW modules on the Cisco 2800, and 3800 series routers.

New Cisco devices that employ inline -48V power are able to power up in a low-power mode. After power-up these devices have the capability to use CDP protocol to negotiate to a high-power mode to enable more features. For example, the Cisco 7970G IP Phone can transition to a 10.25W mode from the initial 6.3W mode and let the user adjust the screen brightness to a higher level than is possible with 6.3W.

Benefits

Extends the automatic inline power levels negotiation to HWIC-4ESW and HWICD-9ESW modules.

Hardware

Routers	• Cisco 2800 and 3800 Series Routers

Additional Information: Power over Ethernet Solution

Product Management Contact: Shaji Ravindranathan (snathan@cisco.com)

10.2) Cisco IOS Security

10.2.1) Cisco Router and Security Device Manager 2.1.2

Cisco Security and Router Device Manager (SDM) combines routing and security services management with ease of use, intelligent wizards, and in-depth troubleshooting capabilities to provide a tool that supports the **Benefits** of integrating services onto the router. Customers can now synchronize the routing and security policies throughout the network, enjoy a more comprehensive view of their router services status, and reduce their operational costs.

The Cisco SDM user interface, online help, and tutorials have been translated into Japanese, Simplified Chinese, French, German, Spanish, and Italian. Microsoft Windows OS also supports these languages.

Benefits

Simplifies router and security management for native language users.

Hardware

Routers	• Cisco SB 100, 830, 850, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco Router and Security Device Manager

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.2) Transparent Cisco IOS Intrusion Prevention System

Transparent Cisco IOS IPS simultaneously scans traffic at Layer 3 and Layer 2. It enables the network administrator to deploy IPS in an existing network without changing the statically addressed peripheral devices on the trusted network.

This is an example of a retail store environment in which wireless devices have been statically addressed. They need to access the database, but the danger is that someone in the parking lot could potentially enter the network and avoid being scanned by IPS. This network is vulnerable to wireless access point intrusion.

Figure 150. Without Transparent Cisco IOS IPS

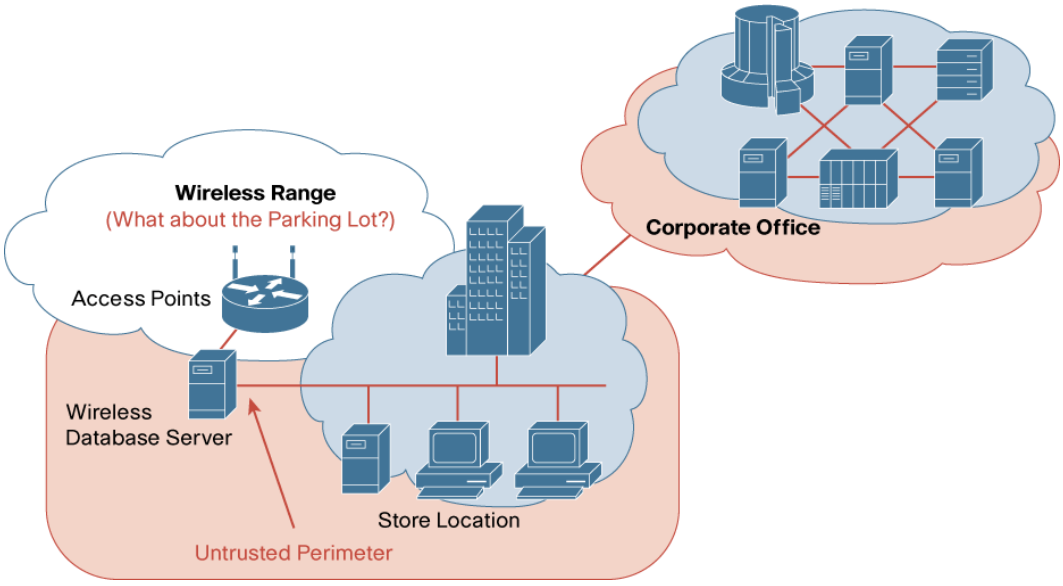
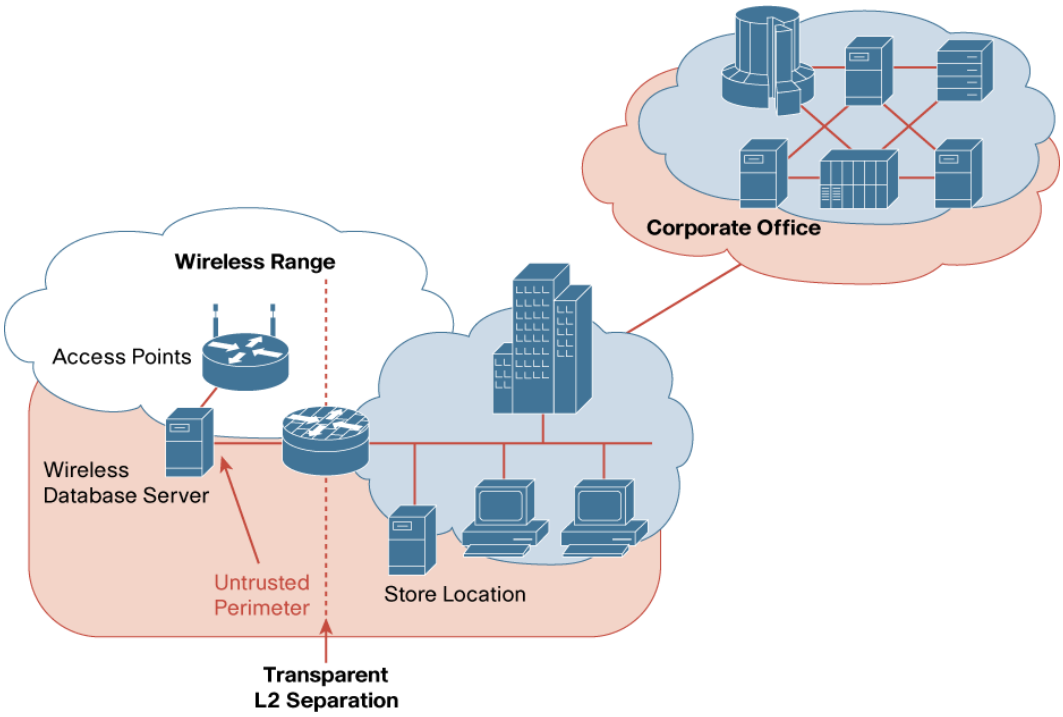


Figure 138 illustrates the effect of Transparent Cisco IOS IPS on a network. If a hacker tries to compromise the wireless side of the network, Cisco IOS IPS can scan the traffic and deny unwanted attacking traffic.

Figure 151. With Transparent Cisco IOS IPS



Transparent Cisco IOS IPS is configured with Layer 3 IPS rules using the “ip ips” command. The ‘ips in/out’ command can be configured on any of the bridged interfaces for Layer 2 protection while also being configured on any LAN or serial interfaces to provide traditional Layer 3 protection. The Transparent IPS operates on bridged packets and the layer 3 IPS continues to operate on routed packets.

Benefits

- Ability to insert IPS within an existing network.
- Eliminates the need to manually readdress previous statically defined devices, which is a tedious and resource intensive task.
- Provides both Layer 2 and Layer 3 IPS capabilities on the same router.
- Cisco IOS Software bridging supports any number of interfaces or sub-interfaces in a bridge-group.
- Supports multiple interfaces.

Hardware

Routers	• Cisco 830, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200, and 7301 Series Routers

Considerations

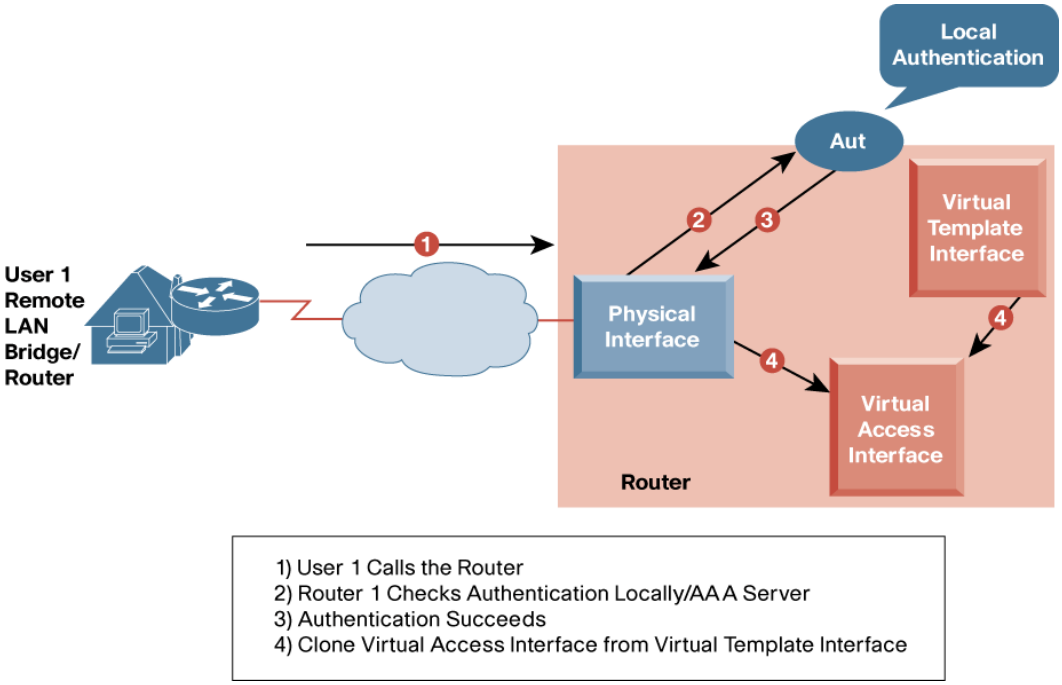
1. Transparent IPS only inspects TCP, UDP and ICMP traffic and supports 802.1Q vlan trunks.
2. Transparent IPS does not support ISL encapsulation. ISL VLANs will work when sub-interfaces are created and placed in the bridge-group.

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.3) Easy VPN Dynamic Virtual Tunnel Interfaces

An IPsec Virtual Tunnel Interface is an interface to support native IPsec tunneling. It has most of the properties of a physical interface. When combined with Easy VPN, it provides a very powerful solution—creating virtual IPsec interfaces dynamically (akin to what is currently done in the dial world) to enable the deployment of large scale IPsec networks with very minimal configuration.

Figure 152. Easy VPN Dynamic Virtual Tunnel Interfaces



Benefits

- Simplified VPN configuration.
  - Eliminates Crypto Maps, Crypto Access Control Lists (ACLs) for ease of management.
  - Minimal configuration on router allows rapid deployment of VPNs.
- Supports per-session features.
  - Per-user attributes such as QoS empower the Admin to set proactive policies in delivering the desired application performance, which results in increased user satisfaction and productivity.
- Integrated with Easy VPN solution.
  - Hardware client has a separate interface context to which tunnel specific features can be applied. This integration of features & investment protection results in lower total cost of ownership.
  - Easy VPN Server has Dynamic Virtual Tunnel Interface to which tunnel specific features can be applied providing the flexibility to customize configuration and security based on site-specific needs.
- Virtual Route Forwarding (VRF) configured on the interface.
  - Multiple VRFs can be terminated in multiple interfaces to simplify large scale Service Provider and Enterprise MPLS deployments.

Hardware

Routers	• Cisco SB 100, 830, 850, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco IOS IPsec

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.4) Other Easy VPN Enhancements

Easy VPN Phase 5 includes the following enhancements to Easy VPN Server and Remote.

- Login banner to Easy VPN hardware clients—allows a banner message to be displayed after Web Based Tunnel Activation.
- Auto update for software clients—supports the new Auto Update feature in the Cisco VPN Client version 4.6 and above.
- Browser proxy configuration—allows the client's browser proxy configuration to be temporarily modified for the duration of the VPN session.

Benefits

- Login banner to Easy VPN hardware clients—enables regulatory compliance of notification and warnings via client side banner message. Also enhances manageability and ease of use.
- Auto update for software clients—eases upgrades and migration by automating software client updates.
- Browser proxy configuration—improves performance and usability by changing browser proxy settings on the fly to remove or modify settings that are invalid during a VPN session.

Hardware

Routers	• Cisco 830, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco IOS IPsec

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.5) Certificate Authority Key Rollover

A Certificate Authority (CA) manages certificate requests and issues certificates to participating network devices. Before any PKI operations can begin, the CA generates its own public key pair and creates a self signed CA certificate; thereafter the CA can sign certificate requests and begin peer enrolment for all the members of the PKI.

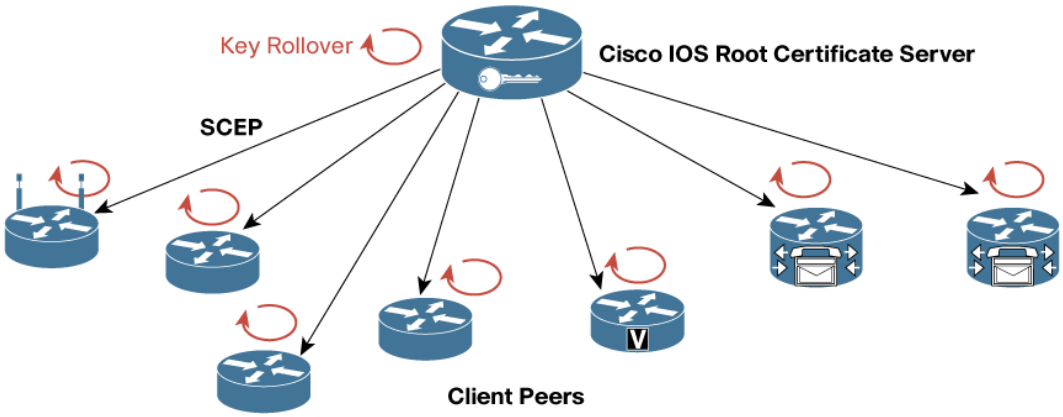
CAs, like their clients have certificates with expiration dates that need to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring, it must generate a new certificate and associated keypairs. This process, called rollover, allows for continuous operation of the network while clients and the certificate servers are switching from an expiring CA certificate to a new CA certificate.

Rollover relies on the PKI infrastructure requirements of trust relationships and synchronized clocks. The PKI trust relationships allow the new CA certificate to be authenticated and it allows rollover to be accomplished without the loss of security. Synchronized clocks allow rollover and the

flag-moment (the moment of time when the current CA certificate expires) to be coordinated throughout the network.

This new CA certificate before it is active is distributed as a shadow certificate. The shadow certificate is sent along with the currently active certificate with the flag moment transition time (time left for the currently active certificate to expire). When the flag-moment occurs, the shadow certificate immediately becomes the active certificate and the previously active CA certificate is deleted.

Figure 153. Certificate Authority Key Rollover



Benefits

- This feature allows the ability for a root or subordinate CA to rollover expiring CA certificates and keys throughout the entire PKI network.
- Prior to this feature, the system administrator would have to manually enroll all PKI devices in the network on expiry of the root CA certificate.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.6) Configurable Certificate Storage Location

In current versions of Cisco IOS Software, certificates are stored by default in the nvram of the router between reboots. Some Public Key Infrastructure (PKI) Endpoints may have an insufficient amount of nvram storage, and network administrators may wish to use alternate forms of local storage, such as a flash card. The user should be able to specify the type of local storage using configuration commands on the router.

A new PKI-specific CLI has been made available, allowing the user to specify the location where the certificates need to be stored. The choices for storage include all forms of local storage available on the router. The configuration setting takes effect when the running-configuration is saved and the router is reloaded. The default location will continue to be the nvram.

Benefits

Provides an alternate form of storage for certificates and improves manageability of the PKI by giving more options to the user.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.7) Network Address Translation Optimize Media Path for Session Initiation Protocol Traffic
This feature allows the creation of a shorter path for Session Initiation Protocol (SIP) media channels by distributing end-point IP addressing information via Session Descriptor Protocol (SDP) of SIP messages. This allows end points to communicate directly by using standard routing and eliminates the need for them to traverse through upstream NAT routers.

Figure 154. NAT Optimize Media Path for SIP Traffic

Benefits

- Media path can be shortened, thereby decreasing voice delay.
- Users can have more control on voice policy since media path will be closer to customer domain and not deep in the service provider cloud.

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3631, 3700, 3800, 7200, 7301, 7400, 800, SOHO 90, and UBR7200 Series Routers

Considerations

B1 and C1 (refer diagram above) should have unique IP Addresses and must have a route to each other for a direct media path to be established between them.

Product Management Contact: ask-stg-ios-pm@cisco.com

10.2.8) Zeroization
In the event where the security of a router is jeopardized, the information stored in the router can be used to the unauthorized person's advantage. Zeroization feature allows the end user to completely erase any trace of user data or binary code, including IP address, Cisco IOS Software, router configuration, or packetized data stored in any subsystem or memory device within the router. After the zeroization is activated, the router can be redeployed by downloading a new image.

Benefits

Allows users to clear the router of sensitive information to prevent unauthorized persons from using the equipment to their advantage.

Hardware

Routers	• Cisco 3200 Series Wireless and Mobile Routers

Additional Information: Cisco 3200 Series Wireless and Mobile Routers

Product Management Contact: Bradley Tips (btips@cisco.com)

10.3) Voice

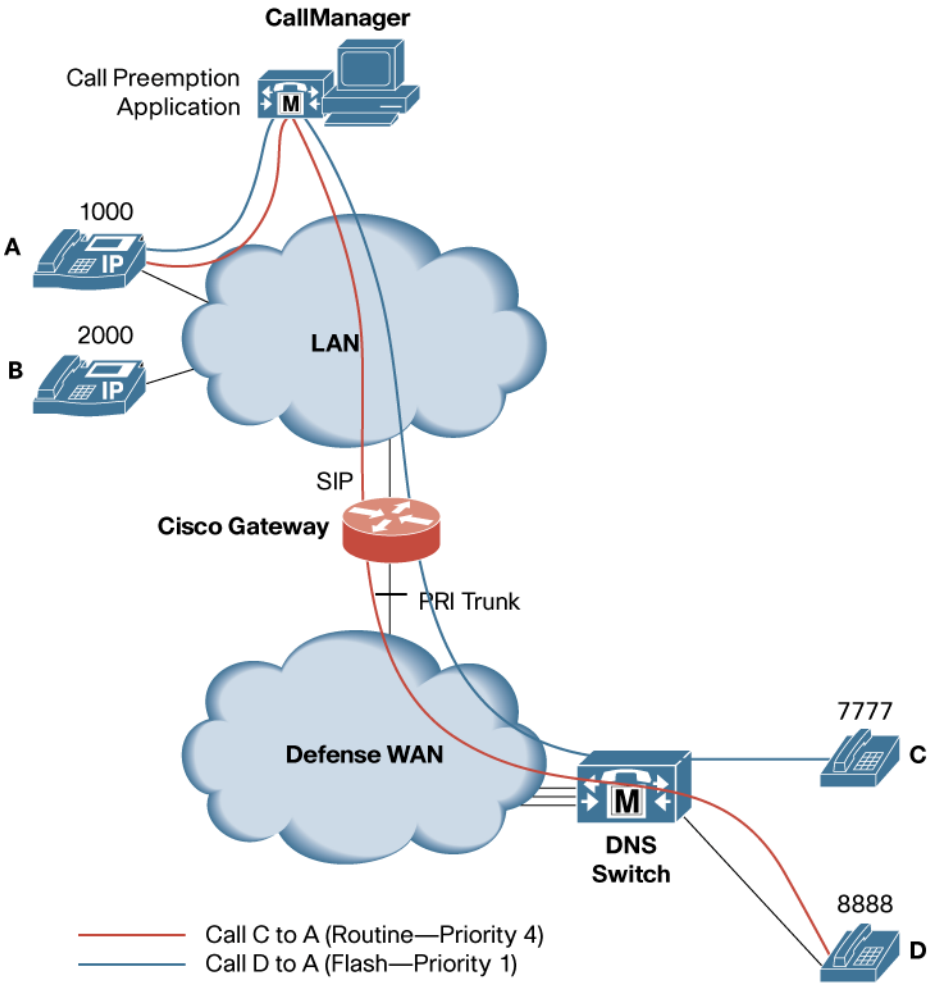
10.3.1) Session Initiation Protocol Support of Resource Priority Header and Reason Header

Session Initiation Protocol (SIP) Support of Resource Priority Header and Reason Header provides Cisco Call Manager the ability to interoperate with other Multi-level Precedence and Preemption (MLPP) capable Circuit Switched Networks connected through Cisco IOS Gateways for providing Call Preemption and Precedence Services.

Each MLPP enabled call has an associated priority level which the applications handling the emergencies and congestion would use to effectively determine which lower priority calls to preempt and dedicate their end system resources to high-priority communications.

The MLPP information in SIP is carried over “Resource-Priority” header as described in “draft-ietf-sip-resource-priority-03”. The header field marks a SIP request as desiring prioritized resource access depending on the Precedence level invoked/assigned to the call originator.

Figure 155. SIP Support of Resource Priority Header and Reason Header



Benefits

Allows high-ranking calls to preempt lower-ranking calls to assure communication to critical resources and personnel during an emergency.

Hardware

Routers	• Cisco 1700, 1800, 2800, 3700, 3800, and 7200VXR Series Routers

Additional Information: draft-ietf-sip-resource-priority-02.txt

Product Management Contact: Steve Levy (stlevy@cisco.com)

10.3.2) Session Initiation Protocol: User Agent MIB

This feature provides Management Information Base (MIB) enhancements for the management of Session Initiation Protocol (SIP) features added to the Cisco IOS Gateways from Cisco IOS Software Releases 12.2(15)T–12.3(8)T. This feature supports the MIB enhancements for following capabilities added to the Cisco IOS Gateway SIP support:

- SIP RFC 3261 signaling enhancements
- SIP Suspend/Resume support
- SIP Hold Timer support
- SIP GTD support
- SIP Bind command enhancements
- SIP Reason Header support
- SIP Registration enhancements
- SIP Call Admission Control support
- SIP VMXL Header Passing
- SIP Call Transfer enhancements

This will extend the CISCO-SIP-UA-MIB with Simple Network Management Protocol (SNMP). SNMP objects that provide configuration also provide counter support equivalent to the command line interface implemented by the IOS SIP Gateway.

Benefits

Provides network administrators with more MIB objects for better monitoring and management of SIP.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 7200VXR, and 7300 Series Routers

Additional Information: Cisco IOS Management Information Base Tool

Product Management Contact: Steve Levy (stlevy@cisco.com)

10.3.3) Configurable Hostname in Locally Generated Session Initiation Protocol Headers

This new feature enhancement allows the Session Initiation Protocol (SIP) gateway to use host or domain names in the “From”, “Call-ID” and “Remote-Party-ID” of the SIP headers when generating an outbound Voice over IP (VoIP) call.

Other SIP headers such as “Contact” and “Via” and the Session Description Protocol (SDP) are not affected by this new enhancement. Those headers will continue to have IP addresses even when this new feature is configured.

Benefits

Easier to identify the gateway by its host name instead of IP address.

Hardware

Routers	• Cisco 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200VXR Series Routers

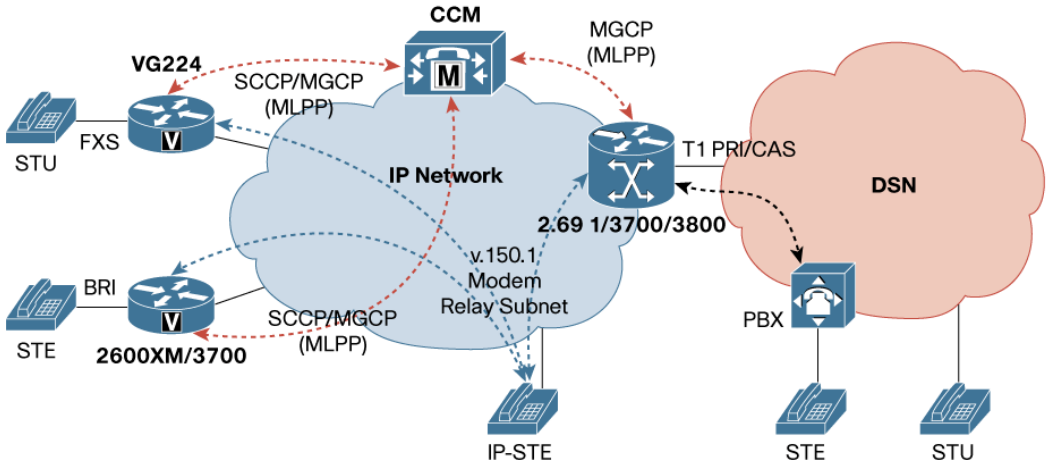
Additional Information: Session Initiation Protocol

Product Management Contact: Steve Levy (stlevy@cisco.com)

10.3.4) Secure Communication between IP-STE Endpoint and STE Endpoint

Secure Telephone Equipment (STE) and Secure Telephone Units (STUs) encrypt voice and data streams with government proprietary algorithms (Type-1 encryption). To provide support for the legacy STEs and STUs and next generation IP Secure Telephone Equipment (IP-STE), Cisco gateways must be able to support voice and data in secure and non-secure modes within the IP network and be able to pass calls within and also to and from government TDM voice networks. This feature supports secure communications between an IP-STE Endpoint and STE Endpoint where both endpoints are controlled by Cisco Call Manager by implementing a subset of v.150.1 modem relay protocol.

Figure 156. Secure Communication between IP-STE Endpoint and STE Endpoint



Secure communication between IP-STE Endpoint and line side STE Endpoint and secure communication between IP-STE Endpoint and trunk side STE Endpoint.

Benefits

Provides US Department of Defense IP Telephony call control, analog gateways and trunking gateways which support type-1 encryption with legacy TDM equipment.

Hardware

Routers	• Cisco VG224 Analog Phone Gateway (line side) • Cisco 2691XM Router (line side and trunk side), Cisco 3700 Series (line side and trunk side), and Cisco 3800 Series (trunk side)

Additional Information: Cisco IP Telephony Solutions Pass Deployment Tests for U.S. Department of Defense

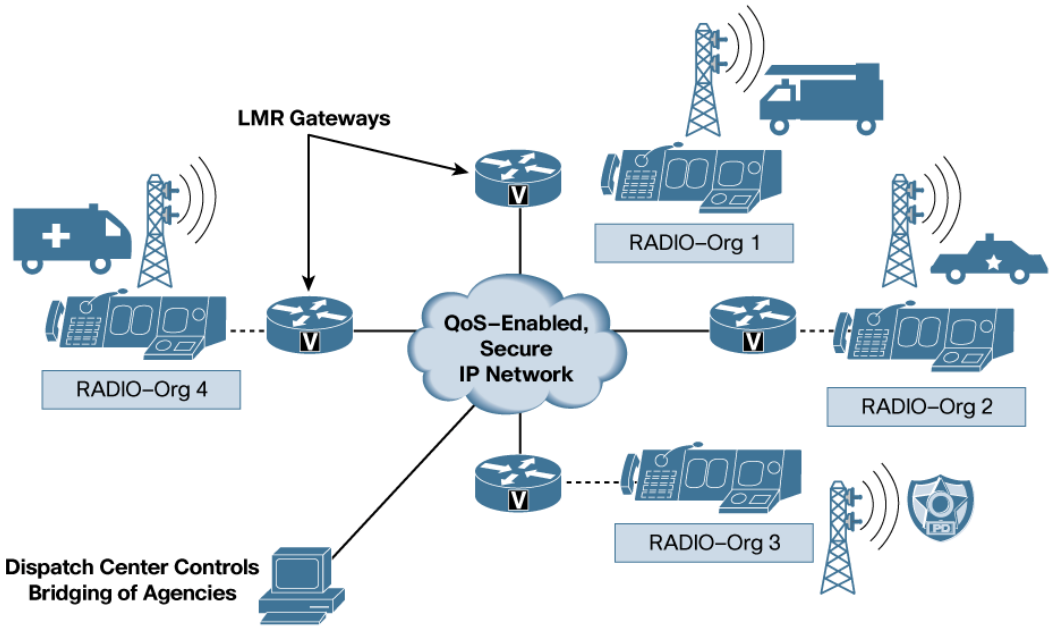
Product Management Contact: Jennifer Blatnik (jennyng@cisco.com)

10.3.5) Land Mobile Radio over IP Enhancement

Land Mobile Radio (LMR) System is a radio operation system that allows many end users who belong to same group to communicate with each other using handsets, which are preset to given radio frequencies. Due to the limitation of available radio frequency and the range of the radio, there are many zones within the country. The interoperability between groups within the same zone or between groups across the zones is problematic.

LMR over IP enhancement provides the solution to this interoperability problem by using Cisco router with LMR gateway functionality through E&M interface with modified signaling protocol and embedding E&M signaling in IP to extend beyond their traditional geographic limitations created by transmitter signal strength. This enables many new possibilities for LMR users, the most compelling of which is interoperability.

Figure 157. LMR over IP Enhancement



Benefits

- Provides LMR users interoperability between groups within the same zone and between groups across the zones.
- Allows LMR users to communicate beyond their radio range.
- Allows LMR traffic to be placed on a data network for remote monitoring by remote clients.
- Replaces leased lines used for backhaul of LMR traffic from remote base stations of a geographically dispersed radio network.

Hardware

Routers	• Cisco 2600, 2800, 3700, and 3800 Series Routers

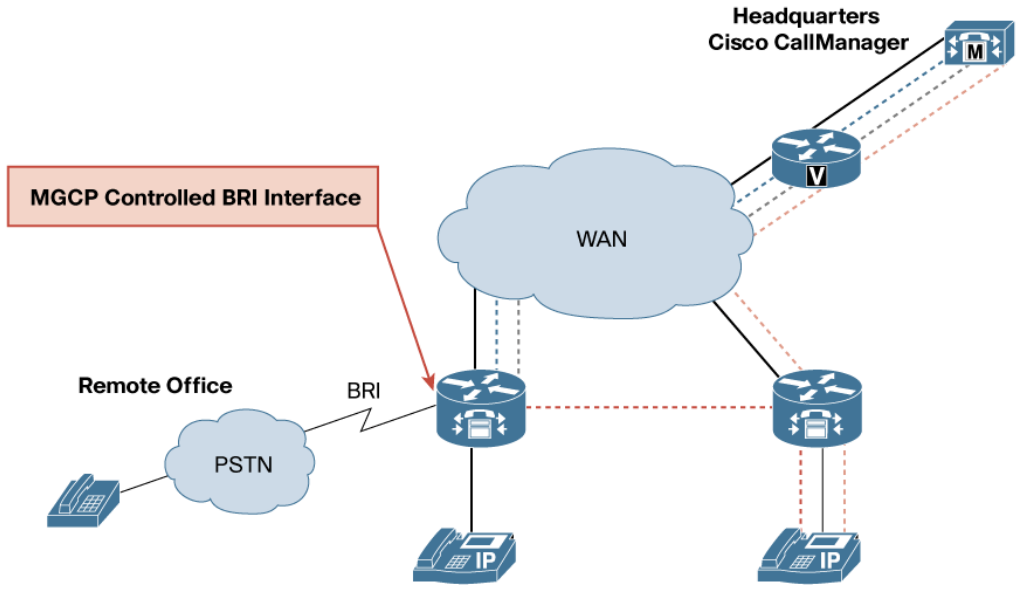
Additional Information: LMR over IP Overview

Product Management Contact: Henry Vinton (hvinton@cisco.com)

10.3.6) Media Gateway Control Protocol Controlled Backhaul of Basic Rate Interface Signaling
The feature enables the enterprise customers to connect their integrated services digital network private branch exchanges (ISDN PBXs) and Key Systems to Cisco ISDN Basic Rate Interface (BRI) network terminal (NT) or connect to Public Switched Telephone Network (PSTN) Class 4/5 switch through Cisco ISDN BRI TE (terminal equipment) interface and utilize external call control entity, such as Cisco CallManager or Cisco PGW 2200 Softswitch, to provide voice service between local and remote branch office.

Transporting signaling information from a branch-office MGCP gateway to a centralized media-gateway controller for processing is called backhaul. D-channel signal information is backhauled to an external call control entity through a TCP session. All Q.931 messages are passed through the TCP connection between the Cisco MGCP gateway and external call control entity. The MGCP gateway neither parses nor has any knowledge of the contents of those messages.

Figure 158. MGCP Controlled Backhaul of BRI Signaling



Benefits

- Centralized call-management architecture, enabling a high degree of network control.
- Short voice cut-through times.
- Ability for Cisco CallManager to take advantage of this feature.

Hardware

Routers	• Cisco 2600, 2800 3700, and 3800 Series Routers
Network Modules and Voice Interface Cards	• NM-HD, NM-HDV2, EVM and VIC2-2BRI

Considerations

- This feature requires Cisco CallManager 4.1(2) and later.
- The Cisco 2801 Router began supporting this feature in Release 12.3(14)T.

Additional Information:

- Cisco PGW 2200 Softswitch
- Configuring MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco CallManager

Product Management Contact: David Sauerhaft (dsauerha@cisco.com)

10.3.7) Skinny Client Control Protocol Analog (FXS) Ports Supplementary Feature Support for Cisco VG 224

Skinny Client Control Protocol (SCCP) Analog (FXS) Ports Supplementary Feature Support for Cisco VG224 adds supplementary call features to make SCCP a feature rich GW control call protocol in Cisco IOS Software for Cisco VG224 analog ports interoperating with both Cisco Call Manager (CCM) and Cisco Call Manager Express (CME) as call control. This new feature uses hook flash on an analog phone as a function key to support call transfer (blind or consultative), 3-way conference, answering waiting call, and toggling between two calls. This feature also supports feature access codes (FAC) for call pickup, group pickup, call forward (all, no answer, busy), cancel call forward, speed dial, and redial. Caller Identification (ID) and audible message waiting indicator are also supported on the Cisco VG224 SCCP analog ports. In addition, directed call park is available on Cisco VG224 SCCP analog ports interoperating with CME.

Figure 159. Cisco Call Manager SCCP Controlled Cisco VG224 FXS Analog Ports

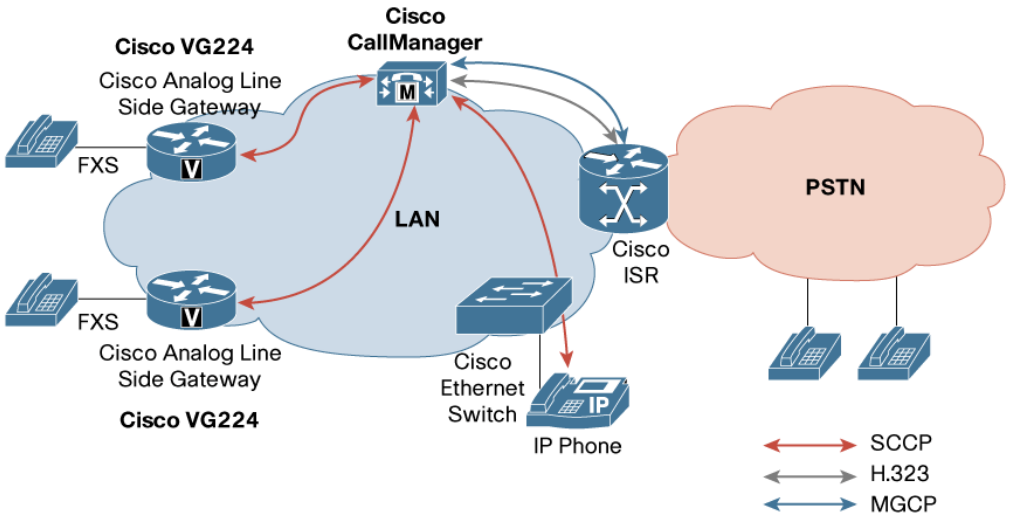
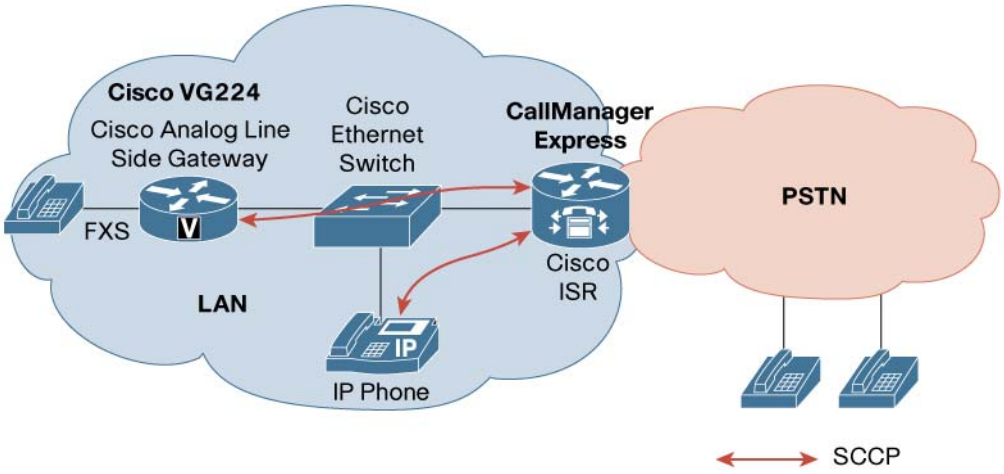


Figure 160. Cisco Call Manager Express SCCP Controlled Cisco VG224 FXS Analog Ports



Benefits

- Rich SCCP call features in Cisco IOS on Cisco VG224 for high density analog needs in CCM and CME IP Telephony environments.
- By adding SCCP analog endpoints into Cisco IOS Software, customers can now deploy a single Cisco IOS Software release for all of their Customer Premises Equipments (CPEs).
- Centralized software release management for all analog ports (H.323, MGCP, SCCP, SIP).

Hardware

Routers	• Cisco VG224 Analog Phone Gateway

Additional Information: Skinny Call Control Protocol

Product Management Contact: Jennifer Blatnik (jennyng@cisco.com)

10.3.8) E1 R2 Collect Call Blocking

E1 R2 Call Blocking provides two ways to block incoming collect calls-category-based and double answer. With category-based call blocking, collect calls will be blocked based on a specific category. For example, in Brazil, collect calls arrive with a category II-8, for which the Cisco access router will send B-7 as a response instead of an answer signal. This approach is only applicable when switches in the central office support category-based blocking.

For legacy switches that do not support category-based blocking, the double answer method is implemented to support the collect-call blocking. For an incoming collect call, the gateway will answer the call with a clearback after one second and re-answer the call after two seconds, causing the collect call to be dropped and normal calls to stay connected. This can be implemented as a command line interface (CLI) option for any country.

Currently, incoming collect call blocking over E1 R2 signaling is only available in Cisco AS5000 series Access Servers.

Benefits

Allows the operators to block incoming collect calls.

Hardware

Routers	• Cisco 1700, 2600XM, 2800, 3700, and 3800 Series Routers

Additional Information: E1 R2 Signaling Theory

Product Management Contact: Michael Wood (mikewood@cisco.com)

10.4) Cisco IOS Infrastructure

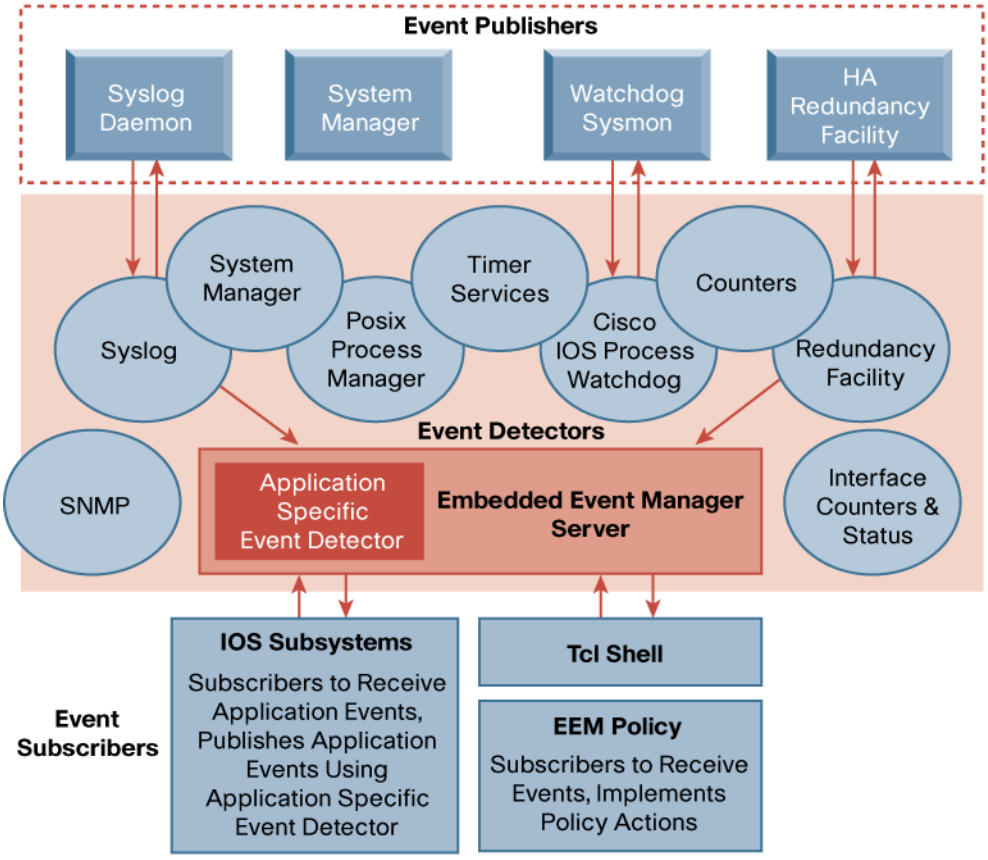
10.4.1) Cisco IOS Embedded Event Manager Version 2.2

Cisco IOS Embedded Event Manager (EEM) 2.2 extends the capabilities of EEM 2.1 and introduces two additional event detectors (EDs); the Object Tracking ED, and the Memory Thresholding ED. EEM is a distributed, scalable, and flexible approach to event detection and recovery offered directly in a Cisco IOS device.

Cisco IOS Embedded Event Manger 2.2 also includes the following two new features:

- **Cisco IOS Embedded Event Manager 2.2:** Track Event Detectors support.
- **First-Hop Redundancy Protocol (FHRP):** Enhanced Object Tracking integration with Embedded Event Manager.

Figure 161. EEM v2 Architecture



Benefits

- More flexibility with the two new event detectors.
- Provides in-box monitoring instead of having to deploy expensive external monitoring devices.

Hardware

Routers	• Cisco 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200VXR Series Routers

Additional Information: Embedded Event Manager Overview

Product Management Contact: Rohit Shrivastava (roshriva@cisco.com)

10.5) Access Technology

10.5.1) Authentication, Authorization, and Accounting CLI Stop Record Enhancement
In the current Cisco IOS Authentication, Authorization, and Accounting (AAA) implementation, when “aaa accounting send stop-record authentication failure” is configured, the router sends the accounting stop record for every call which failed during authentication and those stop records, without the corresponding start record, trigger the remote RADIUS Server to log error messages for each of these failures. This creates a heavy load on the RADIUS Server and renders the logs unusable.

This feature enables the sending of an accounting stop record only when an access-accept is received from the RADIUS Server so the router will not overload the RADIUS server with failed authentication error messages.

Benefits

- Reduces the number of accounting stop messages sent to the log server.
- Reduces the processing load on the Radius server.

Hardware

Routers	• Cisco 7200VXR Series and Cisco 7301 Router

Additional Information: Authentication, Authorization, and Accounting Overview

Product Management Contact: Micheal Lin (mhelin@cisco.com)

10.5.2) Calling Number Suppression for Layer 2 Tunnel Protocol Setup
This functionality allows suppression of all or some part of the calling number field in the Layer 2 Tunnel Protocol (L2TP) setup process via Radius Attribute functionality. This functionality will allow the user to “anonymyze” a calling number in a Call Detail Record (CDR) and allow more granular control for Automatic Number Identification applications. An example of this behavior would be if a call number like “1234567890” were to be sent, it will appear as “123456700x” so that the last three digits (or some other number of digits) would be suppressed.

The three methods of suppressing the calling number:

1. Pass through the complete number with no suppression. This is essential equivalent to having the current behavior without any additional functionality as the base or default case.
2. Suppress the entire number so that no part of it appears explicitly.

3. Suppress a select portion of the number so that part of it appears explicitly and part of it does not appear.

Benefits

Provides options for suppressing Calling Number ID in the router.

Hardware

Routers	• Cisco AS5000 and 7200VXR Series Routers

Additional Information: L2TP Tunnel Setup and Teardown

Product Management Contact: Sanjay Bhardwaj (sbhardwa@cisco.com)

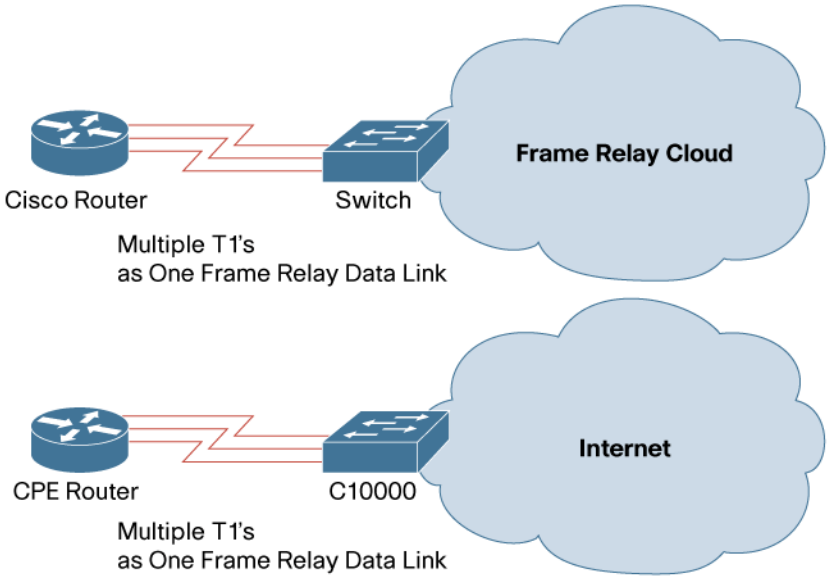
10.5.3) Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support

Multilink Frame Relay (MFR) means logically grouping one or more physical interfaces between two devices as one Frame Relay bundle interface.

FRF.16 specifies 4 different classes, namely A, B, C and D, to represent the trigger point of activating or deactivating a bundle, based on the number of bundle links being up or down. Class A will bring up the bundle as long as there is one bundle link being active, and will bring down the bundle interface when all bundle links go down. Class A is the default configuration. Class B works the opposite to class A and will bring down a bundle interface when any individual Frame Relay physical interface goes down. Class C is based on a configurable threshold value for the number of physical links which need to go down in order for the bundle to be declared down. Class D is implementation specific for a hardware vendor.

This feature adds Class B and C to the existing MFR Bandwidth Class support. Class D is not supported in this feature.

Figure 162. Multilink Frame Relay (FRF.16.1) Variable Bandwidth Class Support



Benefits

- Provides more flexibility in options for declaring MFR bundles to be active or inactive.
- Allows integration with Network Management applications to provide more options for control and management of MFR bundles.

Hardware

Routers	• Cisco 2600XM, 2800, 3700, 3800, and 7200VXR Series Routers

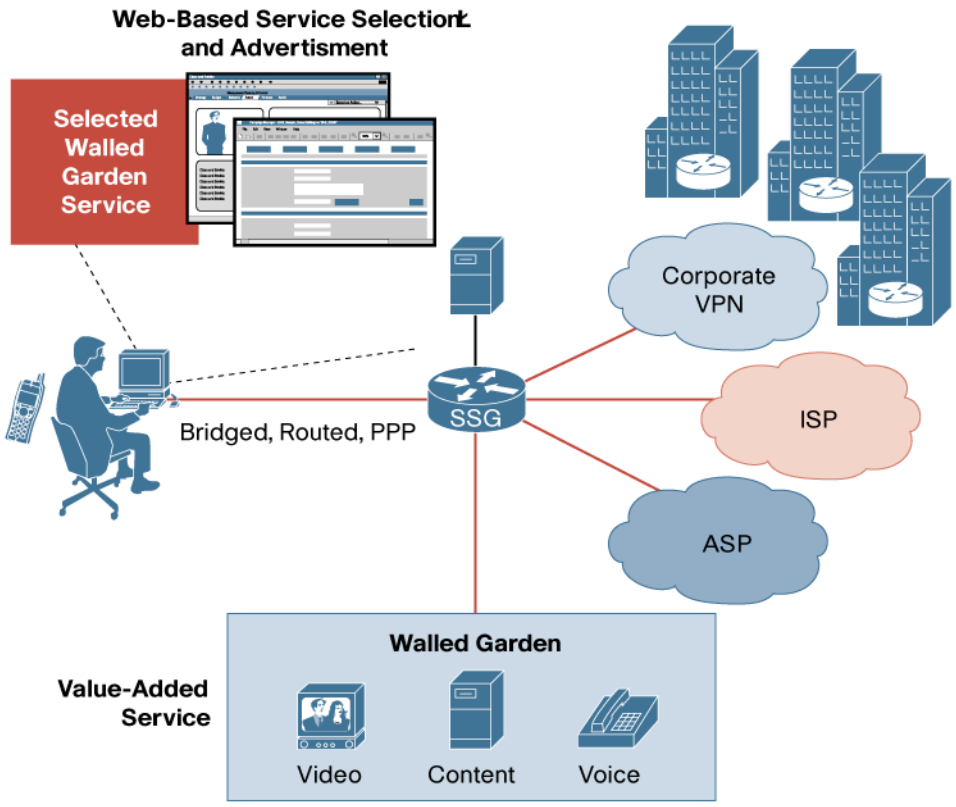
Additional Information: Multilink Frame Relay (FRF.16)

Product Management Contact: Sanjay Bhardwaj (sbhardwa@cisco.com)

10.5.4) Service Selection Gateway—Configurable Maximum Number of Allowed Subscribers Currently Service Selection Gateway (SSG) does not have a limit on the maximum number of host objects activated on the router. This can lead to resource exhaustion on the router. To prevent this, this enhancement introduces a configurable limit on the maximum number of hosts on the SSG. SSG will able to limit the number of host objects created on the box. SSG will also be able to limit the number of active sessions from different types of login methods.

If the maximum limit for users has already been reached on the SSG, it will reject the logon request. SSG will respond with an Access-Reject to SESM with the error code “57” to indicate that the host count has reached the maximum limit.

Figure 163. SSG—Configurable Maximum Number of Allowed Subscribers



Benefits

- Protects the SSG router against resource overuse.
    - Protects the SSG router from denial of service attack.

Hardware

Routers	• Cisco 2600XM, 2800, 3700, 3800, 7200VXR, 7300, 7400, and 7600 MWAM Series Routers

Additional Information: Service Selection Gateway

Product Management Contact: Murali Kolli (mkolli@cisco.com)

10.5.5) Service Selection Gateway Support of WISPr RADIUS Attributes
Service Selection Gateway (SSG) and its concepts of service selection, service delivery, and service billing are gaining popularity as service providers' move away from flat internet connectivity pipe to service oriented, revenue generating services. Several new customers are adapting this model in multiple markets such as Digital Subscriber Line (DSL), Public Wireless Local Area Network (PWLAN), General Packet Radio Service (GPRS) and Cable.

Wireless Hotspot providers want to customize the Web portal based on the location of the client device to better serve their customers. This customization is done by the Cisco Subscriber Edge Services Manager (SESM) during and after user login process of the client. In addition, Hotspot providers also like to model after the Wireless Internet Service Provider (WISP) Roaming recommendations by Wi-Fi alliance. There are several attributes defined by the WiFi alliance, but the current requirement is to support Location-id and Location-name attributes.

This new feature allows the Wireless Hotspot Providers to provide custom web portal by supporting the Location-id and Location-name Radius attributes. SSG will receive these attributes as part of the RADIUS Accounting-Start message from Access Point (AP). SSG then send them to SESM as part of Status Query response. The attributes will also be sent as part of the host and service accounting records as well. This feature will support both authenticated 802.1x users (EAPSIM authentication) and non-802.1x (open authentication) users as well.

Benefits

- Allows hotspot providers to offer relevant services based on client location.
- Potential new source of revenue for hotspot providers.

Hardware

Routers	• Cisco 2600XM, 2800, 3700, 3800, 7200VXR, 7300, 7400, and 7600 MWAM Series Routers

Additional Information:

- Cisco CNS Subscriber Edge Services Manager
- Wireless Internet Service Provider (WISP) Roaming recommendations by Wi-Fi alliance

Product Management Contact: Murali Kolli (mkolli@cisco.com)

10.5.6) Routed Bridge Encapsulation Client Side Encapsulation with Quality of Service
Due to new developments in the Digital Subscriber Line Access Multiplexer (DSLAM) market regarding DSLAMs with Gigabit backhaul instead of the more traditional Asynchronous Transfer Mode (ATM) backhaul, Point-to-Point Protocol (PPPoA) and RFC1483 routed encapsulation

normally used for higher end DSL services are no longer an option (unless in the rare case where termination of these services are supported in the DSLAM). Routing with bridged encapsulation allows the router to transmit and receive bridge encapsulated RFC1483 frames and route them to and from the internal network while allowing for Quality of Service (QoS) features to be applied as supported by the Cisco IOS Software feature sets.

Hardware

Routers	• Cisco 800, 1700, 1800, and 2800 Series Routers

Additional Information:

- Cisco IOS Software Release 12.3(8)YG, Product Bulletin No. 2681
- Routed Bridged Encapsulation

Product Management Contact:

- Geir Leirvik (gleirvik@cisco.com)
- Hari Harikrishnan (harikris@cisco.com)
- Sanjay Kumar (sanjayku@cisco.com)

10.5.7) Define Interface Policy-Map AV Pairs Authentication, Authorization, and Accounting
In current implementation, policies can only be applied via RADIUS during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment.

This feature supports dynamically applying policy maps on virtual circuit when triggered by specific events which will signal the Policy Server (Radius Server) to push policy onto specific VC. Pushing policy onto VC provides the ability to modify an existing quality of service (QoS) profile applied to a session while that session remains active. The current model requires the session to be dropped and re-authenticated (re-authentication is universally seen as unacceptable by service providers (SPs) due to the disruption of the session). This feature allows changing policy-map on the fly without affecting the PPP session itself.

Benefits

- Eliminates the need to “pre-provision” subscribers.
- Allow quality of service (QoS) policies to be transparently applied where and when required without the disruption of sessions re-authentication.
- Provide high degree of flexibility, smaller configuration files, and more efficient usage of queuing resources.

Hardware

Routers	• Cisco 7200VXR Series Routers

Additional Information: Define Interface Policy-Map AV Pairs AAA

Product Management Contact: Micheal Lin (mhelin@cisco.com)

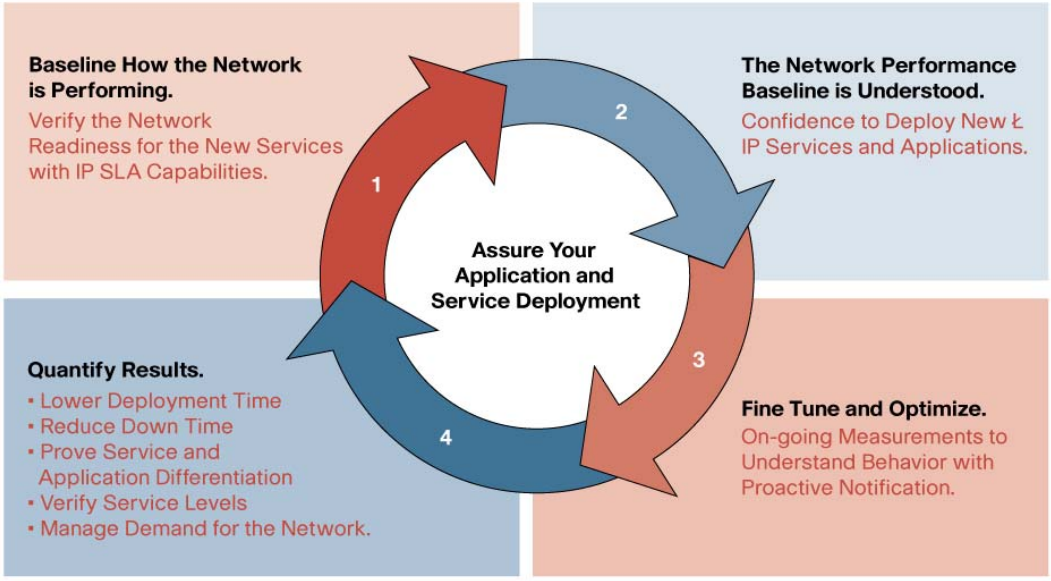
10.6) Management Instrumentation

10.6.1) Cisco IOS IP Service Level Agreements Random Scheduler

Customers demand guaranteed, reliable network services for business-critical applications and services. Cisco IOS IP Service Level Agreements (SLAs) is a capability embedded Cisco IOS Software, which allows Cisco customers to increase productivity, lower operational costs, and reduce the frequency of network outages. IP and SLAs are converging and extending IP performance monitoring to be application aware and are critical for new IP network applications such as Voice over IP (VoIP), Audio and Video, VPN and other business critical applications. Cisco IOS IP SLAs measure end-to-end and can perform network assessments, verify Quality of Service (QoS) and ease deployment of new services, and assist administrators with network troubleshooting. Cisco IOS IP SLAs use unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

As networks grow, the number of Cisco IOS IP SLAs will grow rapidly. Cisco IOS IP SLAs group scheduler has been developed to activate a large number of operations through command line interface or Simple Network Management Protocol at deterministic time over the specified scheduler period. To continuously meet customer's demand, Cisco IOS IP SLAs group scheduler has been enhanced to activate randomly over the specified schedule period. By introducing randomness, Cisco IOS IP SLAs report network performance metrics with enhanced precision.

Figure 164. Cisco IOS IP SLAs Random Scheduler



Benefits

Allows IP SLA to randomly schedule measurements allowing more precision.

Hardware

Routers	• Cisco 800, 1700, 1800, 2800, 3700, 3800, and 7200VXR Series, and Cisco 7301 Router

Additional Information:

- Cisco IOS IP SLAs
- Cisco IOS IP SLAs Documentation

Product Management Contact: Tom Zingale (tomz@cisco.com)

10.6.2) NetFlow Top Talker CLI—Phase 2

Understanding who is using the network and for how long, what protocols and applications are being utilized and where the network data is flowing is a necessity for today's IP network managers. NetFlow data can be used for a variety of purposes, including network management and planning, user and security monitoring, protocol and application monitoring, enterprise accounting, and departmental charge backs, Internet service provider (ISP) billing, data warehousing, and data mining for marketing purposes. NetFlow CLI is used extensively for troubleshooting and understanding network behavior. NetFlow Top Talker CLI—phase 2 provides improved and additional NetFlow features for security monitoring and enhances the first phase of the NetFlow Top Talker show command. For example the new Top talkers functionality can characterize the largest number of packets sent to a destination IP address for a specific application port.

- The new NetFlow show commands help network administrators identify and classify security issues using the command line.
- The command will be useful for troubleshooting and understanding network behavior.

Examples for NetFlow Top Talkers:

- Show the top 10 protocols currently flowing through the device.
- Show the 10 IP addresses which are sending the most packets.
- Show the 5 destination addresses to which the most traffic is routed from the 10.0.0.1/24 prefix.
- Show the top 25 AS's receiving UDP traffic.
- Show the 50 VLAN's which are sending the least bytes.
- Show the top 20 sources of 1-packet flows.

Benefits

- Security-Able to view the list of top talkers to see if traffic patterns consistent with a denial of service (DoS) attack are present in the network.
- Load balancing-able to identify the most heavily used parts of the system and move network traffic over to less-used parts of the system.
- Traffic analysis-consulting the data retrieved by Top Talker CLI.
- Talkers feature can assist in general traffic study and planning for the network.

Hardware

Routers	• Cisco 800, 1700, 1800, 2800, 3700, 3800, and 7200VXR Series, and Cisco 7301 Router

Additional Information: Cisco IOS NetFlow

Product Management Contact: Tom Zingale (tomz@cisco.com)

10.6.3) Advanced Encryption Standard and Triple-Data Encryption Standard Algorithm Encryption Support for SNMPv3

The Advanced Encryption Standard (AES) and Triple-Data Encryption Algorithm (3DES) encryption support for SNMPv3 feature enhances the encryption capabilities of SNMP version 3. The AES and 3-DES encryption support for SNMPv3 feature add AES 128-bit encryption in compliance with RFC 3826. RFC 3826 extensions have been included in the SNMP-USM-AES-MIB. In addition, Cisco-

specific extensions to support 3-DES and AES 192-bit and 256-bit encryption have been added to the CISCO-SNMP-USM-MIB.

Benefits

- Provides stronger encryption technology to SNMPv3.
- More encryption options to choose from based on required level of security and router performance.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, 7300, and 7400 Series Routers

Additional Information:

- Cisco IOS Simple Network Management Protocol version 3
- RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

Product Management Contact: Michael Cheung (cheung@cisco.com)

10.7) Quality of Service

10.7.1) BitTorrent Packet Description Language Modules Native Implementation

Add supports for BitTorrent application recognition in native Cisco IOS Software. Previously, supports for BitTorrent application recognition was through the BitTorrent Packet Description Language Modules (PDLM), which need to be downloaded and installed into Cisco IOS Software. BitTorrent PDLM is an application signature used by Network Based Application Recognition (NBAR) to identity BitTorrent traffic.

BitTorrent is a popular Peer-to-Peer (P2P) software application that facilitates audio, video, and image file-sharing between clients. The BitTorrent application provides complete distributed file-searching and file-sharing with other peers running the BitTorrent application.

Benefits

- No need to download and install the BitTorrent PDLM.
- Added more NBAR application recognition into native Cisco IOS Software.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, and 7301 Series Routers

Additional Information:

- NBAR Packet Description Language Modules
- BitTorrent PDLM ReadMe

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

10.7.2) Citrix ICA Published Applications Native Implementation

Cisco IOS Network Based Application Recognition (NBAR) can classify Citrix Independent Computing Architecture (ICA) traffic and perform subport classification of Citrix traffic based on Citrix published applications. NBAR can monitor Citrix ICA client requests for a published application destined to a Citrix ICA Master browser.

Previous supports for Citrix application recognition was through the Citrix Packet Description Language Modules (PDLM), which need to be downloaded and installed into Cisco IOS Software so Network Based Application Recognition (NBAR) can recognize Citrix application traffic. This feature adds Support for Citrix ICA Published application recognition in native Cisco IOS Software.

Benefits

- Eliminates the need to download and install the Citrix PDLM onto the router.
- Adds more NBAR application recognition into native Cisco IOS Software.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, and 7300 Series Routers

Additional Information:

NBAR Packet Description Language Modules

Classification of Citrix ICA Traffic by Application Name

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

10.7.3) Multiple Matches Per Port

Cisco IOS Network Based Application Recognition (NBAR) has the ability to sub-classify an application based on the value of a specified field in the packet. It is referred to as “protocol parameters”. A good example would be classifying an HTTP stream based on the URL (match protocol http url “cisco.com”). The use of parameters is only available for the writers of Packet Description Language Modules (PDLMs). This new feature extends the “protocol parameters” to the User Defined Custom (UDC) protocol interface to provide NBAR the ability to distinguish between different values of an attribute within the traffic stream of a particular application on a TCP or UDP port. Once different protocol parameters are matched, the network administrators can impose different traffic or security profiles to different streams within the custom application.

The current UDC infrastructure creates a PDLM based on the input from the CLI. For example:

```
ip nbar custom FOO 125 hex 0x15 tcp range 5001 5005
```

The above example creates a protocol named “FOO”. A packet with a TCP port of 5001, 5002, 5003, 5004, or 5005, which contains a hex value of 15 at 125 bytes into the L5—L7 payload, is considered a match. The rest of the packets of that session will be classified as FOO.

The new enhancement allows the user to give a name to the field and specify that the value is variable. The user can then enter the desired value of the field when creating match criteria in a class-map. For example:

```
ip nbar custom FOO field scid 125 variable 1 tcp range 5001 5005
class-map active-craft       match protocol FOO scid 0x15
       match protocol FOO scid 0x21
       match protocol FOO scid 0x27
class-map passive-craft
       match protocol FOO scid 0x11
       match protocol FOO scid 0x22
```

```
match protocol FOO scid 0x25
```

This will allow the user to enter up to 24 different field values and group them into different traffic profiles depending on the value. In the above example, packet steams within the TCP port range of 5001–5005 with scid values of hex 15, 21, and 27 will fall into the active-craft class and those with scid values of hex 11, 22, and 25 will fall into the passive-craft class.

Benefits

- Provides NBAR with more powerful and flexible application matching.
- Provides the network administrators the ability to apply different policies within an application traffic stream.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, and 7300 Series Routers

Considerations

The extra complexity of a custom protocol definition will cause a slight increase in the amount of memory temporarily allocated and a little extra text parsing.

Additional Information: NBAR and Distributed NBAR

Product Management Contact: Tim McSweeney (timcswee@cisco.com)

10.7.4) Modular Quality of Service CLI Policy Map Support on Configured Virtual Circuit Range Asynchronous Transfer Mode

Cisco routers currently support Modular Quality-of-service Command-line-interface (MQC) policy-maps on virtual circuit (VC), but each Asynchronous Transfer Mode (ATM) VC has to be manually configured for MQC policy, which requires lot of configuration effort. This feature makes the configuration simpler, by allowing the network administrators to configure the policy on a range of ATM VCs.

Benefits

Simplified MQC policy-maps configuration on multiple ATM VCs.

Hardware

Routers	• Cisco 7200, and 7301 Series Routers

Additional Information: Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4

Product Management Contact: Amanda Holdan (aholdan@cisco.com)

10.8) IP Multicast

10.8.1) Multicast Listener Discovery Group Limits

This feature enhancement introduces an access control mechanism into Multicast Listener Discovery (MLD) where the number of groups/channels accessed at the receiver end is limited and controlled. A high rate of MLD messages sent to a router can pose a denial of service (DoS) attack scenario because these messages are handled at the process level. This new enhancement reduces the vulnerability of a router to DoS attacks with MLD packets at both a global and interface level.

When the limit is reached, incoming MLD reports for new groups/sources will be dropped and hosts will not receive traffic for those joins.

Benefits

- Limiting the vulnerability of a router to denial of service attacks with MLD packets.
- Ability to control and limit the number of MLD messages received by a router.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, and 7300 Series Routers

Considerations

In Any Source Multicast (ASM), a group is counted towards the limits. In Source Specific Multicast (SSM), a channel or a (S,G) is counted as an entry.

Additional Information: Cisco IOS IPv6 Multicast Introduction

Product Management Contact: Gurvinder Singh (g_singh@cisco.com)

10.8.2) IPv6 Boot Strap Router—Ability to Configure Rendezvous Point Mapping
This new feature allows Cisco IOS IPv6 BSR routers to directly announce scope-to-rendezvous point (RP) mappings instead of learning them from candidate-RP messages. Announcing RP mappings statically from the Boot Strap Router (BSR) without having to listen to candidate-RP messages is useful in many situations:

- If the candidate-RP(s) itself does not support BSR.
- If the candidate-RP(s) is positioned outside the enterprise's BSR domain (limited by "ipv6 pim bsr border"), then it can not be learned because the messages from the remote BSR are filtered. Instead the candidate-RP can be learned by "administratively importing" it using the known remote RP address on the local candidate BSR routers.
- If the candidate-RP address never changes because there is only a single RP or the group range uses an Anycast RP, it may be less complex to simply configure the RP address announcement statically on the candidate BSRs.
- If the RP address is a virtual RP address (ie: with Bidir-PIM), it can not even be learned by the BSR from a candidate-RP itself. Instead, it must be configured as an announced-RP on the candidate BSRs.

Benefits

Provides users the flexibility to have BSR advertise scope-to-RP mappings without having to passively listen to candidate-RP messages or require candidate-RP's to support BSR natively.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, and 7300 Series Routers

Additional Information: Cisco IOS IPv6 Multicast Introduction

Product Management Contact: Gurvinder Singh (g_singh@cisco.com)

10.8.3) IPv6 Source Specific Multicast Mapping

Source Specific Multicast (SSM) Mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for Multicast Listener Discovery version 1 (MLDv1) receivers. This feature allows rapid deployment of IPv6 SSM with hosts that are (at least currently) incapable to provide MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application.

Benefits

- Reduces network complexity by eliminating the need for Rendezvous Points. For example, static RP, Auto-RP, Bootstrap Router (BSR) and Anycast-RP are no longer needed. Resulting from this, a higher level of reliability typically can be achieved purely by means of SSM being 90% less prone to misconfigurations.
- Protects against denial of service attacks by inhibiting unwanted sources. Eliminates the need for IP Multicast address management through address reuse. Provided the IP address of every source in the network does not overlap, each SSM (S,G) channel for a given group, G, is guaranteed to represent a unique flow.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, and 7300 Series Routers

Additional Information: Source Specific Multicast (SSM) Mapping

Product Management Contact: Gurvinder Singh (g_singh@cisco.com)

10.8.4) Multicast Source Discovery Protocol MD5 Password Authentication

This new feature enhancement adds support for MD5 signature protection for Multicast Source Discovery Protocol (MSDP) TCP connections in accordance with RFC2385.

Benefits

- Provides MD5 signature protection to MSDP.
- MSDP compliance with RFC2385.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, and 7300 Series Routers

Additional Information: Configuring Multicast Source Discovery Protocol

Product Management Contact: Gurvinder Singh (g_singh@cisco.com)

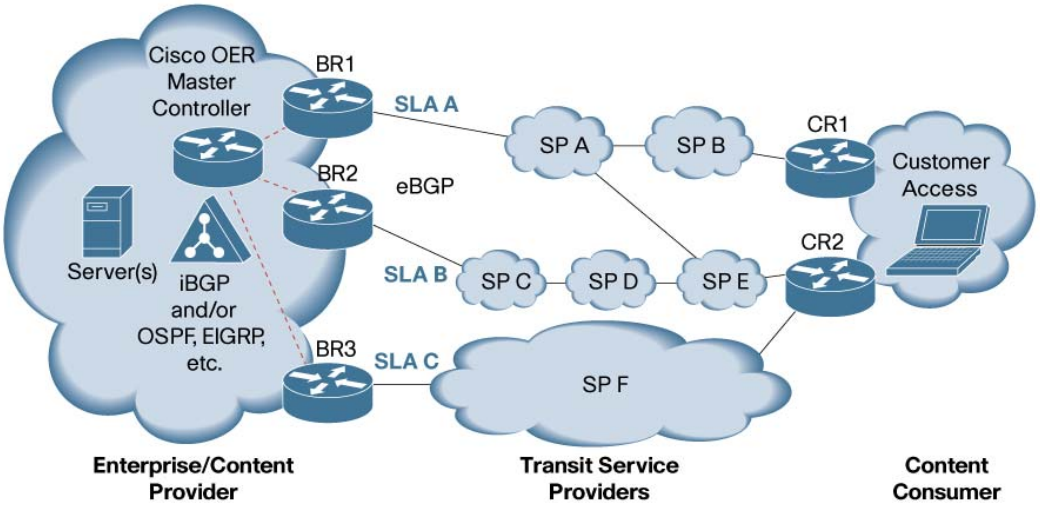
10.9) IP Routing

10.9.1) Application-Aware Routing: Policy Based Routing

This new feature allows Optimized Edge Routing (OER) and Policy Based Routing (PBR) integration to support outbound optimization for specific applications and other fields besides destination IP address such as IP prefix length, protocol, and port number(s).

PBR integration allows routing to be based on portions of the packet other than the destination IP address. PBR only specifies per-hop behavior. No PBR information is redistributed from one hop to the next as in a routing protocol. This is done by first creating a route-map with match clauses that identify a packet using access-lists. Then adding set clauses to the route-map which identify the next-hop IP address and/or outgoing interface.

Figure 165. Application-Aware Routing: PBR



Benefits

Support outbound optimization for specific applications with additional routable fields such as IP prefix length, protocol, and port number(s).

Hardware

Routers	• Cisco 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, 7301 NPE, and 7400 Series Routers

Additional Information:

- Cisco Optimized Edge Routing
- Policy Based Routing White Paper

Product Management Contact: Pepe Garcia (pepe@cisco.com)

10.9.2) TCP Show Extension

The TCP show command line interface (CLI) by default uses hostname in its output. This involves a Domain Name Server (DNS) lookup and is hence often slow. There is also limitation on the size of the hostname string that can be displayed on the output. This new feature enhancement addresses both of these issues by using IP address instead of hostname. This enhancement also displays the table identification associated with a connection for routing systems with multiple routing tables to help in debugging and informative purposes.

Benefits

- Allows the TCP show CLI to display IP addresses instead of hostname.
- Improves TCP show CLI perform by not having to perform DNS lookup.
- Helps in debugging and providing more information.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, 7300, and 7400 Series Routers

Product Management Contact: Pepe Garcia (pepe@cisco.com)

10.9.3) Internet Control Message Protocol Unreachable Rate Limiting User Feedback
Cisco IOS Software is able to rate-limit the generation of Internet Control Message Protocol (ICMP) unreachable messages. By default, the router will not send ICMP unreachable messages more often than once every 1/2 a second. Currently, there is no mechanism to easily see how many ICMP messages have been rate-limited per interface.

This new enhancement will provide counter information on the number of ICMP messages rate limited. During periods of excessive rate-limiting, the router will also display and log a warning message, since this could indicate a Denial of Service attack against the router.

Benefits

Provides warning messages and statistics on the number of ICMP messages that have been rate-limited in an event of a Denial of Service Attack against the router.

Hardware

Routers	• Cisco 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200VXR Series, and Cisco 7301 Router

Product Management Contact: Chetan Khetani (cpk@cisco.com)

10.9.4) “Clear IP Traffic” CLI
In current Cisco IOS Software implementation, there is no way to clear the traffic statistics shown in “show ip traffic” command except reloading the router. These statistics only show the accumulative counters since the router started up, but there is no way to flexibly clear and monitor the counters as the user desires. This feature introduces the “clear ip traffic” command to clear the statistics in the “show ip traffic” command without having to reload the router.

Benefits

- Ability to clear the “show ip traffic” command statistics without having to reload the router.
- Make troubleshooting easier with the ability to clear the statistics.

Hardware

Routers	• Cisco 1700, 1800, 2600XM, 2800, 3700, 3800, and 7200VXR Series, and Cisco 7301 Router

Product Management Contact: Chetan Khetani (cpk@cisco.com)

10.10) IP Services

10.10.1) IPv6 Access Control List Extensions for Mobile IPv6
Several new Internet Control Message Protocol version 6 (ICMPv6) message types have been defined in RFC3775, Mobility Support in IPv6. In addition, the RFC also defines new IPv6 extension headers, the IPv6 Mobility Header, and also a variation on the Routing Header, namely the Type 2 Routing Header.

This new feature allows IPv6 access control list (ACL) entries to match Mobile IPv6 (MIPv6) specific ICMPv6 messages and packets containing the new and modified IPv6 extension headers. In addition, a new command is introduced to control the generation of ICMPv6 unreachable messages.

Benefits

Allow IPv6 access control list entries to match the new ICMPv6 message types and IPv6 extension headers.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, 7300, and 7400 Series Routers

Additional Information: RFC3775—Mobility Support in IPv6

Product Management Contact: Patrick Grossetete (pgrosset@cisco.com)

10.10.2) IPv6 Default Router Preference
The Router Advertisement (RA) mechanism (RFC2461), amongst other things, informs hosts about the default routers on a link. Hosts maintain a default router list from which one is selected for traffic to remote destinations. The selection for a destination is then cached. RA allows round-robin, or "always the same: selection mechanisms."

This is simple and works well in most cases. But there are times where it is suboptimal when some form of traffic engineering is desired. For instance, when two routers on a link provide equivalent, but not equal-cost routing, policy may dictate that one is preferred. In current implementation, there is no mechanism to inform the hosts to prefer one default router over the others.

IPv6 Default Router Preference (DRP) can provide preference metric for default routers. IPv6 DRP is Cisco IOS implementation of the draft-ietf-ipv6-router-selection-07.txt enabling a network manager to assign a priority to a router. This new feature introduces a new command under the interface configuration:

```
ipv6 nd router-preference {High|Medium|Low}
```

The "low" keyword indicates the least preferred, while the "High" keyword indicates the most preferred default router. If this command is not applied, RAs are sent with the default preference of "Medium".

Benefits

- Allow end devices to select a more optimal default router to remote destinations.
- Reduces the number of redirect messages sent from the non-optimal default routers.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200VXR, and 7300 Series Routers

Additional Information:

- draft-ietf-ipv6-router-selection-07.txt
- RFC 2461

Product Management Contact: Patrick Grossetete (pgrosset@cisco.com)

10.10.3) Foreign Agent Local Route Optimization

In Mobile IP networks, endpoint devices sending traffic through a single foreign agent must traverse through a home agent router. Often the home agent is in a different geographic region. Sending the traffic through a home agent may cause latency and unnecessary traffic across a mobile IP network.

The advantage of foreign agent local route optimization is that the Internet traffic between end devices attached to a foreign agent now can communicate with each other directly using the foreign agent router. Because the foreign agent router is further out the in network, fewer network delays are experienced and traffic is optimized across the mobile IP network.

Benefits

- Reduce unnecessary traffic across a mobile IP network.
- Reduce latency.
- Optimized traffic path between two mobile endpoints.

Hardware

Routers	• Cisco 3200 Series Wireless and Mobile Routers

Additional Information: Cisco 3200 Series Wireless and Mobile Routers

Product Management Contact: Bradley Tips (btips@cisco.com)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

c25-409474-03 02/09