Cisco IOS Software Release 15.1(3)T New Features and Hardware Support

Introduction

Cisco IOS® Software Release 15 M&T family provides a more consistent user experience resulting from the evolution of Cisco's software development model. This new model accelerates the sharing of features and applications and enables Cisco® Borderless Network Services. Cisco Integrated Services Routers (ISR) are the first platforms to take advantage of these new capabilities.

Cisco IOS Software Release 15 M&T provides:

- Faster delivery of new feature releases
- Broader feature consistency across major releases
- Predictable new feature release and rebuild schedules
- Proactive individual release support lifecycle policies
- Easier software selection, deployment, and migration

Cisco IOS Software Release 15.1(3)T is the third in a series of individual Cisco IOS Software 15.1T releases. This release offers features from Releases 15.1(1)T and 15.1(2)T, and it introduces new technology and hardware support.

Cisco IOS Software Release 15.1(3)T includes the following important capabilities:

- Selective Packet Discard (SPD) for IPv6 provides a congestion control mechanism for the interface input queues and additional queuing capacity for control plane traffic.
- Performance Monitor provides real-time metrics like packet loss and network jitter for rich-media streams and round trip times for TCP traffic.
- Mediatrace provides automatic path discovery of traffic streams across a network. While discovering both Layer 2 and 3 devices along the path, Mediatrace provides hop by hop information about the state of the media flow.
- IPv6 Rapid Deployment (6rd) allows incremental deployment of IPv6 unicast through existing IPv4 service provider networks.
- Cisco IOS SSLVPN Smart Tunnels Support lets you identify the applications to which you want to grant smart tunnel access. Specify the path to the application and the SHA-1 hash of its checksum to check before granting access.
- Cisco Advanced Foreign Exchange Station (FXS) Analog Gateway and Skinny Client Control Protocol (SCCP) over Transport Layer Security (TLS) with Cisco Unified Communications Manager give you granular troubleshooting capabilities during initial network provisioning.

Cisco IOS Software Release 15.1(3)T is a standard maintenance release. Refer to the release notes for Cisco IOS Software Release 15.1(3)T at http://www.cisco.com/en/US/docs/ios/15_1/release/notes/15_1m_and_t.html for specific hardware platform support.

The remainder of this document discusses the main features of Cisco IOS Software Release 15.1(3)T.

RSVP Ingress CAC (Connection Admission Control)

With load balancing, inbound traffic for the Resource Reservation Protocol (RSVP) agent is not guaranteed to use same WAN link as outbound traffic. This traffic can overrun the priority queue because reservations are currently made only on outgoing CE (Customer Edge) interfaces, in the direction of the Real-Time Protocol (RTP) stream. The Ingress CAC mechanism improves the solution by performing CAC on the ingress interface on the next hop.

Benefits

- RSVP can now work with asymmetric media paths (asymmetric routing cases).
- RSVP can now meet the needs of headquarters–to–branch-office deployment scenarios in which bandwidth profiles are not identical.
- RSVP is now aligned with service provider deployments.

Hardware

- **Routers:** Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 3900 Series

Product Management Contact

Karthik Dakshinamoorthy: karthikd@cisco.com

IP-MIB and IP-FORWARD-MIB for IPv6

IP-MIB and IP-FORWARD-MIB support provide core embedded management capability to systems running IPv6. Both device-level and interface-level IPv6 and ICMPv6 counters are provided. Access to the routing table is available as well. With this capability, network operators can use standard Simple Network Management Protocol (SNMP) to gather and retrieve data related to core IPv6 operations. The current implementation allows the retrieval of IPv6-related information only.

Benefits

- MIB statistics are provided for core IPv6 operations, and separate interface counters are included for IPv6 traffic.
- The use of standard SNMP provides easy access and facilitates integration with current SNMP-based network management systems.

For More Information

- http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&submitClicked=true&mibName=IP-FORWARD-MIB#contents
- http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&submitClicked=true&mibName=IP-MIB#contents

Product Management Contact

Benoit Lourdelet: blourdel@cisco.com

Per-Interface IPv6 Neighbor Discovery Cache Limit

The number of entries in the IPv6 Neighbor Discovery cache can be limited on an interface basis. After the limit is reached, no new entries are allowed. The per-interface Neighbor Discovery cache limit function can be used to prevent any particular host attached to an interface from overloading the neighbor discovery cache, whether intentionally or unintentionally.

Benefits

Denial-of-Service (DoS) attacks coming from Neighbor Cache overflow are prevented.

Product Management Contact

Benoit Lourdelet: blourdel@cisco.com

Selective Packet Discard for IPv6

Selective Packet Discard (SPD) for IPv6 provides a congestion control mechanism for the interface input queues and additional queuing capacity for control plane traffic. The SPD mechanism manages the process-level input queues on the routing processor. SPD gives priority to routing protocol packets and other important traffic-control Layer 2 keepalives during periods of process level queue congestion.

Benefits

- Routing processor–critical resources are kept free for critical traffic such as routing protocol or Layer 2 keepalives.
- Priority is given to most important packets on interface input queues.

Product Management Contact

Benoit Lourdelet: blourdel@cisco.com

Legacy QoS Command Deprecation: Hidden Commands

For years, Cisco IOS Software has supported the coexistence of dual command-line interfaces (CLIs) for configuring Quality of Service (QoS) on its platforms:

- Modular QoS CLI (MQC) is the CLI used by the vast majority of users, because it offers advanced capabilities such as configuration of traffic policing at three levels of policy-map hierarchy.
- The existing, older CLI offers only a reduced set of the functions that MQC offers, and Cisco has always maintained both CLIs at parity to allow early users to easily upgrade their Cisco IOS Software.
- Because of the low use of the older CLI, and given that MQC is recognized as the most complete CLI for configuration of QoS on Cisco devices, Cisco has decided to hide the older CLI commands for QoS.

Benefits

The older commands will still be accessible, though they will no longer be documented, allowing those customers still using the older CLI to smoothly transition to the MQC, which offers richer capabilities.

For More Information

Product bulletin: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/product_bulletin_c25-580832.html

Product Management Contact

Francois-Xavier Mateo: fmateo@cisco.com

Bandwidth Configuration on Logical Interfaces

This release introduces a new command on the routers:

bandwidth qos-reference *bandwidth-amount*

The **bandwidth qos-reference** command is used to configure the bandwidth on a logical interface, such as a tunnel interface. With this command, network operators can specify the amount of bandwidth to allocate to a logical interface.

Benefits

This release introduces a new command required by customers who need to specify the bandwidth on the logical interface.

Product Management Contact

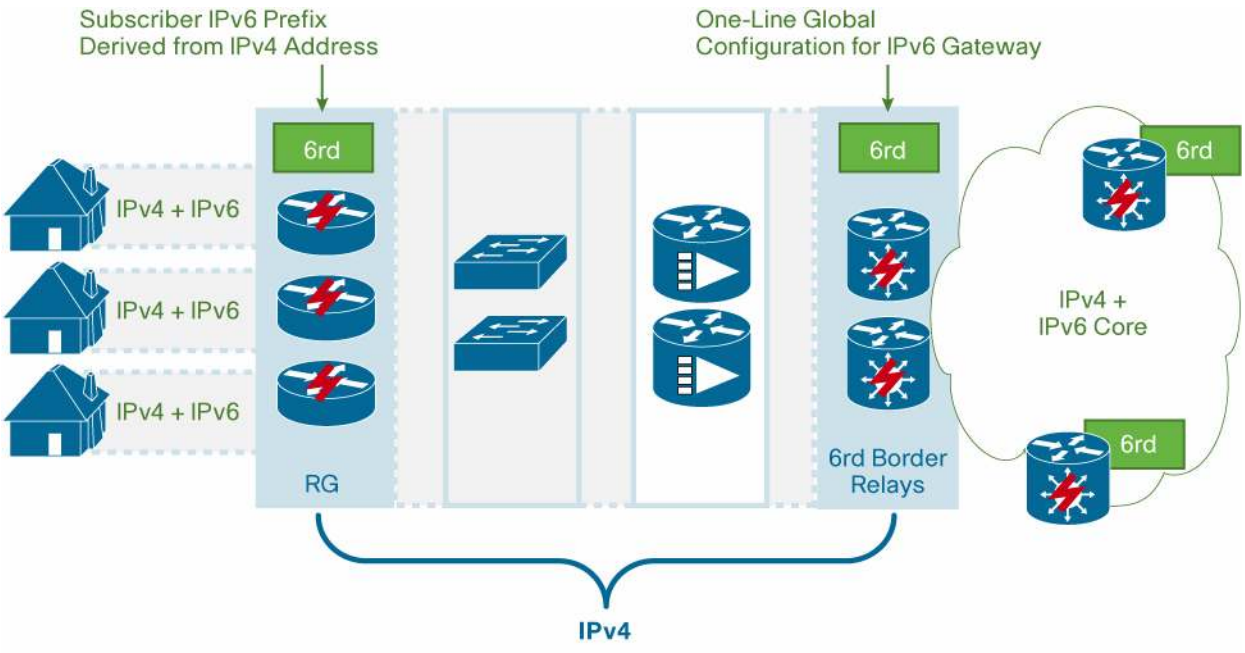
Francois-Xavier Mateo: fmateo@cisco.com

IP Tunneling: IPv6 Rapid Deployment 6RD

6RD enables incremental deployment of IPv6 unicast through existing IPv4 service provider networks. Its approach is similar to Cisco IPv6 Provider Edge (6PE) Router in that it provides native dual-stack services to a subscriber site by using existing infrastructure and operations. The solution builds on the 6to4 IPv4-to-IPv6 transition mechanism (RFC 3056), with the important differences that it uses a service provider's own IPv6 address prefix rather than 2002::/16. By using the service provider's IPv6 prefix, the operational domain of 6rd is limited to the service provider network and is under its direct control. From the perspective of customer sites and the IPv6 Internet at large connected to the 6RD-enabled service provider network, the IPv6 service is equivalent to native IPv6. 6RD operates at two places in the network: the customer edge and the border relay. *6RD* does not translate IPv4 into IPv6; it encapsulates IPv6 in IPv4 to a preconfigured *6RD* border-relay router that can de-encapsulate the IPv4 header and route the IPv6 packet outside the service provider's IPv4 network. The 6RD mechanism is fully stateless, so the border-relay routers can be addressed by anycast within the service provider network for added resiliency. Figure 1 illustrates 6RD.

6RD relies on IPv4 and is designed to deliver production-quality dual-stack IPv6 and IPv4 Internet access to customer sites.

Figure 1. *6RD* Solution



Benefits

- Accelerate the deployment of IPv6 to subscribers through the Service Provider's existing IPv4 network using existing infrastructure and operations.
- 6RD is targeted at unicast IPv6 Internet access.
- The subscriber gets native dual-stack IP service.
- IPv6 traffic automatically follows IPv4 routing.
- 6RD border relays are placed at the IPv6 edge and can be addressed through anycast for load balancing and resiliency.

Hardware

- **Routers:** Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series

For More Information

Defined in draft-ietf-softwire-ipv6-6rd.

Product Management Contact

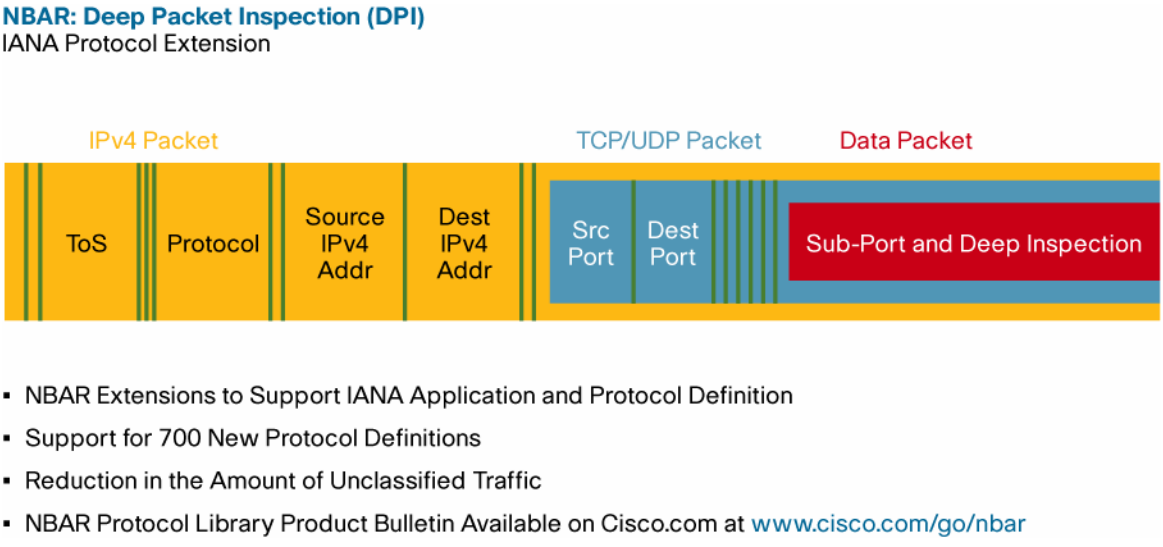
Hari Rakotoranto: hrakotor@cisco.com

NBAR Internet Assigned Number Authority (IANA) Protocol Extensions

Network-Based Application Recognition (NBAR) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications, including web-based, multimedia, peer-to-peer and client-server applications. After the applications are recognized, the network can invoke required services for that particular application: for example, QoS, reporting, or performance routing.

The NBAR protocol library has been extended with the addition of 700 Internet Assigned Number Authority (IANA) application and protocol definitions. This extension dramatically improves classification and visibility in the network. NBAR uses those definitions for last-resort classification (Figure 2).

Figure 2. NBAR IANA Protocol Extension



Benefits

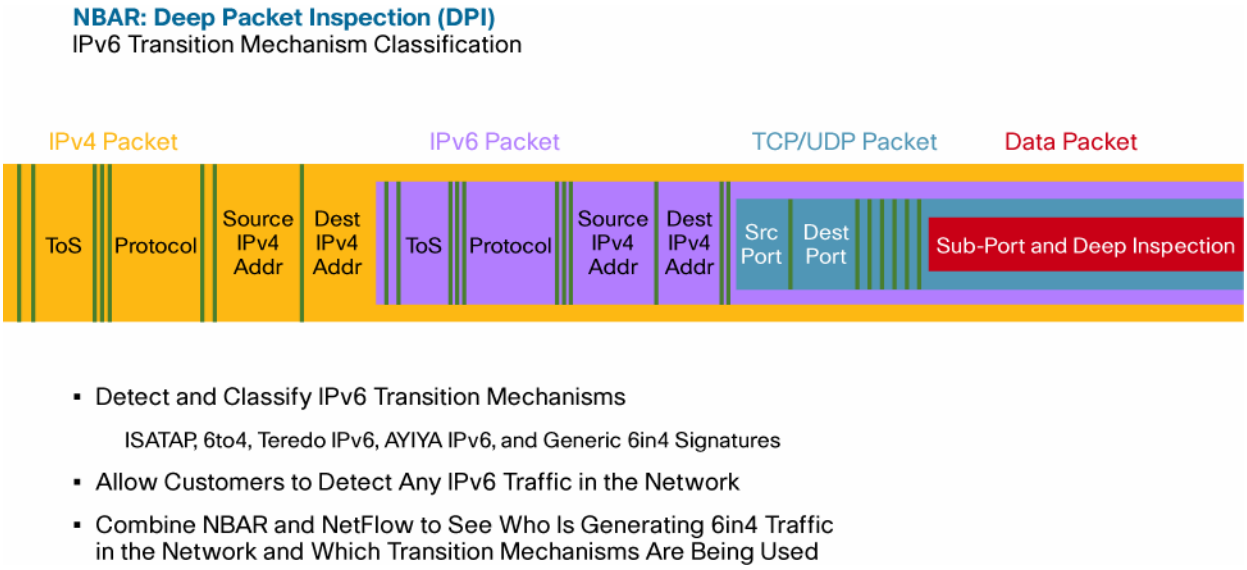
- Improve classification and visibility of traffic in the network.
- Reduce the amount of unclassified traffic.

NBAR IPv6 Transition Mechanism Detection

IPv6 transition mechanisms are used by customers to introduce IPv6 into their IPv4 infrastructure. The main benefit of these mechanisms is that they do not require any modification in the IPv4 infrastructure. To achieve this, IPv4 transition mechanisms encapsulate IPv6 packets within IPv4 packets.

NBAR can detect IPv6 traffic encapsulated in IPv4. It can differentiate IPv6 transition mechanisms such as ISATAP, 6to4, Teredo IPv6, and AYIYA IPv6. When NBAR protocol discovery used, NBAR maintains statistics for each transition mechanisms. Customers can detect any IPv6 traffic sent over IPv4, apply differentiated policies, and monitor the growth of IPv6 traffic in their infrastructures (Figure 3).

Figure 3. IPv6 Transition Mechanism Classification



Benefits

- Allow customers to detect any IPv6 in IPv4 traffic in the network.
- Combining NBAR and NetFlow reveals who is generating 6in4 traffic in the network and which transition mechanisms are being used.

Hardware

- **Routers:** Cisco 800, 1800, 1900, 2800, 2900, 3800, 3900, 7200, 7300 Series

For More Information

www.cisco.com/go/nbar

Product Management Contact

Jean-Charles Griviaud: jgriviau@cisco.com

Performance Monitor

Performance Monitor is an inline performance monitoring engine that provides real-time metrics regarding rich media streams. It provides network-related metrics for both Real-Time Transport (RTP) and Transmission Control Protocol (TCP) traffic. The metrics can be viewed through the CLI, exported through NetFlow, and retrieved through the MIB interface. It also supports threshold-based alerting using syslog and SNMP traps.

Benefits

- Efficient inline real-time performance monitoring is available for large-scale deployments.
- Embedded performance monitoring capabilities available on a wide range of platforms enables system wide solutions.
- Pervasive traffic visibility supports efficient diagnostic and troubleshooting capabilities and reduces operating expenses (OpEx).
- Effective fault detection with threshold-based alerting is supported.

Hardware

- **Routers:** Cisco 800, 2900, and 3900 Series

Product Management Contact

Steve Giles: stgiles@cisco.com

Mediatrace 1.0

Mediatrace is a powerful tracing and dynamic configuration tool. It provides automatic path discovery of traffic streams and can discover both Layer 2 and 3 devices along the path. Mediatrace while following the path of particular flow can gather crucial hop by hop information like packet loss and network jitter that the flow might be experiencing. It can also be used to collect system information such as CPU and memory utilization data of the intermediate hops. Mediatrace can be run on demand or scheduled for periodic monitoring and data collection.

Benefits

- Mediatrace provides powerful troubleshooting and fault isolation from a single point in the network.
- Dynamic configuration provides an efficient monitoring mechanism to help reduce system resource consumption for network devices.
- Support for both Layer 2 and 3 devices provides visibility on the complete path.

Hardware

- **Routers:** Cisco 800, 2900, and 3900 Series

Product Management Contact

Steve Giles: stgiles@cisco.com

Cisco IOS Embedded Event Manager 3.2

Cisco IOS Embedded Event Manager (EEM) is a powerful embedded event and automation engine that enables a wide range of use cases. Cisco IOS EEM 3.2 extends the existing Cisco IOS EEM capabilities with two new event detectors: Neighbor Discovery and Identity. With these new event detectors, Cisco IOS EEM now supports efficient discovery of new devices connected to routers and switches through Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), 802.1x, and MAC Authentication Bypass (MAB) events. A new type of Cisco IOS EEM policy, based on Cisco IOS Shell (IOS.sh), is also added. It allows Cisco IOS EEM users to program Cisco IOS EEM policies using a scripting language similar to the Linux bash shell.

Benefits

- Real-time detection and response of new devices connected.
- Device port autoconfiguration is supported.
- Network administrators have more flexibility in choosing a scripting language for Cisco IOS EEM policy design.

Hardware

- **Routers:** Cisco 800, 1800, 1900, 2800, 2900, 3800, 3900, and 7200 Series

For More Information

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

Product Management Contact

Steve Giles: stgiles@cisco.com

Dynamic Host Configuration Protocol Tunnels Support

This feature introduces the following capabilities:

- IP address assignment on GRE tunnel interfaces from a DHCP server
- Unicast DHCP replies from DHCP relay agent
- Option for DHCP clients to clear the broadcast flag

The Dynamic Host Configuration Protocol (DHCP) Tunnels Support feature provides the capability to dynamically configure a point-to-point generic routing encapsulation (GRE) or multipoint-GRE (mGRE) tunnel interface, thus making IP address assignment on a GRE tunnel interfaces more manageable in a dynamic multipoint virtual private network (DMVPN) deployment.

Benefits

- DHCP eliminates static address assignment on the tunnel interface and allows zero-touch deployment of routers and configurations.
- Large-scale DMVPN deployment is simplified because DHCP-based address assignment on the GRE tunnel interfaces makes it more manageable for network administrators.
- Spoke router rollout and maintenance is simplified.

Hardware

- **Routers:** Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series

Product Management Contact

Vivek Kokkengada: mkokkeng@cisco.com

Cisco IOS Public Key Infrastructure (PKI) Performance-Monitoring Enhancements

New configurations have been provided to enable the user to trigger public key infrastructure (PKI) benchmarking. The user can start and stop the benchmarking session and also specify the limit for the number of records that can be stored for the benchmarking session.

A configuration option allows the user to clear the peer router’s public keys stored on the router's public key cache. By specifying the index, the user can clear a particular entry. If no index is specified, then all the entries will be cleared.

A configuration option allows the user to configure the subject alternative name field of a certificate for a given trustpoint policy.

Benefits

- Simplify performance monitoring in the PKI subsystem and add debugging to analyze PKI performance-related problems.
- Flexibly administer keys on the router.

Hardware

- **Routers:** Cisco 880 and 8901800,1900, 2800, 2900, 3800, and 3900 Series

For More Information

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_deploy_RSA_piki.html

Product Management Contact

Thomas Kodair: tkodair@cisco.com

GET VPN Troubleshooting

The conditional debugging feature provides users with the capability to perform conditional debugging on the key server so that the key server can filter based on group membership or other cooperative key servers. The Event Logging feature enables users to log the last set of events, and the Exit Path capability allows the Cisco Technical Assistance Center (TAC) to troubleshoot error conditions.

Benefits

- Simplify troubleshooting for cooperative protocols for GET VPN with conditional debugging.
- Improve the process of collecting system status information for TAC support.

Hardware

- **Routers:** Cisco 880, 890, 1800, 1900, 2800, 2900, 3800, and 3900 Series

For More Information

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

Product Management Contact

Thomas Kodair: tkodair@cisco.com

Cisco IOS SSLVPN Smart Tunnels Support

A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with Cisco IOS SSLVPN as the pathway. This release lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application.

IBM Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access. Other examples of applications that work through smart tunnels are Telnet, passive FTP, Secure Shell (SSH), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), IBM Lotus iNotes, Citrix Program Neighborhood client, etc.

The remote host originating the smart tunnel connection must be running Microsoft Windows 7, Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.

Depending on whether the application is a client or is a web-enabled application, smart tunnel configuration requires one of these procedures:

- Create one or more smart tunnel lists of the client applications and then assign the list to the group policies or local user policies for the group or local user for which you want to provide smart tunnel access.
- Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, and then assign the list to the dynamic access polices (DAPs), group policies, or local user policies for which you want to provide smart tunnel access.

You can also list web-enabled applications for which you want to automate the submission of login credentials in smart tunnel connections over clientless SSL VPN sessions.

Smart tunnel is provided as an alternative to clientless mode to enhance performance and enable support of advanced web applications with Java and ActiveX content.

Benefits

- Smart tunnel improves performance for certain applications with SSL VPN.
- Smart tunnel supports large sets of applications with clientless mode SSL VPN.
- This mode of operation provides better performance.

Hardware

- **Routers:** Cisco 880, 890, 1800, 1900, 2800, 2900, 3800, and 3900 Series

For More Information

http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_smart_tunnels_support.html

Product Management Contact

Thomas Kodair: tkodair@cisco.com

Internet Key Exchange (IKE) Protocol Version 2 Remote Access Headend (IKEv2 RA)

The goals of Internet Key Exchange Version 2 Remote Access (IKEv2 RA) phase 1 are to implement an IKEv2 RFC–compliant remote access server and test the interoperability with the Microsoft Windows 7 client.

Benefits

Implement the next generation of the IKE Protocol Remote Access capability for the Microsoft Windows 7 operating system.

Hardware

- **Routers:** Cisco 880, 890, 1900, 2900, and 3900 Series

For More Information

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

Product Management Contact

Thomas Kodair: tkodair@cisco.com

IKE Protocol Version 1 CAC Enhancements

Enhancements have been made to enable a CAC limit to be set for all the negotiations taking place in the system (IKE + Phase 1.5 + IP Security [IPSec]) instead of just a CAC limit for IKE negotiations only. A CAC limit can also be set for the number of active IPSec security associations in the system.

Benefits

The infrastructure to support CAC enhancement and PKI-IKE nonblocking improves performance and scalability of the IKEv1 protocol implementation.

Hardware

- **Routers:** Cisco 880, 890, 1800, 1900, 2800, 2900, 3800, and 3900 Series

For More Information

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_call_addmsn_ike.html

Product Management Contact

Thomas Kodair: tkodair@cisco.com

Cisco Unified Communications Manager Express (UCME) and Selected Survivable Remote Site Telephony (SRST) 8.5 Enhancements

The main Cisco UCME and SRST features delivered in Release 8.5 release of the products include support for the following:

- Overlap sending on ISDN and Primary Rate Interface (PRI)
- Forced authorization code (FAC)
- Signal-to-noise ratio (SNR) enhancements on Cisco Unified Communications Manager Express
- SSL VPN client on SCCP UCME Customization of services and directories page
- Immediate divert (iDivert) feature on Session Initiation Protocol (SIP) phones
- Busy lamp field on phone applications

Benefits

- Release 8.5 of Cisco Unified Communications Manager Express and Cisco Unified SRST reduces the cost of Cisco Unified Communications Manager Express teleworkers through improved deployment flexibility of SSL VPN clients on SCCP Cisco Unified IP Phones.
- This release also improves the Cisco IP Phone user interface and the billing and accounting options, and it makes Cisco Unified Communications Manager Express and Cisco Unified SRST easier to deploy and maintain.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series, 88XSRST, 1861, UC520

For More Information

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

Product Management Contact

Tony Huynh: tonhuynh@cisco.com

Cisco Advanced Foreign Exchange Station (FXS) Analog Gateway Features

This release adds advanced FXS Analog Gateway features and SCCP over Transport Layer Security (TLS) with Cisco Unified Communications Manager Express.

The security endpoint uses the existing PKI, which is used to connect to Cisco Unified Communications Manager Express. The PKI obtains the certificate from a third party certificate authority (CA) and uses it to establish TLS sessions with Cisco Unified Communications Manager. Secure RTP (SRTP) is used to encrypt the media.

Advanced supplementary features on FXS analog ports with Cisco Unified Communications Manager include:

- Repetitive call-waiting tone
- Callback on no answer
- Media renegotiation
- cBarge
- Configurable exclusive audio message waiting indicator (AMWI) and visual message waiting indicator (VMWI)
- Single-number reach (SNR) (supported for both Cisco Unified Communications Manager and Cisco Unified Communications Manager Express)

Enhanced serviceability for analog FXS voice port line measurement on Cisco VG224 Analog Voice Gateways and Cisco IAD2430 Integrated Access Devices and certain voice interface cards will be added. New interfaces will be created to measure line voltage, current, impedance, and capacitance of the analog FXS voice port.

Benefits

- The capability to provide granular troubleshooting capabilities during initial network provisioning improves deployment when disparate analog endpoints are included.
- Automated signaling and media continuity checks make network operations and health monitoring easier in large analog deployments.

Hardware

- **Platforms:** Cisco VG202, VG224, and VG204 Series, UC500 ports, C880 ports
- **Interfaces:** VIC3-2FXS-DID, VIC3-4FXS-DID, VIC3-2FXS-E/DID, EVM-HD-8FXS/DID, and EM3-HDA-8FXS/DID

For More Information

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

Product Management Contact

- Sreekanth Menon: sreek@cisco.com
- David Sauerhaft: dsauerha@cisco.com

Cisco ISR SIP Gateway and Cisco Unified Border Element 8.6 Enhancements: Reporting End-of-Call Statistics in SIP BYE Message

Cisco Unified Border Element and the Cisco ISR SIP voice gateway report end-of-call statistics through the SIP BYE message.

Benefits

This gateway can provide demarcation functions on the public switched telephone network (PSTN) gateway as well as the Cisco Unified Border Element. These statistics can be used to update call data records on Cisco Unified Communications Manager or Cisco Unified Communications Manager Express

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR SIP Gateway and Cisco Unified Border Element 8.6 Enhancements: Conditional SIP Header Manipulation

Cisco Unified Border Element 8.6 adds support for manipulation of one SIP header based on the contents of another SIP header. This feature extends the SIP profile function that is already available on the Cisco Unified Border Element. It includes the capability to copy the contents of one header to another, or modify the contents of one header based on the contents of another. SIP headers on the out-leg can be modified based on the contents of any SIP header on any SIP message received on the in-leg.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR Unified Border Element 8.6 Enhancements: Media Flow-Around High-Density Transcoding with SIP Signaling

Cisco Unified Border Element provides support for dynamic media flow-around with no additional media control for SIP calls from branch offices to PSTNs that are controlled by a central Cisco Unified Communications Manager. Cisco Unified Border Element performs the delayed-offer-to-early-offer translation. Cisco Unified Border Element controls SIP signaling for the entire call duration, with media flowing around the Cisco Unified Border Element directly from the branch office to PSTN.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Cisco Unified Border Element 8.6 Enhancements: RFC 3311 SIP UPDATE Message

This release adds RFC 311 SIP UPDATE message support on the Cisco Unified Border Element, which allows modification of the parameters of a SIP session. The UPDATE message allows modification of session parameters just as the reINVITE SIP message does, except that the UPDATE message can be received either during early dialog (during the initial Invite transaction) or during established dialog. This feature enables Cisco Unified Border Element to interwork with service providers that use the UPDATE header instead of ReINVITE.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Unified Border Element 8.6 Enhancements: SIP-Based RSVP to Non-RSVP Cisco Unified Communications Manager Interworking

In this release, Cisco Unified Border Element provides interworking between the Cisco Unified Communications Manager controlled RSVP leg and the non-RSVP call leg for SIP calls. This support includes early offer-to-early-offer, delayed-offer-to-delayed-offer, and delayed-offer-to-early-offer combinations. Interworking between a non-RSVP H.323 call leg and a Cisco Unified Communications Manager controlled RSVP SIP call leg for fast-start-to-early-offer and slow-start-to-delayed-offer calls is also supported.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Cisco Unified Border Element 8.6 Enhancements: SIP Named Signaling Events Capability Negotiations Using Session Description Protocol

The addition of SIP named signaling events (NSE) capability negotiations using the Session Description Protocol (SDP) provides fax and modem interworking.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Cisco Unified Border Element 8.6 Enhancements: SIP Registration Proxy

In this release, Cisco Unified Border Element adds a SIP registration proxy. This feature adds the capability to send outbound registrations based on incoming registrations. It enables direct registration of SIP endpoints with the SIP registrar in hosted unified communications deployments that use Cisco Unified Border Element. This feature allows header manipulation of the REGISTER message through a SIP profile. Cisco Unified Border Element provides the flexibility to use authentication credentials from either the incoming registration requests or the CLI configuration. Registration requests are authenticated, or the authentication occurs end-to-end, in which case Cisco Unified Border Element will pass the credentials.

Benefits

This enhancement increases flexibility in network design.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Cisco Unified Border Element 8.6 Enhancements: SIP Request Processing Limit

This release adds support for limiting SIP request processing on the Cisco Unified Border Element to Incoming SIP call processing. This feature augments the security functions offered by the Cisco Unified Border Element. This feature also enables the monitoring (through the CLI) and display of the current call rate being processed by the Cisco Unified Border Element. This SIP trunk enhancement prevents DoS attacks and provides a mechanism for troubleshooting managed services deployments.

Benefits

This enhancement increases flexibility in network design and management.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Cisco ISR and Cisco Unified Border Element 8.6 Enhancements: Media Flow Release While Maintaining SIP Signaling Control

With this release, Cisco Unified Border Element can dynamically release the media flow while retaining SIP signaling control. This feature is used for media trombone designs and media hairpinning. Cisco Unified Border Element will hairpin SIP calls that end up as PSTN-to-PSTN calls, which may occur as a result of an external call-transfer or call-forward operation. After the media flow is released, Cisco Unified Border Element exerts no further control over media.

Benefits

This enhancement increases flexibility in network design and management.

Hardware

- **Routers:** Cisco 2800, 2900, 3900, and 3900E Series

For More Information

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

Product Management Contact

Darryl Sladden: dsladden@cisco.com

Suite-B IPSec Algorithm Support for the On-Board Crypto Engine for Cisco 2951 and Cisco 3900 Series ISRs

Suite B IPsec algorithm in the hardware crypto engine is now supported on the Cisco 2951 and 3900 Series Integrated Services Router platforms. Suite-B requirements comprise of four user interface suites of cryptographic algorithms for use with IKE and IPSec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

Benefits

Suite B consists of a standardized set of cryptographic algorithms which ensure interoperability

Suite B algorithms provide high strength cryptographic algorithms to secure sensitive data

These algorithms provide the higher security more efficiently which will translates to higher performance for data security

Hardware

- **Routers:** Cisco 2951, 3925, and 3945 Series

Additional Information

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_vpn_ipsec.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec.html

http://www.ciscosystems.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

Product Management Contact

Thomas Kodair: tkodair@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 C25-635704-02 03/11