Product Bulletin No. 3286

Cisco IOS XR Software Release 3.3

PRODUCT OVERVIEW

Cisco IOS® XR Software Release 3.3 for the Cisco® CRS-1 Carrier Routing System and Cisco XR 12000 Series Routers supports private VPN services, helping service providers to offer highly available business services. Release 3.3 delivers the advantages of point-of-presence (POP) consolidation and service separation for direct Internet, private voice, and VPN services through the use of the Cisco Service Separation Architecture. This release extends Cisco IOS XR Software capabilities to the service provider edge by supporting IPv4 Multiprotocol Label Switching (MPLS) VPNs. It also brings Session Border Controller capability to the Cisco XR 12000 Routers through software support.

Cisco IOS XR Software Release 3.3 includes the same features and support of Release 3.2 and prior. Complete documentation for this release is available on CCO at: http://www.cisco.com/univercd/cc/td/doc/product/ioxsoft/iox33/index.htm.

NEW FEATURES

Hardware Support

Cisco IOS XR Software Release 3.3 incorporates support for new hardware, listed in Table 1 and Table 2.

Table 1. New Cisco CRS-1 Hardware Supported

Product Number	Description
4-10GE-ITU/C	ITU grid 4 x 10-GE PLIM C-band
1OC768-ITU/C	ITU grid 40-Gbps PLIM C-band
SPA-8XOC12-POS	8-port Packet over SONET OC-12c/STM-4 and OC-3c/STM-1 shared port adapter
CRS-DRP	Cisco CRS-1 distributed route processor
CRS-16-RP-B	Cisco CRS-1 16-slot route processor, version B

Table 2. New Cisco XR 12000 Series Hardware Supported

Product Number	Description
12000-SIP-601	Multirate 10G IP service engine (modular)
12000-SIP-501	Multirate 5G IP service engine (modular)
12000-SIP-401	Multirate 2.5G IP service engine (modular)
XR-12000/16	Cisco XR 12000 Series 16-slot router
XR-12000/10	Cisco XR 12000 Series 10-slot router
XR-12000/6	Cisco XR 12000 Series 6-slot router
XR-12000/4	Cisco XR 12000 Series 4-slot router
SPA-2XCT3	2-port channelized T3 to DS-0 shared port adapter
SPA-4XCT3	4-port channelized T3 to DS-0 shared port adapter
SPA-2XT3/E3	2-port clear channel T3/E3 shared port adapter
SPA-4XT3/E3	4-port clear channel T3/E3 shared port adapter

Product Number	Description
SPA-2XOC48POS	2-port clear channel OC-48/STM-16 shared port adapter

Software Features

Cisco IOS XR Software Release 3.3 incorporates all the software features supported in Cisco IOS XR Software Release 3.2 and adds support for new features, listed in Table 3.

Table 3. New Software Features for Cisco CRS-1 Systems and Cisco XR 12000 Series Routers

Feature	Description
MPLS VPNs	MPLS VPNs allow a Cisco IOS network to support scalable IPv4 Layer 3 VPN backbone services. VPNs are the foundation for deploying and administering value-added application and data services, and telephony services to business customers. RFC2547 MPLS VPNs offer the following benefits: • A platform for rapid deployment of additional value-added IP services, including intranets, voice, multimedia, and network commerce. • Privacy and security by limiting the distribution of VPN routes to only those routers that are members of the VPN • Easy integration with customer intranets • Scalability of thousands of VPNs, thousands of sites per VPN, and hundreds of thousands of VPNs per service provider IP class of service (CoS), with support for multiple classes of service and priorities within and between VPNs The following features are supported in Release 3.3: • Multiprotocol BGP (MP-BGP) extension to support VPNv4 • Customer edge-provider protocols ◦ Static ◦ External BGP (eBGP) ◦ Routing Information Protocol Version 2 (RIPv2) ◦ Enhanced Interior Gateway Protocol (EIGRP) ◦ Open Shortest Path First Version 2 (OSPFv2) • MPLS Transport based on Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP), and Traffic Engineering (TE) • Per CE/Per Prefix Label Distribution • eBGP Multipath • Autoroute Descriptor Support • VPN Nonstop Forwarding (NSF) • VPNv4 Route Reflector • Distributed BGP
MPLS OAM	Provides MPLS label switched path (LSP) verification commands, which allow you to detect and diagnose data plane failures. These represent the first set of commands in the MPLS Operations, Administration, and Maintenance (OAM) solution.
Border Gateway Protocol Next-Hop Tracking	Lets you specify the delay for triggering next-hop calculations. It allows for a dynamic way (depending on the size and behavior of the network) for Interior Gateway Protocol (IGP) to converge so that BGP can accumulate all notifications and trigger less walks, resulting in fewer interprocess communication connections (IPCs) to routing information base (RIB) for route addition, deletion, or modification, and also less updates to peers.
Generalized MPLS Traffic Engineering	Generalized MPLS Traffic Engineering (GMPLS-TE) consists of extensions to the MPLS-TE mechanisms to control a variety of device types, including optical switches. When GMPLS-TE is used to control a hierarchical optical network – a network with a core of optical switches surrounded by outer layers of routers – it can provide unified control of devices that have very different hardware capabilities. Other control-plane solutions for such network architectures typically use an overlay model, using separate control planes to manage the optical core and the routed network, respectively, with little or no knowledge passing between them. GMPLS-TE protocols and extensions include: Resource Reservation Protocol (RSVP) for signaling, Interior Gateway Protocols (IGPs) such as Open Shortest Path First (OSPF), and Link Management Protocol (LMP) for managing link information.
Multicast Enhancements	Multicast routing technology provides support for: • IPv6 Boot Strap Router (BSR) • Equal-cost multipath (ECMP) load balancing using both S and G fields • Internet Group Management Protocol Version 3 (IGMPv3) MIB • Multicast Source Discovery Protocol (MSDP) MD5 • MSDP MIB • PIM RPF Vector (draft-ietf-pim-rpf-vector-02.txt)

Feature	Description
OSPF Loop Prevention	When Open Shortest Path First (OSPF) Version 2 is used as the provider edge-customer edge (PE-CE) protocol, BGP carries the OSPF route information in the backbone. Some of the information needed to prevent loops may be lost during this process. Draft-ietf-ospf-2547-dnbit-04.txt defines a procedure to prevent looping by using one of the options bits in the link-state advertisement (LSA).
VRRP	Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol between multiple routers that provides the appearance of a single router on the LAN segment. The routers share the same virtual IP and MAC addresses on the LAN segment, therefore, in the event of failure of one router, the hosts on the LAN are able to continue forwarding packets to a consistent IP and MAC address. The process of transferring the routing responsibilities from one device to another is transparent to the user.
MPLS Differentiated Services-Aware Traffic Engineering with Maximum Allocation Model	MPLS Differentiated Services (DiffServ)-Aware Traffic Engineering (TE) is an extension of the regular MPLS-TE feature. Regular TE does not provide bandwidth guarantees to different traffic classes. A single bandwidth constraint is used in regular TE that is shared by all traffic. To support various classes of service, users can configure multiple bandwidth constraints. These bandwidth constraints can be treated differently based on the requirement for the traffic class using that constraint. MPLS DiffServ TE provides the ability to configure multiple bandwidth constraints on an MPLS-enabled interface. Available bandwidths from all configured bandwidth constraints are advertised using IGP. The TE tunnel is configured with bandwidth-value and class-type requirements. Path calculation and admission control take the bandwidth and class type into consideration. RSVP is used to signal the TE tunnel with bandwidth and class-type requirements. DiffServ TE can be deployed with either Russian Doll Model (RDM) or Maximum Allocation Model (MAM) for bandwidth calculations.
LDP Session Protection	This feature lets you configure Label Distribution Protocol (LDP) to automatically protect sessions with all or a given set of peers. When configured, LDP initiates backup targeted hellos automatically for neighbors for which primary link adjacencies already exist. These backup targeted hellos maintain LDP sessions when primary link adjacencies go down.
Inbound Label Filtering for LDP	Provides the ability to filter remote bindings for a defined set of prefixes.
LDP Local Label Allocation	By default, LDP allocates local labels for all prefixes that are not Border Gateway Protocol (BGP) prefixes. This is acceptable when LDP is used for applications other than Layer 3 VPN core transport. When LDP is used to set up transport LSPs for Layer 3 VPN traffic in the core, it is not efficient or even necessary to allocate and advertise local labels for potentially thousands of IGP prefixes. In such an instance, LDP is typically required to allocate and advertise local label for Loopback/32 addresses for provider-edge routers. This is accomplished using LDP local label allocation control, where an access list can be used to limit allocation of local labels to a set of prefixes. Limiting local label allocation provides several benefits, including reduced memory usage requirements, fewer local forwarding updates, and fewer network and peer updates.
LDP IGP Synchronization	This feature lets you synchronize LDP and Interior Gateway Protocol (IGP) to advertise links with regular metrics only when MPLS LDP is converged on that link. LDP considers a link converged when at least one LDP session is up and running on the link for which LDP has sent its applicable label bindings and received at least one label binding from the peer. LDP communicates this information to IGP upon link-up or session-down events and IGP acts accordingly, depending on sync state.
Keychain Management	Keychain management is a common method of authentication that lets you configure shared secrets on all entities to exchange secrets before establishing trust with each other. Routing protocols and network management applications on Cisco IOS XR Software often use authentication to enhance security while communicating with peers.
Fault Manager	Cisco IOS Embedded Event Manager (EEM) TCL script works with AAA/task ID model. To register a Fault Manager policy, you must specify the username that is used to run the script. This name can be different from the user who is currently logged in, but the registering user must have permissions that are a superset of the username that will run the script. Otherwise, the script is not registered and the command may be rejected. In addition, the username that will run the script must have access privileges to the commands run by the Fault Manager policy being registered.
Cisco IOS IP Service-Level Agreements	This originated from the technology previously known as Service Assurance Agent (SAA). IP SLA performs active monitoring by generating and analyzing traffic to measure performance, either between the router or from a router to a remote IP device such as a network application server. Measurement statistics (provided by IP SLA operations) are used for troubleshooting, problem analysis, and designing network topologies.
Cisco Craft Works Interface (CWI) Improvements	Improvements include: • Enhanced configuration editor with IDE functionality • Hyperlinks to referenced portions of configuration • Route policy language (RPL) syntax highlighting • Simplified installation from a router or HTTP server • Support for new inventory schema
Cisco Service Separation Architecture	This release supports the Cisco Service Separation Architecture (SSA) for the complete physical separation of network and system resources between each Secure Domain Router instance on the Cisco CRS-1 and Cisco XR 12000 Series chassis. This SSA allows service providers to consolidate multiple networks and services onto a single, “virtualized” platform while keeping each network and service instance separate and secure. The Secure Domain Routers are defined by a route processor (and standby if needed) and a configurable group of line card slots. The logical routing instances are segmented on line-card-slot boundaries to maximize service separation and isolation.

Cisco IOS XR Software Release 3.3 incorporates all software features supported in Release 3.2 and adds support for new features on Cisco CRS-1 systems, listed in Table 4.

Table 4. Additional New Software Features for Cisco CRS-1 Systems

Feature	Description
Link Bundling (VLAN/LDP)	802.1Q VLAN subinterfaces can be configured on 802.3ad Ethernet link bundles.
MAC counting (on existing 10-GE PLIMs)	On an existing 10-GE physical layer interface module (PLIM), the MAC address accounting feature provides accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces. This feature calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a time stamp for the last packet received or sent.
LDP ether-bundle	Provides new interface-media support over ether-bundle interfaces.
Packet Length Filter	Enables packet classification and filtering based on the Layer 3 packet length in the IP header. This is supported on all interfaces and in any direction, ingress or egress.
BFD over VLAN over ether-bundles	When running a Bidirectional Forwarding Detection (BFD) session on an interface, the BFD session is active as long as the VLAN bundle is up. As long as the VLAN bundle is active, the following events do not cause the BFD session to fail: • Failure of a component link: Fiber unplugged • Online insertion and removal (OIR) of a line card that hosts one or more of the component links • Addition of a component link (by configuration) to the bundle • Removal of a component link (by configuration) from the bundle • Shutdown of a component link • RP failover
1:1 redundancy over link bundles	For 1:1 redundancy, you can configure the minimum number of active links using the **bundle minimum-active links** command. To support the 1:N redundancy feature, you can configure the minimum bandwidth in kbps using the bundle **minimum-active** links command.
QoS support on Cisco CRS-1 fabric	Provides support for fabric quality of service (QoS).
QoS support for VLANs over bundles	Supports QoS over VLANs over bundles.
Sampled NetFlow support over VLANs	Extends the IPv4 Sampled NetFlow support to VLANs.

Cisco IOS XR Software Release 3.3 incorporates all software features supported in Release 3.2 and adds support for new features on Cisco XR 12000 Series Routers, listed in Table 5.

Table 5. Additional Software Features for Cisco XR 12000 Series Routers

Feature	Description
QoS Enhancements	Support for To-Fab QoS, dynamic queue allocation, hierarchical queuing, label sharing, and class map scalability.
IPv6 Multicast	Support for IPv6 multicast.
Multicast QoS	Cisco IOS XR Software provides for the configuration of multicast QoS. When configured on specific interfaces, systemwide, general QoS operations are applied to multicast traffic as well as general network traffic. QoS expedites the processing of mission-critical applications, while sharing network resources with noncritical applications. QoS also ensures available bandwidth and minimum delays required by time-sensitive multimedia and voice applications. It also gives network managers control over network applications, improves cost efficiency of WAN connections, and enables advanced differentiated services.
Sampled NetFlow for IPv4	Support for NetFlow data collection in sampled mode. Sampled NetFlow provides configurable sampling rates that help ensure accuracy and allow the user to control the consumption of router resources.
Local Packet Transport Services (LPTS)	Support for protection of locally sourced traffic, including rate limiting of control plane traffic, peer filtering (TCP/UDP unicast), and packet priority for egress and ingress traffic to the route processor.
Unicast Reverse Path Forwarding (URPF) support	URPF aids in the prevention and mitigation of network attacks by limiting an attacker's ability to spoof source IP addresses of network packets. E3 and E5 engines support IPv4 URPF in Loose Mode. For IPv6, E3 supports Loose Mode and E5 supports Strict Mode.

Feature	Description
MPLS VPN InterAS	MPLS VPN Interautonomous System (InterAS) enables a VPN service provider network to exchange IPv4 routes with MPLS labels. Using InterAS, a local provider edge (PE) router needs to know the routes and label information for the remote PE router. This information can be exchanged between the PE routers and autonomous system boundary routers (ASBRs) in one of two ways: • **Internal Gateway Protocol (IGP) and Label Distribution Protocol (LDP):** The ASBR can redistribute the IPv4 routes and MPLS labels that it learned from eBGP into IGP and LDP and conversely. • **Internal Border Gateway Protocol (iBGP) IPv4 label distribution**: The ASBR and PE router can use direct iBGP sessions to exchange VPNv4 and IPv4 routes and MPLS labels. Using BGP to distribute IPv4 routes and MPLS label routes has the following benefits: • Improved scalability because the route reflectors store VPNv4 routes • Ability to enable a non-VPN core network to act as a transit network for VPN traffic • Elimination of the need for any other LDP between adjacent label switch routers (LSRs)
Session Border Controller	Basic software support for data border element (DBE) and signaling border element (SBE) capabilities for Session Initiation Protocol (SIP) back-to-back user agent (B2BUA). H.323 with Network Address Port Translator (NAPT) traversal and media bridging. Service control interface support via H.248.

ORDERING INFORMATION

Table 6 lists the software versions and applicable ordering information for Cisco IOS XR Software Release 3.3 for the Cisco CRS-1 Carrier Routing System and Cisco XR 12000 Series Routers.

These are the only part numbers that will be orderable. When re-releases of Cisco IOS XR Software Release 3.3 are available, ordering these part numbers will automatically result in the latest re-release being shipped.

Table 6. Software Versions and Ordering Information

Part Number	Description
XC-RP-03.03	Cisco CRS-1, all packages except cryptographic support
XC-RPK9-03.03	Cisco CRS-1, all packages with cryptographic support
XC-XR12K-03.03	Cisco XR 12000 Series Router, all packages except cryptographic support
XC-XR12KK9-03.03	Cisco XR 12000 Series Router, all packages with cryptographic support

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C25-351060-00 05/06