Cisco IOS Software Release 15.1(2)T New Features and Hardware Support

PB620744

Last updated: September 2010

Introduction

Cisco IOS Software Release 15 M and 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 Borderless Network Services. Cisco Integrated Services Routers are the first platforms to take advantage of these new capabilities. Release 15 M and T provides:

- New feature releases deliver sooner (three new Release 15 M and T family feature releases per year)
- Broadened operational feature consistency across major releases
- Predictable new feature release and rebuild schedules
- Proactive individual release support lifecycle policies
- Easier software selection, deployment, and migration guidelines.

Release 15.1(2)T is the third in a series of individual Cisco IOS Release 15 M and T new feature releases, each of which delivers aggregate functionality through its predecessor (including feature inheritance from Releases 12.4T and 12.4 Mainline), and introduces new technology and hardware support. Key features in Release 15.1(2)T include:

- MPLS VPN over mGRE
- BGP Dynamic Neighbors
- Static Route Support for BFD over IPv6
- Unified Communications (UC) feature enhancements for CUCME, SRST, and CUBE

Release 15.1(2)T is a Standard Maintenance release (19 months support). Refer to the Release Notes for Cisco IOS Software Release 15.1(2)T for specific hardware platform support: http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151TREQS.html

BFD MIB v2

Bidirectional Forwarding Detection (BFD) Management Information Base (MIB) support provides the embedded management capability to system running BFD. With this capability, network operators can use the standard SNMP protocol to gather and retrieve data related to BFD operation from systems running BFD. Current implementation allows the retrieval of both IPv4 and IPv6 BFD related information.

Benefits

Provides MIB statistics for BFD operations for both BFD IPv4 and BFD IPv6 sessions.

Easy access via the use of standard SNMP protocol and facilitate integration with current SNMP based network management systems

Hardware

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

Additional Information

http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-IETF-BFD-MIB

Product Management Contact

Hari Rakotoranto, hrakotor@cisco.com

BFD IPv6 Support

Bidirectional Forwarding Detection (BFD) is the de-facto connectivity check mechanism for failure detection at layer IP. This functionality enhances the current BFD implementation so that support for IPv6 address family can be used. It provides the necessary infrastructure for running BFD over an IPv6 enable networks.

BFD clients such as Open Shortest Path First (OSPF) v3 and static IPv6 route can leverage this capability and use BFD as the mechanism providing fast hellos.

Benefits

Provides fast failure detection capability which improves and optimizes network performance and availability for IPv6 based networks.

Allows the use of single hello fast detection mechanism which can be leverage by multiple clients

Hardware

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

Additional Information

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html

Product Management Contact

Hari Rakotoranto, hrakotor@cisco.com

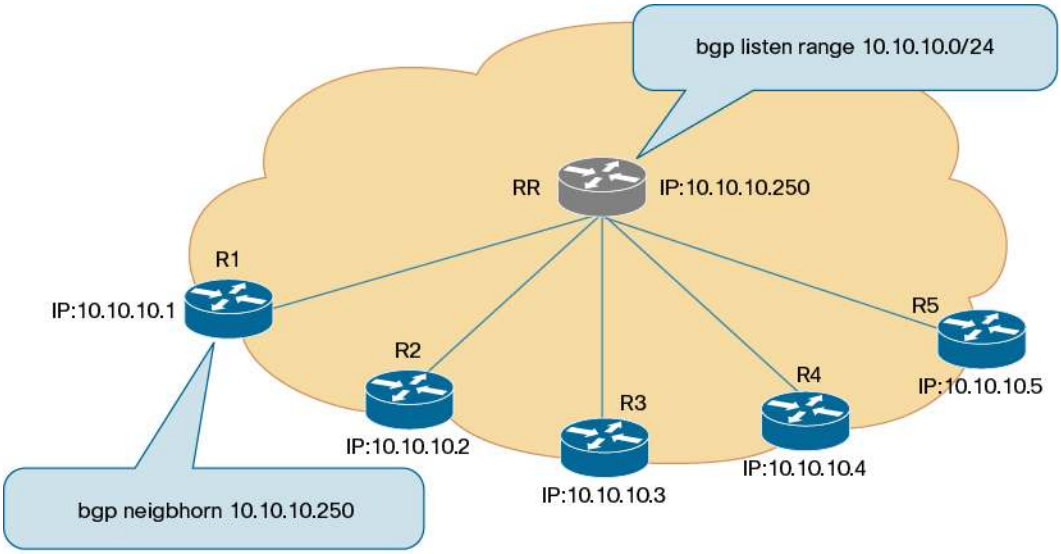
BGP dynamic neighbor

Without BGP dynamic neighbor, the user must configure each BGP peer sessions one by one, with BGP dynamic neighbor, the user could define a peer-group and address a range of BGP peer's reducing route-reflector configuration to one peer-group.

The basis

- Passively listens to a prefix (eg. 10.10.10.0/24) for incoming BGP sessions configured by using "bgp listen range 10.10.10.0/24 peer-group FOO" command
- Currently uses peer-group as a template for the neighbor session parameters and policy parameters configuration for the subnet range
- BGP neighbors are created for incoming TCP connections based on the source IP address of the TCP connection and which needs to be in the valid range of the subnets configured for listening.
- TCP options (like MD5, TTL, PMTU and others) are all preserved for each Subnet group

Benefits



- In a hub and spoke deployment, only the spokes need configuration when they are added The spokes can use addresses from a single subnet. The hub only need to know about the subnet.
- In RR configurations, RR can be configured to listen to a specific subnet (10.10.10.0/24) and the RR-clients can connect to the RR in that subnet .
- Similarly confederations can be easily configured for scaling iBGP connectivity.

Hardware

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

Additional Information

http://wwwin.cisco.com/ios/tech/rtgsvcs/iprouting/bgp/

Product Management Contact

Bertrand Duvivier, bduvivier@cisco.com

L3VPN (IPv4 & IPv6) over mGRE (IPv4)

L3VPNs (Also known as MPLS-VPNs: Multi-Protocol Label Switching-Virtual Private Network) are one of the most widely deployed VPN architectures in the global Internet. However, a major prerequisite for MPLS-VPN is the support for MPLS in all the customer core routers.

The situation becomes complicated when customer themselves use a backbone carrier to bring connectivity to their networks since the ability of the backbone to support MPLS (Multi-Protocol Label Switching) connectivity would be crucial to the customer.

Generic Routing Encapsulation (GRE) is a tunneling protocol designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet.GRE is commonly used in a point-to-point form, having two peers form the endpoints at either end of the tunnel.

MGRE is another derivative of GRE but it differs in that at one end of the tunnel is a single endpoint that has multiple endpoints associated with it at the other end. A MGRE tunnel is logically a collection of GRE tunnels. However, there are multiple tunnel destinations and they are not known ahead of time. Therefore, tunnel destination option is not available. The MGRE tunnel provides a common linkage between all the

branch offices that want to connect into the same VPN. While GRE requires full mesh topology, the MGRE used point-to-multipoint topology and thus less number of tunnels.

MPLS-over-GRE (generic routing encapsulation) tunnel is a concept that has been proposed to bring MPLS connectivity between networks that are connected by an IP-only network.

Thus, MPLS LSPs can use GRE tunnels to cross routing areas, Autonomous Systems, and ISPs. MPLS VPN over MGRE specifies such a service using IPv4 based multipoint GRE tunnels (RFC 2784) to encapsulation VPN labeled IPv4 and IPv6 packets between PEs without the need to deploy MPLS/LDP between the PEs and without the need to deploy the traditional VPN overlay techniques.

Benefits

- Provide a solution for Enterprise and SP customers to deploy L3VPN over IP transport Network.
- Support IPv4 and IPv6 address families
- Simplified configuration
- Scalable VPN solution
- Ease the migration from using multiVRF to an integrated and scalable Wan VPN solution.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 Series • Cisco 7600, ASR1000 (other release)

Additional Information

http://wwwin.cisco.com/ios/tech/mpls/l3vpns/bgp/

Product Management Contact

Bertrand Duvivier, bduvivie@cisco.com

IPv6 Support for Cisco IOS Zone Base Firewall (ZBFW)

The Cisco IOS Firewall runs on the Cisco Integrated Services Router (ISR) both at the branch office and head offices for secure Internet connectivity. The increasing awareness of IPv6 from our customers has created a demand for adding IPv6 capability in the Cisco IOS Zone Base Firewall(ZBFW). Supporting IPv6 in ZBFW not only addresses the next generation of IP addressing but also builds value on Cisco's IOS FW security architecture. With this new IPv6 support, Cisco IOS ZBFW will help bridge the challenges with regard to migration from IPv4 networks to pure IPv6 networks

The IPv6 Support for Cisco IOS ZBFW is the following:

1. Extend Common Classification Engine (CCE) IPv6 classification capability for ZBFW.
2. Global Parameter Map (GPM) and Default parameter-map support.
3. Unified Management Information Base System (MIBS) support for IPv6
4. Intrazone traffic support for IPv6
5. Conditional debugging support for ZBFW IPv6
6. Log summarization support for ZBFW IPv6
7. IPv4 FTP engine is changed to dual stack and is capable of processing control stream packets in Cisco Express Forwarding(CEF) path itself.

Hardware

Routers	• Cisco 800, 1800, 2600, 2800, 3700, 3800, 1900, 2900, 3900, 3900E

Product Management Contact

Nelson Chao, nechao@cisco.com

DMVPN Tunnel Health Monitoring and recovery (Backup NHS)

Dynamic Multipoint VPN Tunnel Health Monitoring and Recovery feature allows the Enterprise or Service Providers to support flexible control and administration to multiple data centers or central sites for spokes routers. Spokes routers can be provisioned with a set of active and standby hub sites. This enables the spoke to have active connection with nearest data center sites and standby connections others based on the hub site priority order.

With this feature, the spoke is configured with the required number of active spoke to hub tunnels, such as 2 for dual hub scenario. This instructs the spoke router to maintain two active connection with highest priority and available hubs.

As a result, there can be the following scenarios cases for the deployment on the DMVPN spoke:

Case 1: a spoke router with active connection to two hubs, and the rest of the hubs are in standby. If one or both of the top priority hub fails. The spoke tries to re-connect to all existing hub based on the priority order, and fails back to the highest priority when it becomes available.

Case 2: with spoke router configured with multiple hubs at the default priority and with maximum connection of 2. this enables the spoke to connect to any two of the available hubs. If an active hub connection fails, the spoke find the next available hub to connect to, but it does not fail back for another hub in the same priority, and it can only failback to a hub in a higher priority.

Case 3: Spoke connected with two datacenter, each data center has two hub. Using group attribute, the spoke router can be configured with a group for each of the datacenter. This way the spoke maintains at least one tunnel to each of the data centers, and can failover the second hub in the same data center if necessary.

Case 4: full flexibility for customizing the policy as a combination of the above cases.

This feature does not effect or change the dynamic routing behavior with DMVPN, and it only controls the active Spoke to hub tunnel.

Benefits of DMVPN Tunnel Health Monitoring and recovery (Backup NHS)

- Allows remote office router to recover dual hub topology during failure of any primary active hub
- Improve administration of the spoke allocation to different hubs
- Flexible method for allocating the failover hub sites for regional and global recovery.

Hardware

Routers	• Cisco 800, 1800, 2600, 2800, 3700, 3800, 1900, 2900, 3900, 3900E

Product Management Contact

Thomas Kodair, tkodair@cisco.com

Documentation link

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

DMVPN configuration using FQDN

DMVPN spoke router relies on static tunnels to hub for the initial connectivity of the DMVPN topology. Prior to this feature, the spoke router has to have a static ip address of the hubs defined in the configuration. This feature allows the spoke to have the FQDN of the hub in the configuration too.

Benefits of DMVPN configuration using FQDN:

- Simplifies the DMVPN spoke deployment and the renumbering of the Hub addresses.
- Allows for DNS based load balancing from the spoke to the hub
- Supports dynamic IP address on the hubs
- Simplifies the NHS configuration on the spoke router

Hardware

Routers	Cisco 800, 1800, 2600, 2800, 3700, 3800, 1900, 2900, 3900, 3900E

Product Management Contact

Thomas Kodair, tkodair@cisco.com

Documentation link:

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

Cisco Unified Border Element (CUBE) Feature Enhancements

- Box to Box Redundancy for SIP Trunk calls with active call preservation
- Support for mid call negotiation of an audio codec with SIP calls Additional MIBs to all monitoring utilization of critical resources on the Border Element
- Dial-peer level bind for SIP Messages allowing configuration of multiple incoming SIP Trunk providers
- Inbound Dial-peer Matching Based on Remote IP Address for SIP Messages;Topology Hiding in History-info, and Call-routing Based on History-info
- Support for Voice Mail Waiting Indicator (VMWI) over SIP on Cisco IOS Gateways

Benefits

- Box to Box redundancy is important for many large scale deployment of SIP Trunks. This feature provides a important tool to improve resiliency of Cisco SIP Trunk solution Mid call codec renegotiation enabled new deployment scenarios that allow for calls to be transferred between regions that support different codecs. Additional MIBs enable Service Providers to better profile calls, enforce security policies, and perform profile based billing of calls on a SIP trunk to gateway routers
- The improved SIP features enhances privacy by preventing topology leaks across domains; prevents call-routing loops and unnecessary retries
- Support visual message waiting on analog phones

Hardware

Routers	• Cisco 2900, 2900E,3900, 3900E Series support all features • Some features available on 1800,2800 and 3800 Series • Some features available on the ASR1000 Series

Additional Information

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

Product Management Contact

Darryl Sladden: dsladden@cisco.com

External Mailer: ask-cube-pm@external.cisco.com

Cisco Unified Communications Manager Express and Survivable Remote Site Telephony Feature Enhancements

- Toll-fraud security enhancements on voice routers
- Video Telephony support with Cisco Unified Video Advantage (CUVA) for Cisco Unified IP Phones 6921, 6941, and 6961 in CME
- Automatic upload of CDR records collected during SRST
- Single number reach service localization and 4 new locales (Latvian, Lithuanian, Estonian, Arabic)

Benefits

- Reduced toll-fraud incidents for customers
- Improve video adoption using CUVA with low cost Cisco Unified IP Phones 6900 series
- Improved user experience through localization for CME customers

Hardware

Routers	• Cisco 1800, 2800, 3800, 2900, 2900E,3900, 3900E Series

Additional Information

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

http://www.cisco.com/en/US/products/sw/voicesw/ps2169/index.html

Product Management Contact

access-ccme-cue@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 C25-620744-01 09/10