Cisco IOS Software Release 15.2(1)T New Features and Hardware Support

Product Bulletin No. 682635

Cisco IOS® Software Release 15.2(1)T provides the latest innovations for the world's most demanding networks, designed for the borderless network to provide a unified architecture that is easier to operate, more reliable, and more secure.

New features are fully integrated with extensive capabilities already available in Cisco IOS Software Release 15.1(4)M to provide solutions for enterprise, service provider, and smart-grid networks. New features include:

- VPN encryption acceleration support
- Security enhancements including more IPv6 VPN functionality
- Cisco® Unified Communications Border Element (CUBE) enhancements
- Deep packet inspection capabilities for IPv6 with enhanced Network Based Application Recognition (NBAR)

Cisco IOS Software 15.2(1)T supports Cisco 800 Series Routers; Cisco 1900, 2900, and 3900 Series Integrated Services Routers; the Cisco 1861E Integrated Services Router; and the Cisco CGR 2010 Connected Grid Router.

New Features and Hardware Support

ISM-VPN for VPN Acceleration

Cisco IOS Software Release 15.2(1)T will provide support for the Integrated Services Module (ISM) for VPN acceleration. ISM-VPN offloads crypto processing to the dedicated hardware to free up the house router resources for other Cisco IOS features such as firewall, quality of service (QoS), or Network Address translation.

The module offers plug-and-play capability, allowing quick and easy installation. It provides up to 3 to 5 times throughput improvement over the onboard crypto engine on ISR-G2 and supports hardware acceleration on advanced cryptographic algorithms, such as Internet Key Exchange Version 2 (IKEv2), and Suite B.

VPN and Security Enhancements

Group Member Removal and Policy Replacement for Group Encrypted Transport VPN

The group member (GM) removal feature facilitates efficient removal of unwanted GMs from the network without modifying the existing network operation. Network operators can remove a group member instantly from the key server (KS). This action instructs the key server to send a message to all group members to redownload policies and rejoin the group if they are allowed. This causes the unauthenticated group member to be rejected from the group as per the security policy.

Policy replacement for group encrypted transport VPN (GETVPN) creates a new EXEC command to allow the KS to trigger rekey on demand after the configuration changes are completes. GETVPN policy changes alone will not trigger rekey anymore. When customers change the policy and exit from config mode, a syslog message will be

displayed on the primary KS that the policy has been changed and a rekey is needed. The user can enter this new triggered rekey command to send a rekey based on the latest security policy in the running configuration.

Benefits

- Provides additional control capability to manage GETVPN
- Simplifies implementing new policy changes and updates on the network

To learn more about GETVPN, visit http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html.

GDOI MIB Support for GETVPN

Group Domain of Interpretation (GDOI) MIB support for GETVPN provides new standard Simple Network Management Protocol (SNMP) management capabilities for routers with GETVPN enabled. Network operators can now use SNMP to gather and retrieve data related to core GETVPN functions to simplify troubleshooting, recording network events, and operating the network.

The GDOI MIB consists of MIB objects and notifications (traps). The MIB objects and notifications reflect the status on both the key server and the group member. MIB objects included in the MIB are key and traffic encryption key tables, traffic, and policy tables. Notifications include new registrations, rekey, reregistrations, and rekey failure.

Benefits

- MIB statistics provide detailed visibility for core GDOI operation and counters.
- Standard SNMP with GETVPN provides easy access and facilitates integration with current SNMP-based network management systems.

IPv6 Transport for Dynamic Multipoint VPN

This feature allows sites deployed with an IPv6 WAN address to have access and connectivity with a virtual private network. Both IPv4 and IPv6 passenger traffic can be secured and transported over the IPV6-only WAN. The IPv6 site can connect to an IPv6-capable hub and get full access to VPN. This provides the IPv6 site with dual stack access to all the VPN. This feature allows connecting IPV6-only sites with IPv4-only sites through the hub and the core network.

New sites and deployments are faced with the challenges of running out of registered IPv4 addresses. New sites in various regions are starting to require IPv6 addresses on the WAN interface. IPv6 transport for Dynamic Multipoint VPN (DMVPN) eases the migration to and rollout of IPv6-only sites. This feature allows the mGRE interface to be IPv6 aware with source, destination, and tunneled traffic, and also allows the Next Hop Resolution Protocol (NHRP) to work over the IPv6 interface. IPv6 transport for DMVPN integrates with existing Cisco IOS services that are supported with IPv6, including generic routing encapsulation (GRE), NHRP, and Cisco Express Forwarding.

This release provides support for the following with IPv6 transport DMVPN:

- Dual hub topology for resiliency and failover
- Hub and spoke tunnel topology with access between the spokes through the hub

- Dynamic routing for IPv6 and IPv4 with Enhanced Interior Gateway Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol Version 2 (RIPv2)
- NHRP MIB and syslog enhancements
- Backup Next Hop Server (NHS) and hub configuration with fully qualified domain name (FQDN)
- Virtual Route Forwarding (VRF) awareness for the tunneled traffic and GRE tunnel

Benefits

- Allows IPv6-only sites to have full VPN access for both IPv4 and IPv6 passenger traffic
- Eases the migration and rollout of IPv6 addresses in the public and private WAN
- Maintains end-to-end connectivity for passenger traffic over any mix of IPv4 or IPv6 addresses in the WAN
- Supports private addresses across the network without the need for address translation across the network

For additional detailed information, visit http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dmvpn_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

DHCP Automatic IPv4 Address Pool Assignment for DMVPN Spokes

The Dynamic Host Configuration Protocol (DHCP) automatic IPv4 address pool assignment for DMVPN spokes feature uses the DHCP On-Demand Address Pool (ODAP) feature to support the centralized management of overall IP addresses and zero-touch spoke DMVPN deployments.

Support for dynamic IP address allocation for the DMVPN spoke's GRE tunnel interface was introduced in Release 15.1(3)T. The spoke devices in DMVPN deployments must be configured statically for local DHCP pools so that they can distribute addresses to hosts on their inside LAN interface. This involves substantial administrative overhead. The management of large pools of IP subnets needs to be centralized to simplify the configuration of subnets allocated to LAN interfaces in large DMVPN networks.

The Cisco implementation of DHCP provides an additional functionality of ODAP subnet allocation. The ODAP subnet allocation allows DHCP to be used not only to allocate and install an IP address for the DMVPN mGRE or peer-to-peer tunnel on the spoke, but also to allocate an IP subnet to be used by the spoke to distribute addresses on its inside LAN interface. ODAP is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of subnets and IP addresses.

Benefits:

- Centralized IP address manageability, which reduces administrative overhead
- On-demand IP address assignment on branches or spokes

Cisco AnyConnect VPN Client with IPsec and IKEv2

The Cisco AnyConnect Secure Mobility Client 3.0 added the secure connectivity option with IPsec tunnels and Internet Key Exchange Version 2. This Cisco IOS release provides support for a Cisco AnyConnect Essentials 3.0 license connecting to Cisco ISR G2 routers. A preinstalled Cisco AnyConnect client can use the IKEv2 profile and be configured with various Extended Authentication Protocol (EAP) methods including EAP-MSCHAPv2, EAP-MD5, and EAP-GTC. In the case of certificate authentication (RSA-Signature Auth), the Cisco IOS server and AnyConnect 3.0client post advanced certificate requests to the common trust-point certificate server and obtain the certificates and use them for mutual authentication.

Benefits

- Eases client administration: Allows the administrator automatically to distribute policy updates from the VPN headend
- Allows service providers to offer secure managed connectivity service with VRF support
- Provides an optimized connection for latency-sensitive traffic when security policies require use of IPsec/IKEv2

To learn more, visit the Cisco AnyConnect VPN Client data sheet.

For additional detailed information, visit http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html.

Windows 7 Client Termination with IPsec and IKEv2

This feature allows a PC with Windows 7 to connect to Cisco IOS devices with IPsec and IKEv2. With this release, Windows 7 can establish an IPv6 tunnel for IPv6 passenger traffic and an IPv4 tunnel for IPv4 passenger traffic.

Benefits

- Provides secure connectivity for standalone systems operating with Windows 7
- Supports both IPv4 and IPv6 connectivity

For further detailed information, visit http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html.

PKI with IPv6 Support

Cisco IOS Public Key Infrastructure (PKI) provides certificate management to support security protocols and solutions in Cisco IOS Software. With this release the PKI with IPv6 will support IPv6 addresses in certificates and Certificate Authority (CA) authentication, CA revocation, Certificate Revocation List (CRL) checking, and Cisco IOS CA server.

Benefits

- Facilitates IPv6 VPN solutions and IPv6 applications in Cisco IOS Software to support PKI
- Centralized authentication protocol for simplifying VPN deployment with PKI

For detailed information, visit http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_pki_feat_rmap_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

IKEv2 Remote Access Support

This release provides support for a remote access (RA) solution based on IKEv2. This feature is applicable to the remote router and to the hub router. It provides migration from the EasyVPN Solution to the IKEv2 standard-based solution. This migration includes a change from the mode-config parameter to IKEv2 equivalent-based parameters and updates the existing command-line interface (CLI) to support remote access and site-to-site configuration in the same VPN solution.

Features in this release include:

- Support for multiple IPv4 proxies over IPv4 transport
- Support for dynamic routing protocols
- Flexible route injection through mode-config

- Using a virtual tunnel interface with a point-to-point interface
- Full support for a wide range of authentication schemes except EAP-based authentication
- Split Domain Name System (DNS) support
- Windows Internet Naming Service (WINS)/Netra Blade Management Suite (NBMS) client push
- Automatic and manual connect modes
- Track-based tunnel activation
- NAT
- VRF support
- Enhanced backup schemes: Backup gateway list, multiple peer with default peer support, primary and backup tunnels
- Reactivation of primary peer
- Dual tunnel configuration

Benefits

- Provides a single infrastructure for a secure VPN capable of delivering remote access and a site-to-site solution
- Modular configuration supporting a wide range of parameters and network designs

For additional information, visit http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

Enhanced Network Based Application Recognition

Identifying and classifying network traffic is an important first step in implementing policies for effectively managing traffic based on applications and business needs. A network administrator can more effectively implement QoS and other policies after identifying the amount and the variety of applications and protocols that are running on a network.

NBAR gives network administrators the ability to see the variety of protocols and the amount of traffic generated by each protocol. After gathering this information, NBAR allows users to organize traffic into classes. These classes can then be used to provide different levels of service for network traffic, thereby allowing better network management by providing the right level of network resources for network traffic.

NBAR allows deep packet inspection and application reporting for IPv6 traffic.

Benefits

- Advanced IPv6 classification allows customers to classify IPv6 traffic based on the application layer using NBAR2, which can recognize more than 900 applications.
- Advanced reporting for IPv6 traffic: Combining NetFlow Version 9 and IPv6 NBAR to provide application-aware IPv6 flow records, which give a more granular view of IPv6 traffic flowing on customers' infrastructures.

Cisco Unified Border Element Enhancements

With this release, the Cisco Unified Border Element, the Cisco IOS Software embedded Session Border Controller (SBC), continues to be enhanced with several important new features. For a complete introduction to CUBE, visit http://www.cisco.com/go/cube.

Media Forking

A major new feature in this release is media forking, which provides network-based duplication of Session Initiation Protocol (SIP) media and signaling packets for real-time recording of voice conversations. Media forking allow customers greater choice when it comes to recording architectures for compliance needs. Customers will now be able to move the role of packet duplication for media calls from a dedicated appliance or a port span solution into a "smart recording" solution where the network is aware of which calls to fork.

Domain-Based Routing

A second important feature is the support of domain-based routing of voice and video calls through CUBE. This feature paves the way for more dynamic and flexible call routing, allowing the customers to have more choices about how to interconnect with partners for sharing voice and video calls.

Midcall RE-INVITE Consumption

Midcall RE-INVITE consumption focuses on having the CUBE software interconnect different devices that have different methods for midcall feature invocation (that is, RE-INVITEs). For example, customers can now more effectively use CUBE for interconnecting between Cisco WebEx® conferencing solutions to Cisco Unified Communications Manager voice solutions.

CUBE SIP Trunking

The Cisco 800 Series integrated services router now supports SIP trunk connectivity, including demarcation and interworking, based on CUBE, Cisco's SBC. The CUBE feature license on the Cisco 880 and 892F ISR is available as a bundled offer to simplify both ordering and network capacity planning. CUBE IP-IP Voice gateway functionality for connecting to SIP trunking services may be used as a replacement for Primary Rate Interface (PRI) or Foreign Exchange Office (FXO) voice connectivity to the service provider.

OSPFv3 Multiaddress Family Support (RFC 5838)

Provides the ability to route IPv6, IPv4, unicast, and multicast traffic with one common routing protocol implementation. Since OSPF is designed to support multiple routing table instances, OSPFv3 multiaddress family support is a natural way to extend support for IPv6 requirements with complete feature functionality and consistent routing behavior.

Benefits

- Simple IPv4/IPv6 interoperability and migration
- Easy to debug and operate with separate link-state databases per address type
- No configuration changes for the existing configuration in most cases
- Interoperability within mixed IPv4 and IPv6 environments

To learn more, visit OSPFv3 Address Families At-A-Glance.

OSPFv3 MANET Enhancements

Cisco OSPFv3 enhancements for mobile ad hoc networks (MANETs) improve the performance and scalability of OSPFv3 in dynamic wireless mobile environments.

Benefits

- Scalability: Improves routing efficiency and reduces overhead in mobile ad hoc environments, so network clusters can scale to support more users
- Fast convergence
- Easy migration: Allows OSPFv3 to extend to ad hoc environments
- Simple: Use one routing protocol for IPv6 and IPv4 to integrate wireless MANETs with existing wire-line networks

To learn more, visit OSPFv3 MANET Enhancements At A Glance.

AAA over IPv6

Vendor-specific attributes (VSAs) are available to support authentication, authorization, and accounting (AAA) for IPv6. Customers can deploy IPv6 RADIUS or the TACACS+ server to communicate with Cisco IOS routers.

Additional New Features

MPLS-TE—TE over GRE support

Transporting MPLS over GRE allows separate networks to run MPLS and connect across an ISP or WAN with each other without losing MPLS functions. The tunnel acts as a link between the MPLS networks. These enhancements allow the suite of MPLS traffic engineering (MPLS-TE) capabilities to work in the same architecture.

Support is included for:

- Traffic engineering, policy routing onto MPLS tunnels, forwarding adjacency, RSVP Hello State Timer
- Advanced MPLS-TE signaling including label-switched path (LSP) attributes, IP explicit address exclusion, Cisco Prime™ Collaboration Manager for tunnels, Verbatim path support
- Support of PW mapping onto TE tunnels
- RFC4379-compliant MPLS Operations, Administration, and Maintenance (OAM) support for MPLS-TE

Benefits

- Makes use of MPLS segmentation capabilities, such as Layer 2 and Layer 3 VPNs
- Implements explicit path forwarding and bandwidth management over GRE tunnels
- Simplifies MPLS/IP layer traffic encryption using IP crypto devices and IPsec

Performance Routing and RSVP CAC Integration

Performance routing (PfR) complements traditional routing technologies by using the intelligence of the Cisco IOS infrastructure to improve application performance and availability. PfR can select the best path for an application based upon criteria such as reachability, delay, loss, jitter, and Mean Opinion Score (MOS). Performance routing can also improve application availability by dynamically routing around network problems like black holes and brownouts that traditional IP routing may not detect. The intelligent load balancing capability of performance routing can optimize path selection based upon link utilization or circuit pricing.

Two new features extend PfR path selection to include RSVP:

- PfR RSVP control
- PfR/RSVP CAC integration

These features tie network call admission control (CAC) models to application-aware routing. For example, when RSVP detects a reservation failure locally, it can now request PfR to resolve an alternate path. Customers can improve network resiliency and service-level agreements (SLAs) by more effectively balancing the RSVP-controlled bandwidth reserved for voice or video.

QoS Overhead Accounting

This feature allows customers to specify an overhead parameter for egress LAN shaping.

Benefits

- Improves QOS accuracy on LAN interfaces where an extra encapsulation layer is used (for example, IPsec)
- Simplifies QOS deployment on LAN interfaces by allowing customers to specify the exact encapsulation overhead to be used by the QOS scheduler

Service Advertisement Framework Enhancements

Cisco Service Advertisement Framework (SAF) is a Layer 4 communications framework built into Cisco IOS Software that distributes service messages around the local and wide area network much like how routing protocols propagate routes.

Two new SAF features are introduced:

- EIGRP/SAF HMAC-SHA-256 Authentication provides neighbor authentication using the Hashed Message Authentication Mode HMAC-SHA-256 algorithm.
- SAF Dynamic Neighbors adds the ability to peer SAF forwarders as neighbors without explicit configuration of the neighbor.

Benefits

- SAF is now more secure with stronger neighbor authentication.
- SAF is now simpler to manage.

For More Information

The Cisco IOS 15.2M&T release notes provide more information on each new feature.

For:

- Cisco 800 Series Routers visit http://www.cisco.com/en/US/partner/products/hw/routers/ps380/index.html
- Cisco 819 Integrated Services Routers, visit http://www.cisco.com/en/US/products/ps11615/index.html
- Cisco 1800, 1900, 2900 and 3900 Series Integrated Services Routers, visit http://www.cisco.com/en/US/partner/products/ps10906/Products_Sub_Category_Home.html
- Cisco CGR 2000 Series connected grid routers, visit http://www.cisco.com/en/US/partner/products/ps10977/index.html

Cisco routing and switching services are available to plan, build, and run a more intelligent, responsive, integrated routing and switching network. To learn more, visit http://www.cisco.com/en/US/products/ps6897/serv_group_home.html or contact your local account representative.

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 C25-682635-00 08/11