Cisco IOS Software Release 15.1(1)T New Features and Hardware Support

1.0 Introduction

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

Developed for wide deployment in the world's most demanding enterprise, access, and service provider aggregation networks, Cisco IOS Software Release 15 M and T provides a comprehensive portfolio of Cisco® technologies, including the leading-edge functionality and hardware support from releases 12.4 and 12.4T. These integrated technologies are delivered on the broadest range of hardware in the industry, including Cisco's Integrated Services Routers Generation 2 (ISR G2).

Release 15 M and T key innovations span multiple technology areas, including security, voice, high availability, IP routing and multicast, quality of service (QoS), IP mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

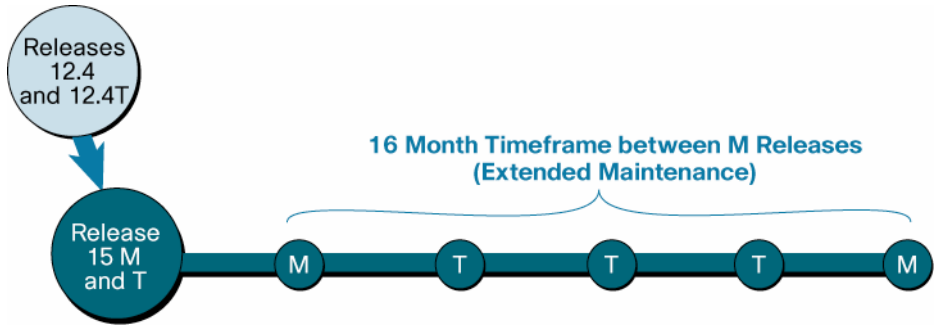
Release 15 M and T provides:

- New feature release delivery in a shorter amount of time (three new feature releases a year)
- Broadened operational feature consistency across major releases
- Predictable new feature release and rebuild schedules
- Proactive release support lifecycle policies
- Easier software selection (universal image, simplified packaging), deployment (software activation for services enablement), and migration guidelines.

Key highlights of Release 15 M and T, illustrated in Figure 1, include the following:

- Feature inheritance from Cisco IOS Software Releases 12.4T and 12.4 Mainline
- Extended maintenance 15 M releases every 16 months: Allow customers to qualify/deploy/remain on a release longer with active bug fix support
- Standard maintenance 15 T releases (between 15 M releases): Ideal for the very latest features and hardware support before the next M release becomes available on Cisco.com
- Rebuilds of 15 M and T releases to provide ongoing bug fixes only

Figure 1. Release 15 M and T Overview

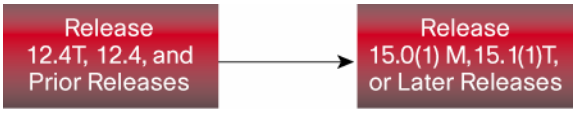


1.1) Migration Guide

Cisco recommends that customers running Release 12.4T, 12.4, or earlier Cisco IOS Software M and T releases upgrade to Release 15.0(1)M or later releases where possible. Customers should determine their functionality needs and choose the appropriate release.

Figure 2 illustrates the current migration path from Cisco IOS Software Releases 12.4 and 12.4T and releases prior to Release 15.0(1)M.

Figure 2. Migration Path



Hardware Requirements for Release 15.1(1)T

Cisco IOS Software Release 15.1(1)T supports Integrated Services Routers Generation 1 and Generation 2 Series. Release 15.1(1)T does not support the Cisco 7200 Series or 7301 Router. Refer to the Release Notes for Cisco IOS Software Release 15.1(1)T for specific hardware platform support at http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151TREQS.html.

Note: Cisco 7200 Series and Cisco 7301 Routers will continue to be supported in Cisco IOS Software 15 M releases. Refer to the following product bulletin for more information: http://www.cisco.com/en/US/prod/collateral/routers/ps341/product_bulletin_c25_597353.html

Please refer to the following website for Integrated Services Routers feature sets and memory recommendations:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletins_list.html

Additional information can be found on the Cisco.com products and services and support websites:

- http://www.cisco.com/en/US/products/index.html
- http://www.cisco.com/go/support

AppleTalk Support Discontinuation

Due to a significant decrease in AppleTalk usage and demand among its customer base, and given the fact that Apple now fully supports the TCP/IP family of protocols, Cisco has reached the decision to discontinue AppleTalk support in Cisco IOS Software Releases 15.0(1)M and later. Refer to the following product bulletin for more details:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/product_bulletin_c25-520459.html

Cisco Service Selection Gateway (SSG) Feature Discontinuation

The Cisco Service Selection Gateway (SSG) feature is not supported from Cisco IOS Software Release 15.0(1)M onward. Refer to the following product bulletin for more information:

http://www.cisco.com/en/US/prod/collateral/routers/ps341/end_of_life_notice_c51-501483.html

1.2) Release 15.1(1)T Support Lifecycle Guidelines

Cisco IOS Software Release 15.1(1)T is a Standard Maintenance release. Standard Maintenance releases are positioned for a short deployment cycle (until the next Extended Maintenance release becomes available on Cisco.com).

Release 15.1(1)T will receive bug-fix rebuilds for 13 months, plus an additional 6 months support for security/vulnerability issues such as Product Security Incident Response Team (PSIRT) advisories; visit http://www.cisco.com/en/US/products/products_security_advisories_listing.html for more information.

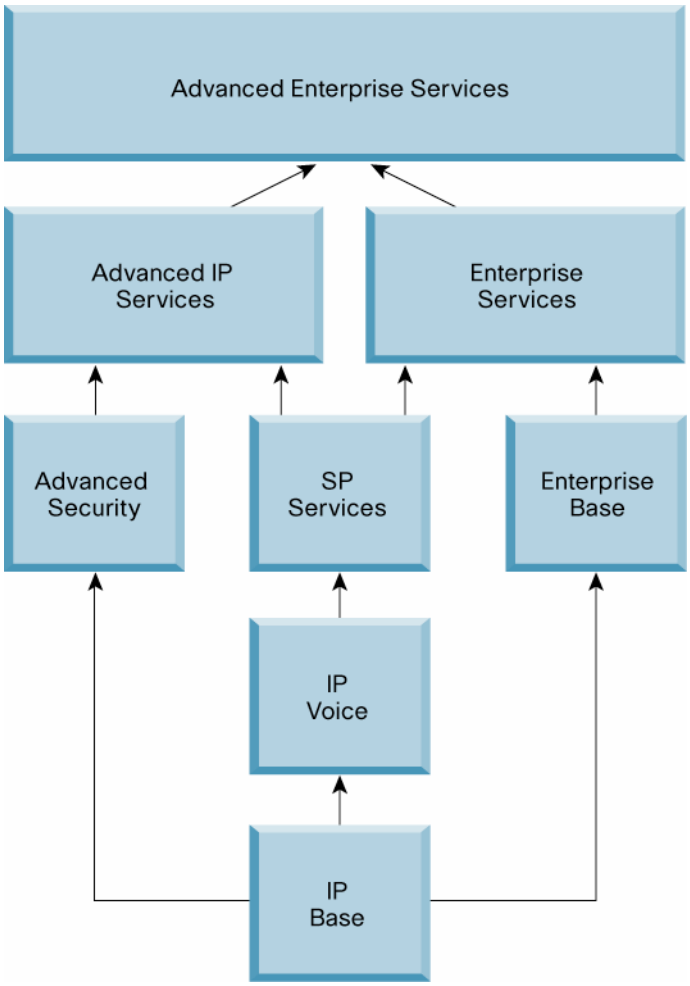
The software support lifecycle for Release 15.1(1)T is illustrated in Figure 3.

Figure 3. Support Lifecycle for Cisco IOS Software Release 15.1(1)T

1.3) Cisco IOS Packaging Consideration

Figure 4 shows the framework for Cisco IOS Packaging for Cisco routers previously supported in Cisco IOS Software Release 12.4T.

Figure 4. Cisco IOS Software Release 15.0(1)M (and Later) Packaging Framework for Cisco Routers Previously Supported in 12.4T *

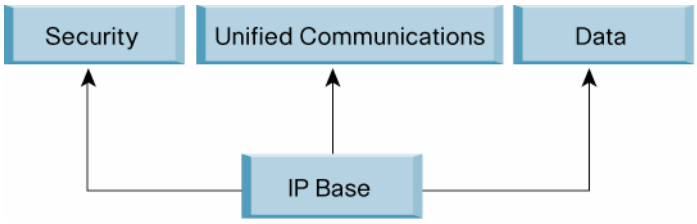


* Hardware-specific feature sets may affect respective Cisco IOS Software package availability. Refer to the Cisco Product and Services support page on Cisco.com to obtain additional information specific to your hardware platform at http://www.cisco.com/en/US/products/index.html. For more information on Cisco IOS Software packaging, visit http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletins_list.html.

Cisco IOS Packaging for Cisco Integrated Services Routers Generation 2

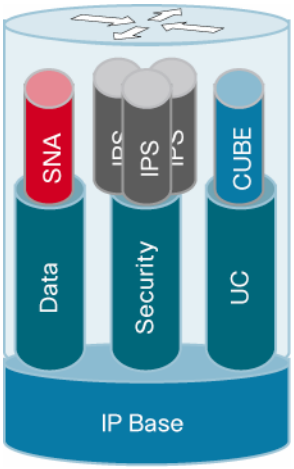
Cisco Integrated Services Routers Generation 2 1900, 2900, and 3900 Series support services on demand through the use of software licensing that enables customers to realize operational savings through ease of software ordering and management. When you order a new ISR G2 platform, the router is shipped with a single universal Cisco IOS Software image and corresponding feature set packages as shown in Figure 5.

Figure 5. Cisco IOS Software Release 15.0(1)M (and Later) Packaging for ISR G2 1900, 2900, and 3900 Series



For more information on Cisco IOS Software packaging for ISR G2, visit http://www.cisco.com/en/US/prod/collateral/routers/ps10616/white_paper_c11_556985.html.

1.4) Cisco IOS Software Activation for Integrated Services Routers Generation 2



Software Activation enables an on-demand service activation model for Cisco ISR G2 and supported network modules with consistent licensing policies and manageability as available on other Cisco Software Activation platforms. Customers will realize operational savings through reduced truck rolls, ease of software ordering, simplified software management, and greater flexibility in deploying new features.

Each ISR G2 will ship with a universal Cisco IOS Software image and will use Software Activation licensing keys to activate Cisco IOS Software functionality. Features ordered with the router will be preactivated at the factory or by your Cisco partner.

For more information on Cisco IOS Software Activation visit http://www.cisco.com/go/sa.

1.5) Cisco IOS IPv6 Repackaging for Integrated Services Routers Generation 2

For years, Cisco IOS Software has expanded support of IP Version 6 (IPv6) to the majority of its technology areas and hardware platforms. Due to market trends, such as available IPv4 address pool exhaustion and regional registries issuing advisories to the Internet community to adopt IPv6 and national mandates, Cisco IOS packaging for IPv6 is now evolving.

Cisco now supports packaging parity for IPv6 with IPv4 for Integrated Services Routers Generation 2 starting with Cisco IOS Software Release 15.0(1)M. Support for IPv6 features for a technology will now be packaged in the same feature set as IPv4 for these platforms.

This new Cisco IOS Software packaging for IPv6 is already available on the following Cisco IOS Software Releases:

- Catalyst® 3700 and 3560 Series images starting with Release 12.2(50)SE
- Catalyst 4500 Series images starting with Release 12.2(52)SG
- Catalyst 6500 Series images starting with Release 12.2(33)SXI

Cisco will expand the package parity effort to additional Cisco IOS Software releases and hardware platforms in the near future.

1.6) Additional Information

- Cisco IOS Software Page

  http://www.cisco.com/go/ios
- Additional details on features in Cisco IOS Software Release 15.1(1)T:

  http://www.cisco.com/en/US/docs/ios/15_1/15_1_1_t/15_1_1_t_newfeatlist.html
- Release notes for Cisco IOS Software

  http://www.cisco.com/cisco/web/psa/default.html
- Cisco IOS Software Download Center

  Download Cisco IOS Software releases and access software upgrade planners.

  http://www.cisco.com/cisco/web/download/index.html
- Cisco Feature Navigator

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

  http://www.cisco.com/go/fn/
- Cisco Software Advisor

  Determine the minimum supported software for selected hardware.

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

New Features in Cisco IOS Software Release 15.1(1)T

Cisco Integrated Services Routers Generation 2: 3945E and 3925E

The new Cisco 3945E and 3925E Series Services Performance Engines (SPE250 and SPE200) offers 4 onboard Gigabit Ethernet ports, 2 Small-Form Factor Pluggable (SFP) ports, 3 EHWIC slots, 3 PVDM slots, up to 1040 watts in power over Ethernet (PoE) boost mode, dual integrated redundant power supplies, and up to 350 Mbps WAN access with services. The Cisco 3945E and 3925E are available with SPE ports preinstalled in the router or are sold separately. The SPE250 and SPE200 provide a modular approach to system upgrades, because you can easily upgrade the SPE on a Cisco 3945 or Cisco 3925 for improved router performance.

The Cisco 3945E and Cisco 3925E provide highly scalable security and Unified Communications (UC)/Cisco Unified Border Element (CUBE) services and offer investment protection for customers who purchase a Cisco 3925 or Cisco 3945 today, providing an upgrade option for higher performance levels in the future when increased bandwidth demands require higher performance levels. See Figure 6.

Figure 6. Cisco Integrated Services Routers Generation 2: 3945E and 3925E

Generation 2 of the Integrated Services Router portfolio consists of three product families similar to the current generation of ISR: the Cisco 1900, 2900, and 3900 Series Integrated Services Routers. From the Cisco 1941 through the Cisco 3945E, the routers in the portfolio provide increasing performance, module slot density, and features to match the needs of diverse branch offices running varying degrees of rich services.

Ethernet Enhancements: 802.1ag–IEEE D8.1 Standard-Compliant Connectivity Fault Management, Y.1731 Multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet

Ethernet Connectivity Fault Management (CFM) is an end-to-end per service instance Ethernet layer operations, administration, and maintenance (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet MANs and WANs.

This feature is the implementation of IEEE 802.1ag Standard-Compliant CFM in Cisco IOS Software.

The following documents provide more information about this feature:

- http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee.html
- Y.1731 Enhancements: http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_y1731.html
- IP SLA for Ethernet: http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html

Benefits of Ethernet CFM

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Easier fault and performance management for Ethernet

Product Management Contact

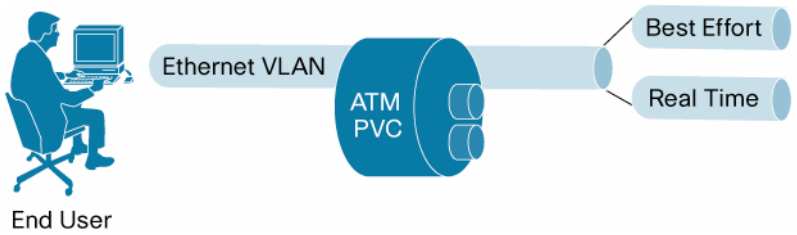
Aseem Srivastava, asesriva@cisco.com

Transporting VLAN Tags over ATM Links

VLAN-Based Service Differentiation over ADSL

VLAN-based service differentiation allows service providers to offer a range of broadband-enabled services and applications to end users. It supports IP connectivity applications that require real-time network performance and applications that use best-effort, or Internet-grade, performance (Figure 7).

Figure 7. VLAN-Based Service Differentiation at PVC Level



Benefits of the Transporting VLAN Tags over DSL Links Feature

This feature offers the following benefits:

- Customer premises equipment (CPE) to carry traffic with provider-specific 802.1Q tags.
- Deployment of voice, video, and data services at customer premises: This service combination offers a real-time channel dedicated to voice over IP (VoIP) traffic and a second channel that delivers best-effort Internet service.

Additional Information

You can find additional information at http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_trans_vlan-tags_dsl_links.html.

Product Management Contact

Aseem Srivastava, asesriva@cisco.com

Smart Call Home Support on ISR

A Proactive, Smart Service Capability of Cisco SMARTnet Service for the ISR Family

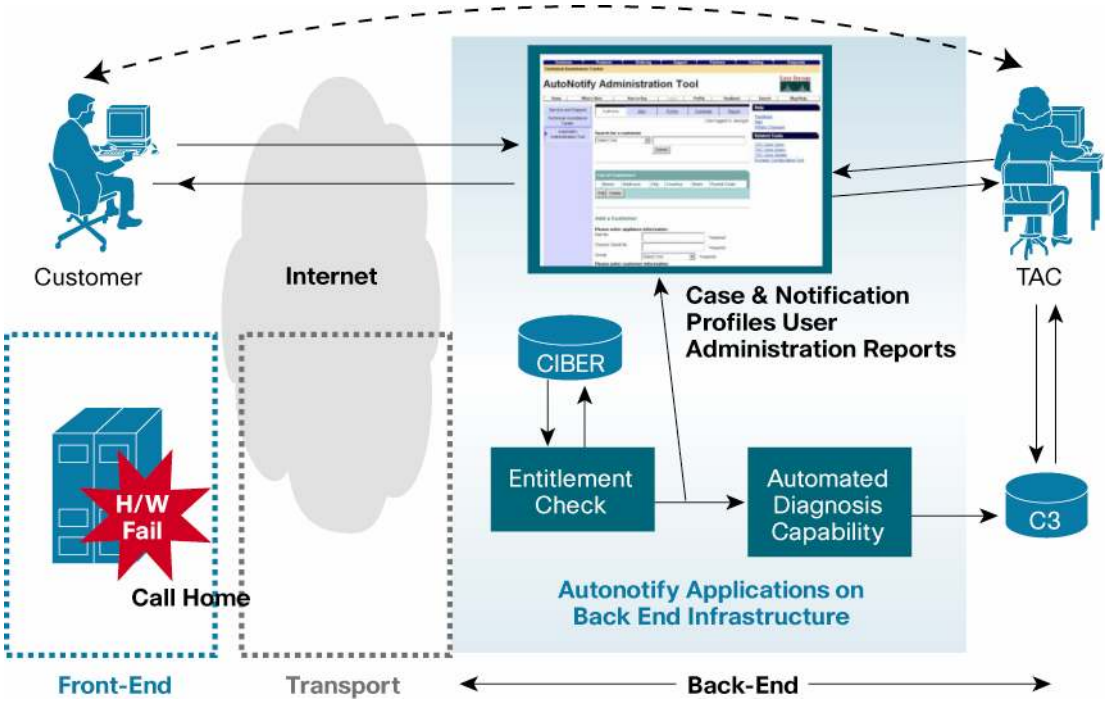
Cisco Smart Call Home is an award-winning, embedded support feature of Cisco SMARTnet® and Cisco SP Base, available at no additional cost for ISR customers (Figure 8).

Smart Call Home can help speed issue resolution by sending proactive, real-time alerts to your operations team with detailed diagnostic information and even remediation recommendations based on Cisco best practices.

Cisco Smart Call Home provides the following:

- Higher availability through proactive, fast issue resolution
- Increased operational efficiency through less time troubleshooting
- Quick and convenient web-based access to personalized information

Figure 8. Smart Call Home Support on ISR Topology



Device can generate call home messages that are encrypted and transmitted to the Smart Call Home Interactive Technical Services system. The system inspects and analyzes the message, assesses the severity of the issue, and activates the appropriate notification sequence based on the profile you have set up.

When you set up Smart Call Home, you can specify whom you want to be notified, how you want messages transported, and for what types of events you want to receive alerts. If you choose to allow Smart Call Home to send configuration information, sensitive details such as passwords and community strings are removed to protect your network privacy. Smart Call Home also provides you with access to a Smart Call Home web portal that contains personalized call home messages, recommendations, and additional up-to-date information for your call home devices.

Additional Information

You can obtain additional information at http://www.cisco.com/en/US/products/ps7334/serv_home.html.

Product Management Contact

Aseem Srivastava, asesriva@cisco.com

Voice Feature Enhancements

SG3 Fax Support on Cisco TDM-IP Voice Gateways

Fax remains a key component of communication between businesses. This feature provides support for V.34 fax relay based on the ITU Specification T.38 version 3 (04/2007) and for fax pass-through at SG3 speed. Prior to this release, SG3-to-SG3 calls would fail because the V.34 modulation was not supported. A fallback solution allowed SG3-to-SG3 connections to be made, but the transmission speed was set to G3 levels. The new SG3 fax feature allows for fax connection speed up to 33.6 kbps on Cisco TDM-IP voice gateways.

SG3 fax helps customers reduce costs and improve productivity with almost twice the fax connection speed and better error correction.

Cisco Unified Border Element (CUBE) 1.4

Cisco Unified Border Element continues to add numerous new capabilities in each Cisco IOS Software release to increase the capabilities it brings to enterprise networks as a session border controller. CUBE 1.4 provides new features including:

- **Operational:** SIP Options PING enhancement enables the customer to customize the error return code when the SIP trunk is down. This enables new call rerouting capabilities for the enterprise call agents.
- Management: SNMP MIB enhancements report SIP trunk utilization, call arrival rate information, and DSP utilization and active sessions for transcoding and MTP applications.
- **Interoperability:** RTP payload interworking supports configuration of different payload types for codecs, DTMF relay and fax on either side of CUBE—and converting between these values. This enables interoperability between applications and networks that assign different payload types to the same service. ISAC codec support is also introduced with CUBE 1.4.
- **SIP interworking:** Several SIP 183 and 181 message enhancements allow better interoperability with Intrado 911 call services, Microsoft OCS and Avaya PBXs.
- **Platforms:** CUBE 1.4 feature support for Cisco Integrated Services Routers Generation 2 2900, 3900, and 3900E series platforms.

A session border controller such as CUBE is critical for enterprises to connect seamlessly and securely to service provider SIP trunks for public switched telephone network (PSTN) access as well as to help overcome interoperability issues between disparate enterprise applications.

Cisco Unified Communications Manager Express (CME) 8.0

Cisco Unified Communications Manager Express adds new capabilities in the areas of endpoint enhancements, application integration, and security enhancements. CME 8.0 provides the following new features:

- Support for new Cisco Unified IP Phone 6901/6911/6921/6941/6961
- Skinny Client Control Protocol (SCCP)/SIP endpoint support for IPv6
- Enhanced music-on-hold (MOH) with support for up to five MOH streams
- Enhanced security with support for logical class of restriction (LPCOR) partitioning
- Industry-standard computer telephony integration (CTI) interface for third-party call control
- Department of Defense functionality:
  - Secure device support, IP-STE
  - Multilevel precedence and preemption (MLPP)

Product Management Contact

Tony Huynh, tonhuynh@cisco.com

Unified Survivable Remote Site Telephony 8.0

Unified Survivable Remote Site Telephony (SRST) 8.0 adds new capabilities in the areas of endpoint and security enhancements:

- Support for new Cisco Unified IP Phone 6901/6911/6921/6941/6961
- Secure SIP SRST support with endpoint registration through TLS; media encryption with secure RTP
- Enhanced music-on-hold with support for up to five MOH streams

Additional Information

For more information, visit http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srs_map.html.

Product Management Contact

Hanlin Fang, hfang@cisco.com

Web Services Management Agent with TLS

The Web Services Management Agent (WSMA) defines a mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. WSMA uses Extensible Markup Language (XML)–based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages. Multiple WSMA clients can connect to the WSMA server running on Cisco IOS Software. Currently, WSMA operates in listener mode, in which connections are initiated by external applications, and supports Secure Shell Protocol Version 2 (SSHv2), HTTP, or HTTPS transports.

The WSMA with TLS feature (Figure 9) adds Transport Layer Security (TLS), a cryptographic protocol, as another transport protocol for WSMA. Adding initiator mode to WSMA is very critical in deployment scenarios where the devices are in a Network Address Translation (NAT) environment or behind a firewall and in Zero Touch Deployment models where the device needs to initiate connection to external servers. WSMA with TLS adds the additional security needed for WSMA initiator mode.

The capabilities of the WSMA with TLS feature include:

- TLS 1.0/SSL 3.0 as transport protocol for WSMA
- ITU-T's X.509 standard for defining digital certificates
- WSMA in initiator and listener modes over TLS
- WSMA in initiator mode over SSH, HTTPS, and HTTP
- Configurable TLS port numbers
- User authentication and authorization using WSSE SOAP headers

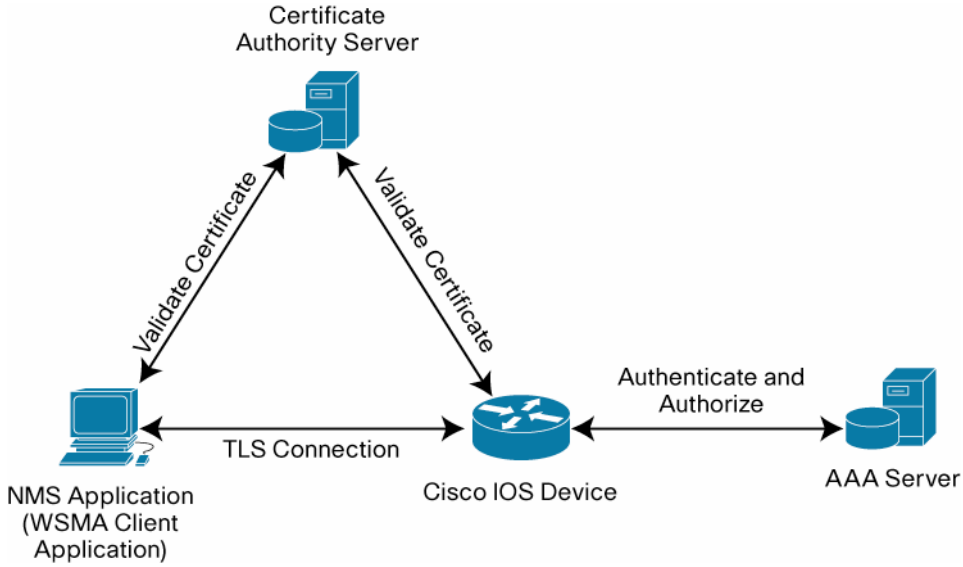
Cisco continues to invest and innovate in building features to facilitate manageability of Cisco products using open standards. The WSMA with TLS feature provides network management system (NMS) applications the ability to communicate to Cisco products over both trusted and untrusted networks. With WSMA initiator mode, this feature enables the deployment models that were not possible before.

Benefits

Key advantages to using WSMA with TLS include:

- Validation of NMS applications using digital certificates
- Prevent "man in the middle" security attacks when WSMA is in initiator mode
- Support Zero Touch Deployment models
- Support manageability of devices with WSMA when the devices are in NAT setup or behind a firewall
- Scalable model with less memory requirements compared to SSH
- Embedded in most Cisco IOS devices

Figure 9. WSMA with TLS Deployment Diagram



Additional Information

For additional information, visit http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma.html.

Product Management Contacts

Sunil Gudurvalmiki, sunilgv@cisco.com

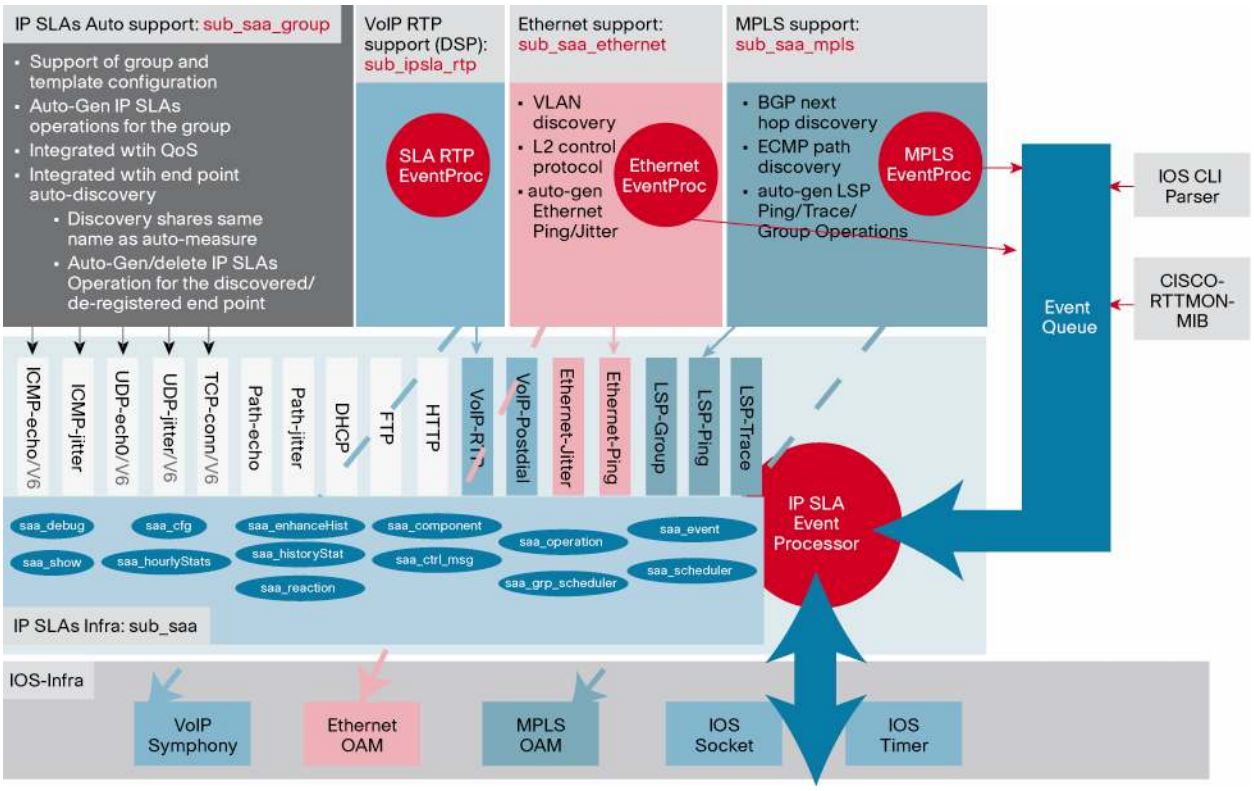
IPSLA Engine 3

IPSLA is the industry-leading performance and monitoring feature built into Cisco IOS Software for service-level monitoring and management. IP SLA actively generates synthetic traffic from within the router or switch to exactly mimic the experience of users in the network. With IP SLA, you can monitor and control service Levels within your organization without additional hardware or probes.

IP SLA Engine 3 extends existing IPSLA capabilities to make it easier to use and more powerful than ever. See Figure 10. New capabilities include:

- Template-based based configuration
- Simplified command-line interface (CLI) user experience
- Automatic endpoint provisioning
- Advanced scheduling
- Hierarchical performance monitoring
- QoS Integration

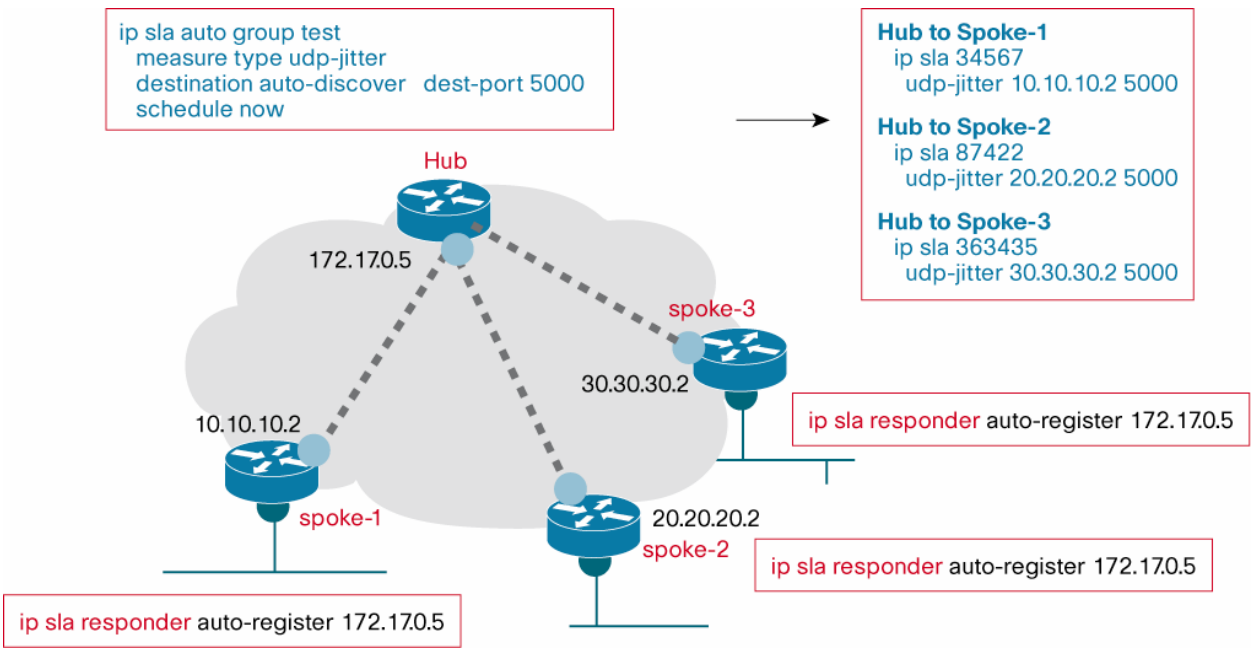
Figure 10. IPSLA Engine 3 Architectural Design



Auto-IPSLA

With IPSLA Engine 3, Cisco announces a new way to simplify and modularize IPSLA provisioning and configuration. Auto-IPSLA provides discovery and template-based configuration to reduce the complexity and improve the accuracy of deploying large IP SLA networks. With Auto-IPSLA, endpoint IPSLA responders can be automatically discovered and configured using a new feature called Endpoint Auto Registration (Figure 11).

Figure 11. Auto-IPSLA Endpoint Registration



Backward Compatibility

Cisco continues to innovate and build around IPSLA capabilities in a fully backward-compatible way that adds new powerful capabilities while preserving existing investment in IPSLA applications and systems.

Benefits

Key Advantages to using IPSLA Engine 3 include:

- Advanced SLA monitoring and management
- Template-based configuration; configure once, use many
- Automatic endpoint auto-registration and discovery
- Seventeen synthetic probes, from User Datagram Protocol (UDP) jitter to Dynamic Host Configuration Protocol (DHCP) and HTTP
- Integrated with EEM (Embedded Event Manager) automation and programming
- Embedded in most Cisco IOS devices
- Consistent feature sets
- Highly scalable
- High performance, supports thousands of operations per second

Additional Information

For more information, visit http://www.cisco.com/go/ipsla.

Product Management Contacts

Steve Giles. stgiles@cisco.com, and Tracy Jiang, jiangy@cisco.com

Direct IPS Signature Update Package Downloads from Cisco.com

This enhancement within the Cisco IOS Software IPS feature allows customers to download signature update packages directly from the Cisco.com location those packages are posted to by the Cisco Signature Team.

The router can be configured for periodic downloads (if there is an updated package) from Cisco.com with a valid username and password. It will be also possible to use this enhancement for (single) one-time downloads using an EXEC command on the router.

The enhancement eliminates the need for a local HTTP/FTP/TFTP server on which the customer has to download the latest signature package from Cisco.com manually and then download it to the router (from a server).

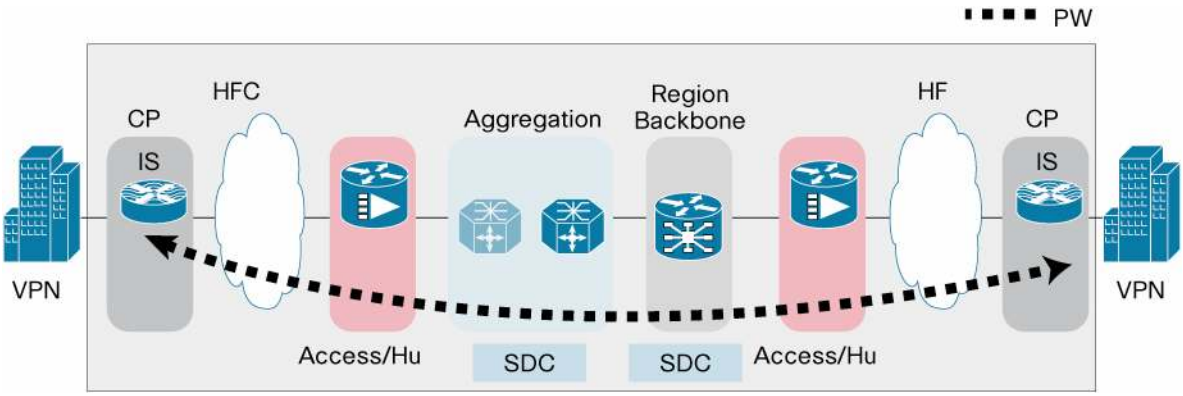
Product Management Contacts

Kemal Akozer, kemal@cisco.com

MPLS MTU over GRE Tunnels

An increasing number of Cisco cable MSO ((Multiple System Operator) customers are starting to offer business services over their existing DOCSIS/HFC access infrastructure. Cisco’s Cable Converged and Commercial Solution CESNA 3.x defines a target architecture for delivering Layer 2 VPN Ethernet Services over DOCSIS CPE–based VPNs, which include E-LINE and E-LAN services. These VPN services are being implemented using MPLS Pseudowire encapsulation of Ethernet traffic, which, in turn, is encapsulated into GRE tunnels.

Figure 12. Layer 2 VPNs over GRE Tunnels in Cisco's CESNA Solution



The DOCSIS 2.0 cable network infrastructure standard imposes a 1500-byte maximum transmission unit (MTU) limit on the User Network Interface (UNI), which connects CPE to the operator's CMTS access system. Currently the MPLS MTU limit on the MPLS-enabled GRE (UNI) interface is forced to 1500 bytes due to the 1500-MTU limit of the underlying interface. Since Ethernet frames can range up to 1518 bytes, EoMPLSoGRE Pseudowire encapsulation of these frames can result in packets that exceed the underlying 1500-MTU limit, which will result in packet loss.

A new configurable MPLS MTU command is available now for GRE tunnels, which allows the MTU packet size to be set to at least the maximum size of MPLS/PW-encapsulated Ethernet packets. The increased MPLS MTU size will prevent potential EoMPLS packet drops across the CPU uplink to the operator's CMTS system. The net result will be that fragmentation and defragmentation of EoMPLSoGRE packets will take place only at the link/UNI interface layer.

Benefits

- **Flexibility and customization:** The user has the ability now to configure a specific MPLS MTU size for Layer 2 VPN traffic over GRE tunnels at the link/UNI interface layer, connecting CPE to the cable network.
- **Prevention of packet loss:** The configurable MPLS MTU size for GRE tunnels allows for increasing the MTU size for MPLS packets carried over GRE tunnels, independently of the MTU size of the underlying physical interfaces, and this way any potential packet loss can be prevented.

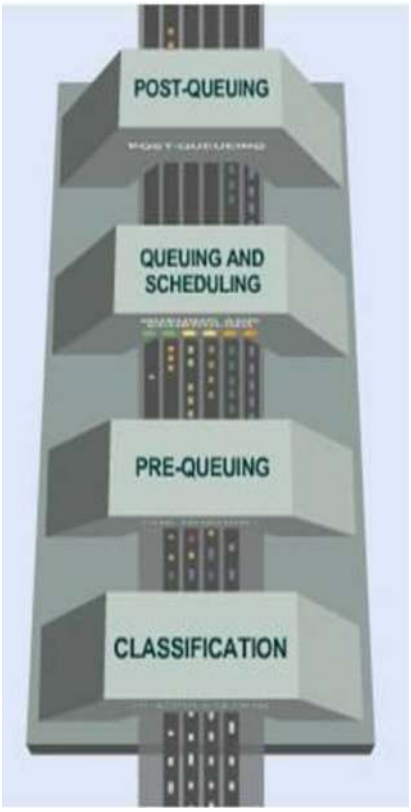
Product Management Contact

Harmen van der Linde, havander@cisco.com

Switch Virtual Interface for Integrated Services Router Platforms

Switch Virtual Interface (SVI) on Cisco Integrated Services Routers is designed to provide basic Layer 3 functions for the Layer 2 switch ports that belong to a specific VLAN. The SVI does not provide the same feature set and functions as the integrated Layer 3 Ethernet ports of the integrated services routers and should not be used to entirely replace the Layer 3 Ethernet ports. See Figure 13.

Figure 13. Switch Virtual Interface Support



Product Management Contact

Francois-Xavier Mateo, fmateo@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 C25-603193-00 05/10