Cisco IOS Software Release 15.2(2)T

Last updated: May 2012

Introduction

Cisco IOS® Software Release 15.2(2)T offers new features for borderless networks to provide a unified architecture that is easy to operate, secure, and reliable.

New features are fully integrated with the existing capabilities in Cisco IOS® Software Release 15.1(4)M to provide best of class solutions for enterprise, service provider, and smart-grid networks. New features in this release include the following:

New Hardware Feature Support in Cisco IOS Release 15.2(2)T

- Cisco 860 Series Integrated Services Routers
- G.SHDSL EFM/ATM Multimode
- SM-32A Module Support on ISR G2 3900/3900E Platforms

New Software Feature Support in Cisco IOS Release 15.2(2)T

Security

- Cisco TrustSec Support for IOS ISR
- FlexVPN Spoke-To-Spoke
- Dynamic Multipoint VPN (DMVPN) Smart Spoke Enhancements

Routing Innovations

- LISP Network Virtualization
- OSPFv3 Not So Stubby Areas (NSSA) (RFC3101)

Cloud and Virtualization

- Next Generation Network Based Application Recognition (NBAR)
- Performance Routing (PfR) Data Export 1.0

Video and Collaboration

- IP Service Level Agreements (IP SLAs) Video Operation
- Video Monitoring Management Information Base (MIB)
- Medianet Video Monitoring Phase 2
- Performance Monitor (Phase 2)
- RSVP-NAT Integration
- CME SIP Phone Video
- SIP Paging and Shared Line

Network Management

- Embedded Event Manager (EEM) Version 4.0
- IPSec MIB for IPv6
- Flexible NetFlow IPv6 Enhancements

Cisco IOS Software Release 15.2(2)T supports Cisco 800 Series Routers; Cisco 1800 1900, 2900 and 3900 Series Integrated Services Routers; the Cisco 1861E Integrated Services Router; and the Cisco CGR 2010 Connected Grid Router.

New Hardware Feature Support

Cisco 860 Series Integrated Services Routers

Cisco IOS Software Release 15.2(2)T supports r the Cisco 860VAE Integrated Services Router, Generation 2. The Cisco 860VAE is ideal for deployments into small offices or service provider managed CPEs. The Cisco 860VAE is flexible, silent, compact and cost optimized. The Cisco 860VAE provides multiple WAN options for maximum deployment flexibility, along with optional market leading features such as Scansafe connector, BGP, IPSec and firewall. The Cisco 860VAE series ISR is available as a Base Router (BR) with an IPBase IOS image, or as a Secure Router (SR) with an advanced security IOS image, with or without payload encryption.

G.SHDSL EFM/ATM Multimode

The Cisco multimode 4-pair G.SHDSL enhanced high speed WAN interface card is designed to deliver high-speed Ethernet services over SHDSL access, as required in Ethernet in the first mile (EFM)/Asynchronous Transfer Mode (ATM) service networks. EHWIC-4SHDSL-EA will offer symmetric data rates over one to four pairs (1-4) of copper wire, and supports both EFM and ATM modes. They connect Cisco Integrated Services Routers Generation 2 (ISR G2s) with central office digital subscriber line access multiplexers (DSLAMs), and provide up to four lines of G.SHDSL (ITU-T 991.2) connectivity. The C888EA provides four pairs of multimode G.SHDSL connectivity.

One EHWIC Model and One Fixed Platform Model

- EHWIC-4SHDSL-EA—A double-wide multimode EHWIC G.SHDSL, 4 pair, 802.3ah, EFM and ATM mode interface card
- C888EA—A multimode G.SHDSL, 4 pair 802.3ah, EFM and ATM mode fixed platform

SM-32A Module Support on ISR G2 3900/3900E Platforms

The SM-32A single-wide service module 32 asynchronous (async) ports are capable of running at speeds up to 230.4 kbps. The asynchronous ports provide connection flexibility that allows access to EIA-232 devices across a TCP/IP network. The SM-32A module greatly increases asynchronous port density for the Cisco 3900/3900E Series Integrated Services Routers Generation 2 (ISR G2).

New Software Features Support

This section describes new and enhanced features in Cisco IOS Release 15.2(2)T.

Security

Cisco TrustSec Solution on ISR Platforms

Cisco TrustSec Solution (CTS) is a system that provides security for CTS-enabled network devices at each routing hop. In this system, each network device works to authenticate and authorize its neighbor devices and applies some level of security (group tagging, role-based Access Control Lists (ACLs), encryption, etc.) to traffic between the devices.

The Cisco TrustSec network policy based access control runs on the Cisco Integrated Services Routers Generation 2 (ISR G2) providing policy based access uniquely positioned for the branch office. Cisco TrustSec provides policy based access and user identity context awareness that is secure and scalable, all with simplified ease of deployment. In addition, this feature enables business productivity, delivers security and risk management, as well as improves IT operational efficiency.

Cisco TrustSec delivers consistent identity features supported on ISR G2 switch models, in addition to authenticating authorized users (802.1X), devices (MAB/profiling) and guests (Web Auth).

FlexVPN Spoke-To-Spoke

FlexVPN Spoke to Spoke allows a FlexVPN client to create a direct flex tunnel with another FlexVPN client by leveraging the Virtual Tunnel Interfaces (VTI), Internet Key Exchange Version 2 (IKEv2) and Next Hop Resolution Protocol (NHRP) in building a Spoke-to-Spoke connected relationship.

The Internet Key Exchange Version (IKEv2) is a next-generation key management protocol based on RFC 4306 as an enhancement of the original IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining Security Associations (SAs).

FlexVPN is the Cisco implementation of the IKEv2 standard that features a unified paradigm and CLI, that also brings together four VPN topologies; site to site, remote access, partial mesh (spoke to spoke direct), and hub to spoke designs. FlexVPN's simple but modular framework extensively leverages the tunnel interface archetype while remaining compatible with traditional VPN's through the use of crypto maps.

DMVPN NHRP Event Publisher

The DMVPN Next Hop Resolution Protocol (NHRP) event publisher allows you to publish NHRP specific events to its Event Detector (ED), so they can be intercepted and acted upon by the Embedded Event Manager (EEM) system through the use of custom scripts. In this system, NHRP publishes its own NHRP specific events with data to the NHRP-ED handler. The DMVPN NHRP event publisher feature enhances Dynamic Multipoint VPN (DMVPN) with the capability to monitor, control, and react to the building of dynamic spoke-to-spoke tunnels in real-time through NHRP. The EEM combined with NHRP can leverage the actions of the NHRP-ED to support unique deployment requirements, when building dynamic spoke-to-spoke tunnels.

Routing Innovations

LISP Network Virtualization

LISP is a network architecture and protocol that implements a new semantic for IP addressing, by creating two new namespaces: Endpoint Identifiers (EIDs), which are assigned to end hosts, and Routing Locators (RLOCs), which are assigned to devices (primarily routers) that make up the global routing system. Splitting EID and RLOC

functions yields several advantages including improved routing system scalability, improved multi-homing efficiency and ingress traffic engineering. LISP support is configured on devices such as Cisco routers.

To provide improved routing scalability while also facilitating flexible address assignment for multi-homing, provider independence, mobility and virtualization, the Locator Identifier Separation Protocol (LISP) was created. LISP describes a change to the Internet architecture in which separate IP addresses are used to indicate RLOCs for routing through the global Internet, and EIDs for identifying network sessions between devices.

OSPFv3 Not-So-Stubby Area (NSSA) Option—RFC 3101

In OSPF for IPv4, stub and NSSA areas were designed to minimize link-state database and routing table sizes for the areas' internal routers. This allows routers with minimal resources to participate in even very large OSPF routing domains.

In OSPF for IPv6, the concept of stub and NSSA areas are retained. In IPv6, of the mandatory LSA types, stub areas carry only router-LSAs, network-LSAs, inter-area-prefix-LSAs, link-LSAs, and intra-area-prefix-LSAs. NSSA areas are restricted to these types and NSSA-LSAs. This is the IPv6 equivalent of the LSA types carried in IPv4 stub areas: router-LSAs, network-LSAs, type 3 summary-LSAs and for NSSA areas: stub area types and NSSA-LSAs.

Cloud and Virtualization

Next Generation Network Based Application Recognition (NBAR)

NBAR Categorization and Attributes

The NBAR categorization and attributes feature provides the mechanism of matching the protocols grouped under specific categories based on the attributes. These categories are available for Class-Based Policy Language (CPL) as a match criteria for application recognition.

Because there are many protocols and applications, categorizing them into different groups will help with reporting as well as performing group actions, such as applying QoS policies, on them. Attributes are statically assigned to each protocol or application, and they are not dependent on the traffic. The following attributes are available to configure the match criteria using the match protocol attribute command. They are the Application-Group, Category, Sub-Category, Encrypted, and Tunnel attributes.

NBAR PDL Support in Release 15.2(2)T

NBAR PDL adds support for 30 new protocols in release 15.2(2)T, adding to the already extensive PDL support on the ISR platforms. In the previous 15.2(1)T release, 38 additional new protocols were added to a growing list that now contains over 1,000 unique protocols.

Visit: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/product_bulletin_c25-627831.html to see the list of the NBAR protocols available.

NBAR Protocol Pack

The NBAR protocol pack feature provides an easy way to load a protocol pack, which is essentially a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file for them all as one. Using NBAR protocol packs, a set of required protocols can be loaded in a more simplified manner, in a

single operation, making rapid changes one less thing to be concerned about. This helps Network-Based Application Recognition (NBAR) recognize additional protocols for classification on your network.

NBAR Protocol Pack Overview

Application recognition modules (also known as PDLMs) can be used to extend the functionality of NBAR, by enabling NBAR to recognize additional protocols on your network. A PDLM is used to add support for a protocol that is currently not available as part of the Cisco IOS Software. A PDLM extends the list of protocols that NBAR can recognize.

A protocol pack is a single compressed file that contains multiple PDL files and a manifest file. Your company or organization determines the contents of the protocol pack. Protocol packs allow you to load a set of protocols together versus loading them separately.

NBAR protocol packs provide three benefits:

1. They help to simplify the loading of new protocols.
2. They make it easier to upgrade to a higher version protocol pack or revert to a lower version protocol pack .
3. They provide only the required set of protocols.

Cisco provides a specific identity number for the organization (also known as the "publisher") that creates the protocol packs and uses Cisco tools and processes to create new protocol packs. The organization that creates the protocol pack owns the pack. The Default Protocol Pack (DPP) is provided as the base protocol pack version with the Cisco IOS image in the router.

Performance Routing (PfR) Data Export 1.0

The Performance Routing (PfR) Data Export v1.0 NetFlow v9 Format feature allows your NMS systems to simplify real-time data collection from PfR. The data is exported in real-time over the NetFlow v9 transport supported in RFC 3954. PfR exports both regular performance trend data, as well as PfR Route Policy Control Events, or real-time Out Of Policy Alerts and their data.

This feature exports data from the Master Controller (MC) to data collectors in your network and allows you to see more easily how your critical business applications and networks are performing, in addition to letting you know the moment PfR takes any protective actions based on your company set policies, to instantly redirect your critical business applications onto a safe and stable path, letting you know Performance Routing is helping keep your business running.

Performance Routing (PfR) Data Export in NetFlow v9 (RFC 3954) allows you to simplify real-time application and network performance PfR policy change notifications, trends, and correlations. This is based on the NetFlow v9 standard protocol and formats under RFC 3954. This feature exports both regular time-based performance data, as well as PfR Route Policy Control Events based data.

Video and Collaboration

IP Service Level Agreements (IP SLAs) Video Operation

IP Service Level Agreements (SLAs) is a feature embedded in Cisco software. This feature allows you to understand IP service levels, increase productivity, lower operational costs, and reduce the frequency of network

outages. IP SLAs perform the active monitoring of network performance and can be used for network troubleshooting, network readiness assessment and health monitoring.

The Cisco IP SLAs Video Operation feature generates synthetic traffic and creates a custom profile from that activity. This feature can imitate a sufficient packet generation for a true video stream. IP SLAs Video Operation capable devices can act as a source or a responder for their video operations.

Video Monitoring MIB Support for Medianet Video Monitoring

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco specific SNMP Management Information Base (MIB) modules:

- CISCO-FLOW-MONITOR-TC-MIB—Defines the textual conventions common to the following MIB modules.
- CISCO-FLOW-MONITOR-MIB—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- CISCO-MDI-METRICS-MIB—Defines objects that describe the quality metrics collected for media streams that comply to the Media Delivery Index (MDI) [RFC 4445].
- CISCO-RTP-METRICS-MIB—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- CISCO-IP-CBR-METRICS-MIB—Defines objects that describe the quality metrics collected for IP streams that have a Constant Bit Rate (CBR).

Performance Monitor (Phase 2)

Cisco Performance Monitor Phase 2 introduces IPv6 support, which enables configuration of IPv6 fields, and this release also introduces Flex Keys support which opens up all the remaining Flexible NetFlow collect and match commands for use that were not supported in the previous release. Cisco Performance Monitor Phase 2 continues to enable monitoring of the flow of packets in your network and it will become aware of any issues that might impact the flow, before it starts to significantly impact the performance of the application in question. Performance monitoring is especially important for video traffic because high quality interactive video traffic is highly sensitive to network issues. Even minor issues that may not affect other applications, may have dramatic effects on video quality.

New in this release is where flows are now correlated, if the same policy is applied on the same input and output interface, the show command will display a single flow for the input and output interfaces.

Cisco Performance Monitor uses similar software components and commands as Cisco NetFlow and Cisco Flexible NetFlow, familiarity with these products will help you to understand how to configure Cisco Performance Monitor. These products provide statistics on packets flowing through a router and are the standard for acquiring IP operational data from IP networks.

NAT Aware RSVP

RSVP technology is used for three primary purposes today: RSVP CAC, RSVP as Transport, and RSVP-TE. Commonly, in the first two applications of the three (RSVP CAC and RSVP as Transport), the RSVP control plane messages need to transit through and be processed by the Network Address Translator (NAT) devices. NATs, while providing many benefits and being very common today, also comes with occasional challenges in some

network designs. One of these challenges is the fact that they interfere with some existing IP applications, and it can be difficult to deploy new applications.

RSVP, like many other control plane protocols (SIP, ICMP, etc.), have embedded IP addresses as part of their control plane messages. These IP addresses are used for path determination as well, and since RSVP messages are not handled by NAT devices today, RSVP applications work incorrectly in a NAT network deployment based scenario.

NAT Aware RSVP enables RSVP-Network Address Translation (NAT)-Application Layer Gateway (ALG) functionality. Now the RSVP-NAT-ALG functionality is enabled, and as the RSVP messages pass through a NAT device, the IP addresses embedded in the RSVP payload get translated appropriately.

Network Management

Embedded Event Manager (EEM) Version 4.0

EEM Version 4.0 features major enhancements on security, resource throttling, deployment, performance, and usability.

Cisco IOS® Embedded Event Manager (EEM) is a unique capability in Cisco IOS Software. EEM is a powerful and flexible tool used to automate tasks and customize the behavior of other Cisco IOS Software features and capabilities to suit the operations of the device to your needs. Customers use EEM to create and run programs or scripts directly on their router or switch. The scripts are referred to as EEM policies and can be programmed using a simple Command-Line-Interface (CLI)-based interface or using a complete 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 customized commands, and take local automated action based on conditions detected by the Cisco IOS Software itself.

Below is a short list of v4.0 features and benefits. In this release, the following enhancements related to EEM security, resource management, event detection and policy execution capabilities are introduced:

- **EEM Email Action Enhancements**
  - Custom TCP port for SMTP mail actions
  - Tcl-based and CLI-based EEM policies to establish secured SMTP connections with public email servers using Transport Layer Security (TLS)
- **EEM Security Enhancements**
  - Tcl policy checksum integrity check (MD5/SHA-1)
  - 3rd party digital signature support
  - Tcl policy owner identification
  - Registration of remote Tcl policies
- **EEM Resource Management**
  - Manually set CPU, memory, and EEM queue thresholds
  - Blocks new policy execution when system is already busy with existing functionalities
- **EEM Event Detector Enhancements**
  - IPv6 routing event detector support

- Syslog event detector performance enhancement
- New environment variables for CLI event detector

- **EEM Usability Enhancement**
  - Capability to report policy execution statistics including number of times a policy is triggered, dropped, length of policy execution time, and next policy execution for timed events
  - Powerful file operation support for applet policies

IPv6 Compliance of Cisco IPSec MIBs and IKEv2 Extensions to Cisco IPSec MIB

The IPv6 compliance of Cisco IPSec MIBs and IKEv2 extensions to Cisco IPSec MIB feature provides IPv6 and IKEv2 support for the Cisco IPSec MIBs.

The following MIBs are supported by the IPSec and IKE MIB support for Cisco VRF-Aware IPSec feature:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB

The CISCO-IPSEC-POLICY-MAP-MIB continues to be supported. However, because this MIB applies to the entire router rather than to a specific VPN VRF instance, it is not VRF aware; therefore, polling of the Object Identifiers (OIDs) that belong to this MIB is accomplished with respect to the global VRF context.

Flexible NetFlow: Export to an IPv6 Address

This feature enables Flexible NetFlow to export data to a destination using an IPv6 address. A flow exporter allows Flexible NetFlow to export data from the network device to remote NMS collector systems, such as a UNIX server running a NetFlow collector server. Now the NetFlow collector's destination address can be an IPv6 host network address or an IPv4 address.

Irrespective of whether or not the data being exported carries IPv6, IPv4, or a combination of both types of network traffic information, customers can now send that information onto any v4 or v6 NetFlow collector necessary. This is another step to help simplify your company preparation and migration to IPv6 as Flexible NetFlow is one of the most widely used Cisco IOS measurement technologies today.

NetFlow provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks, and provides data to support network and security monitoring, network planning, traffic analysis, and IP accounting.

For Additional Reference:

Cisco 860VAE Integrated Services Router Generation 2:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-693249.html

G.SHDSL EFM/ATM Multimode:
http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_HWICS.html

SM-32A Module Support on ISR G2 3900/3900E Platforms:
http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/sm_32a.html

Cisco TrustSec Support for IOS, for more information please refer to the Cisco TrustSec Configuration Guide, Cisco IOS Release 15.2M&T:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/15-2mt/sec-usr-cts-15-2mt-book.html

Introduction to FlexVPN:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-intro-ikev2-flex.html

FlexVPN Configuration Guide, Cisco IOS Release 15.2M&T:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15.2M&T:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn-dmvpn-15-2mt-book.html

DMVPN NHRP Event Publisher, Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15.2M&T:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn-dmvpn-nhrp-event-publisher.html

For more information on Locator/ID Separation Protocol (LISP) go to:
http://www.cisco.com/go/lisp

OSPFv3 Support for Not-So-Stubby Area (NSSA) Option—RFC 3101:
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2mt/iro-cfg.html

NBAR Protocol Pack:
http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-2mt/NBAR_Protocol_Pack.html

Performance Routing (PfR) Data Export 1.0:
http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-2mt/pfr-netflow-v9.html

Performance Routing (PfR) Data Export Configuration Guide:
http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/xe-3s/pfr-netflow-v9.html

IP SLAs Video Operations, for more information, please go to the Configuring IP SLAs Video Operations Feature Guide: http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/12-2se/sla_video.html

Video Monitoring MIB Support for Medianet Video Monitoring, for more information about these commands, see the Cisco IOS Master Command List:
http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_pasv_mon_support_TSD_Island_of_Content_Chapter.html - wp1137257

Medianet Performance Monitor (Phase 2):
http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html
http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-2mt/mm-pasv-mon.html

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator: http://www.cisco.com/go/mibs

For more information about the design, configuration, and troubleshooting of Performance Monitor and other Cisco Medianet products, including a quick start guide and deployment guide, please go to the Cisco Medianet Knowledge Base Portal: http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html

NAT Aware RSVP:
http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-2mt/config_rsvp.html

EEM Version 4.0

For more information about Cisco IOS Software EEM, please go to: http://www.cisco.com/go/eem, contact your local account representative, or email askabouteem@external.cisco.com.

IPv6 Compliance of Cisco IPSec MIBs and IKEv2 Extensions to Cisco IPSec MIB:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_imgmt/configuration/15-2mt/sec-ipsec-mib-vrf.html

Flexible NetFlow: Export to an IPv6 Address, for detailed information about this feature, see the following documents:
http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-2mt/cfg-de-fnflow-exprts.html
http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-2mt/get-start-cfg-fnflow.html

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 C25-706011-00 05/12