Release Notes for Cisco NCS 5000 Series Routers, IOS XR Release 6.5.1

Revised: June 9, 2023

Network Convergence System 5000 Series Routers

Note *This software release has reached end-of-life status. For more information, see the* End-of-Life and End-of-Sale Notices.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Release 6.5.1 Packages

This table lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames.

Table 1: Release 6.5.1 Packages for Cisco NCS 5000 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5k-mini-x.iso	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image • Alarm co-relation
Individually-Installable Optional Packages		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs5k-mgbl-3.0.0.0-r651.x86_64..rpm	XML, Parser, HTTP Server, Telemetry, and gRPC.

Cisco IOS XR MPLS Package	ncs5k-mpls-3.1.0.0-r651.x86_64.rpm	Label Distribution Protocol (LDP), MPLS forwarding , MPLS operations , Administration and maintenance (OAM), Layer3-vpn , layer-2 vpn.
Cisco IOS XR MPLS RSVP TE package	ncs5k-mpls-te-rsvp-1.1.0.0-r651.x86_64.rpm	Supports MPLS RSVP-TE (Resource Reservation Protocol with Traffic Engineering extensions)
Cisco IOS XR Security Package	ncs5k-k9sec-3.2.0.0-r651.x86_64.rpm	Support for Encryption, Decryption, and Secure Shell (SSH),
Cisco IOS XR Multicast Package	ncs5k-mcast-2.2.0.0-r651.x86_64.rpm	Multicast routing protocols (PIM, IGMP, Auto-rp, BSR) and infrastructure (Multicast routing information Base) , Multicast forwarding (mfwd)
Cisco IOS XR ISIS package	ncs5k-isis-2.2.0.0-r651.x86_64.rpm	Supports ISIS
Cisco IOS XR OSPF package	ncs5k-ospf-2.0.0.0-r651.x86_64.rpm	Supports OSPF

Supported Packages and System Requirement

Supported Hardware

For a complete list of supported optics, hardware and ordering information for NCS 5001 and NCS 5002 series router, see the *Cisco NCS 5000 Series Data Sheet*

For a complete list of supported optics, hardware and ordering information for NCS 5011 router, see the *Cisco NCS 5011 Series Data Sheet*

To install the Cisco NCS 5000 series routers, see *Hardware Installation Guide for Cisco NCS 5000 Series Routers*.

Software Features Introduced in this Release

Bridge Virtual Interface on VRF

Bridge Virtual Interface (BVI) on VRF feature enables VRF support on BVI when the BVI is part of the bridge domain that is configured with Layer 2 main interfaces and Layer 2 single-tagged sub-interfaces with rewrites. BVI is a virtual interface that is defined with Integrated Routing and Bridging (IRB).

BGP Session Authentication and Integrity using TCP Authentication Option

BGP Session Authentication and Integrity using TCP Authentication Option feature enables you to use stronger message authentication codes that protect against replays, even for long-lived TCP connections.

It supports current infrastructure uses of TCP MD5, such as to protect long-lived connections, for example, as used in BGP. This feature supports a larger set of message authentication codes with minimal other system and operational changes.

This feature is compatible with both a static Master Key Tuple (MKT) configuration or an external, out-of-band MKT management mechanism. In either case, using traffic keys derived from the MKT, this feature also protects connections when using the same MKT across repeated instances of a connection, and it coordinates MKT changes between endpoints.

For more informnation about the feature, see the chapter *Implementing BGP* in the *BGP Configuration Guide for Cisco NCS 5000 Series Routers, IOS XR Release 6.5.x*.

Ingress ACL Over BVI

Access lists perform packet filtering to control which packets move through the network and where. An access control list (ACL) consists of one or more access control entries (ACE) that collectively define the network traffic profile.

Bridge Virtual Interfaces (BVIs) provide a bridge between the routing and bridging domains on a router. A BVI is configured with an IP address and operates as a regular routed interface. You can configure an ACL on a BVI to filter the traffic for the network that uses the interface.

Prior to Release 6.5.1, ACLs could be applied only on the bridge domain interfaces. Therefore, both L2 and L3 traffic was filtered based on the ACLs applied on bridge domain interfaces. The feature ACL over BVI allows you to configure ACL on the BVI interfaces in the IRB domain. Thereby, only L3 traffic flows are filtered based on the ACLs applied on BVI interfaces. This helps in filtering the traffic flows towards the core-network and overall performance of the network improves.

For more information about the feature, see the chapter *Ingress ACL over BVI* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*

Unicast Reverse Path Forwarding

Configuration of Unicast IPv4 and IPv6 Reverse Path Forwarding (uRPF) enables a router to verify the reachability of the source addresses, in the packets being forwarded. Configuring uRPF, both strict and loose modes, helps to mitigate problems caused by the introduction of spoofed IP source addresses into a network. Configuration of uRPF discards IP packets that lack a verifiable IP source address after a reverse lookup in the CEF table.

For more information about the feature, see the chapter *Implementing Cisco Express Forwarding* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*

EVPN-VxLAN Layer 2 Gateway with All-Active Support

This feature provides support for EVPN-VxLAN on Cisco NCS 5000.

DHCP Circuit-ID and Helper Address Interface Configuration

This feature supports DHCP circuit-ID and helper address interface configuration on Cisco NCS 5000.

Bridge Virtual Interface on VRF

Bridge Virtual Interface (BVI) on VRF feature enables VRF support on BVI when the BVI is part of the bridge domain that is configured with Layer 2 main interfaces and Layer 2 single-tagged sub-interfaces with rewrites. BVI is a virtual interface that is defined with Integrated Routing and Bridging (IRB).

100 ms Convergence Under Software Upgrade or Failure

This feature supports convergence enhancements on Cisco NCS 5000 in case of software upgrade or failure.

Global LLDP Knob to Enable LLDP Configuration

Earlier, in IOS-XR platforms, LLDP was enabled only with global LLDP configuration and administrators had to manually disable each interface.

With this feature, you can now enable the global LLDP configuration per-interface basis. To enable the feature, you must make the necessary configuration changes. For more information on the feature, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 5000 Series Routers*.

EVPN VXLAN All-Active Multihoming

The EVPN VXLAN All-Active Multihoming feature allows you to manage VXLAN Ethernet services in a spine-leaf data center or service provider network over VXLAN IP tunnel. This feature allows routers to be used as top of racks (ToRs). This feature simplifies fabric management, optimizes the fabric infrastructure, and automates provisioning across physical and virtual environments.

MAC Move Notification

The MAC Move Notification feature enables you to configure MAC address security at the interfaces and at the bridge access ports (subinterfaces) levels. However, MAC security configured under an interface takes precedence to MAC security configured at the bridge domain level. When a MAC address is first learned on an Ethernet Flow Point (EFP) that is configured with MAC security and then the same MAC address is learned on another EFP, the following events occur:

- the packet is dropped
- the second EFP is shutdown
- the packet is learned and the MAC from the original EFP is flushed

NETCONF Install YANG Actions

Traditionally, **install** operations are executed using CLIs, which require access to the routers. The NETCONF protocol is designed to automate the CLI executions for install operations, and address the shortcomings where the router access is required by implementing RPC mechanism.

For more information about this feature, see *Components to Use Data Models* Chapter of the *Programmability Configuration Guide for Cisco NCS 5000 Series Routers*.

IPv6 Configurable LPTS

In Cisco IOS XR, the control packets, which are destined to the Route Processor (RP), are policed using a set of ingress policers in the incoming ports. These policers are programmed statically during bootup by Local Packet Transport Services (LPTS) components and applied on the basis of the flow type of the incoming control traffic.

This feature enables you to modify default policer rates and hence control traffic of a particular IPv6 LPTS session matching a IPv6 ACL rule and VRF ID.

For more information about the feature, see the chapter *Configure IPv6 ACL-based LPTS Policers* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

IPv6 VPN Provider Edge

IPv6 VPN Provider Edge (6PE/VPE) uses the existing MPLS IPv4 core infrastructure for IPv6 transport. 6PE/VPE enables IPv6 sites to communicate with each other over an MPLS IPv4 core network using MPLS label switched paths (LSPs).

VLAN Switch

The VLAN Switch feature enables you to configure L2 VLAN switching with minimum configuration. This feature allows you to configure L2 bridging without having to configure and manage separate bridge instances and sub-interfaces for each per VLAN L2 forwarding domain.

Prior to implementation of this feature, to configure and manage basic L2 bridging, numerous sub-interfaces were required. Using separate sub-interfaces for each VLAN on a port overloads the system scalability and consumes hardware resources, slows down provisioning, and makes the device harder to manage due to the large number of sub-interface constructs that exists in the system.

For more information on this feature, see the *Configure Virtual LANs in Layer 2 VPNs* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5000 Series Routers*.

RPF Vector Encoding

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a MPLS-based BGP-free core, where the MPLS core router is without external routes learned from BGP). The RPF vector encoding is now compatible with the new IETF encoding. Use the **rpf-vector use-standard-encoding** command to enable the feature.

For more information on RPF, see the *Implementing Layer-3 Multicast Routing* chapter in the *Multicast Configuration Guide for Cisco NCS 5000 Series Routers*

Replace Installed Files with Golden ISO

Golden ISO (GISO) upgrades to a version that has a predefined list of software maintenance update (SMUs) with a single operation. However, to update to the same version with a different set of SMUs requires a two-step process. This two-step process can be avoided using the `install update replace` functionality to replace the currently active version with the full package including the image and SMUs from the newly added GISO.

For information about the functionality and configuration, see *Customize Installation using Golden ISO* chapter in the System Setup and Software Installation Guide for NCS5000 Series Routers, IOS XR 6.5.x.

Purge Originator Identification TLV for IS-IS

At present, an IS-IS purge does not contain any information to identify the Intermediate System (IS) that generates the purge. This makes it difficult to locate the source IS.

To address this issue, the Purge Originator Identification (POI) TLV for IS-IS feature defines a type, length, and value (TLV) that can be added to the purges, to record the system ID of the IS that had initiated the purge. This makes it easier to locate the origin of the purge and its cause. If you are using cryptographic authentication, then the **enable-poi** keyword in **lsp-password** command must be enabled to insert the Purge Originator Identification (POI). If you are not using cryptographic authentication, then the POI is inserted by default. This TLV is also helpful in lab environments.

For more information about this feature, see *Implementing IS-IS* Chapter of the *Routing Configuration Guide for Cisco NCS 5000 Series Routers*.

Telemetry over gNMI subscribe RPC

Cisco IOS XR supports Google network management interface (gNMI) protocol in dial-in mode where the client establishes a connection to the router. gNMI is an unified mangement protocol for streaming telemetry data using OpenConfig RPC framework. This framework and protocol does not need explicit configuration, but simplifies telemetry configuration on the router by only starting the gRPC server.

In addition, support is provided for transport layer security (TLS) ciphers in gRPC session. Two new gRPC configuration parameters `max-streams` and `max-streams-per-user` are provided to stream only the gRPC-specific requests.

To enable the gRPC server in dial-in mode, see *Configure Model-driven Telemetry* chapter in *Telemetry Configuration Guide for Cisco NCS 5000 Series Routers*.

OSPF Authentication with Keychain

OSPF Authentication with Keychain feature enables the support of Hashed Message Authentication Code (HMAC) during OSPF authentication. New crypto algorithms such as, HMAC-SHA-256 and HMAC-SHA1-96 are added under key-chain infra as part of this feature. These algorithms provide more secured authentication.

Keychains can be configured at different levels of OSPF like at the router level, or the area level, or the interface level.

For more information about OSPF Authentication, see *Implementing OSPF* Chapter of the *Routing Configuration Guide for Cisco NCS 5000 Series Routers, IOS XR Release 6.5.x*.

For more information about Keychain configuration, see *Implementing Keychain Management* Chapter of the *System Security Configuration Guide for Cisco NCS 5000 Series Routers, IOS XR Release 6.5.x*

Minimum Remaining Lifetime for IS-IS

The Minimum Remaining Lifetime for IS-IS feature helps to maintain the stability of the network when the *Remaining Lifetime* field in a Link State Protocol (LSP) is corrupted. Corruption of the *Remaining Lifetime* field in a LSP data unit can go undetected. In certain scenarios, this may cause or exacerbate flooding of LSPs. This feature resolves this problem by enabling IS-IS to reset the *Remaining Lifetime* value of the received LSP, to the maximum LSP lifetime (1200 seconds), if the *Remaining Lifetime* value of the received LSP is less than the maximum LSP lifetime configured in a local node. If the received LSP lifetime value is less than the Zero Age Lifetime (60 seconds), IS-IS generates an error message indicating that it's a corrupted lifetime event.

IS-IS saves the received *Remaining Lifetime* value in LSP database. The value is shown in the **show isis database** command output under the **Rcvd** field.

For more information about the **show isis database** command, see *IS-IS Commands* Chapter of the *Routing Command Reference for Cisco NCS 5000 Series Routers*.

For more information about this feature, see *Implementing IS-IS* Chapter of the *Routing Configuration Guide for Cisco NCS 5000 Series Routers*.

IS-IS Authentication with Keychain

IS-IS Authentication with Keychain feature enables the support of Hashed Message Authentication Code (HMAC) and Cipher-based Message Authentication Code (CMAC) during IS-IS authentication. New cryptographic algorithms such as, AES-128-CMAC-96, HMAC-SHA-256, and HMAC-SHA1-96 are added under Keychain infra as part of this feature. These algorithms provide more secured authentication.

Keychains can be configured at the router level (in case of the **lsp-password** command) and at the interface level (in case of the **hello-password** command) within IS-IS. These commands refer to the global keychain configuration and instruct the IS-IS protocol to obtain security parameters from the global set of configured keychains.

For more information about Keychain configuration, see *Implementing Keychain Management* Chapter of the *System Security Configuration Guide for Cisco NCS 5000 Series Routers*.

Replace Installed Files with Golden ISO

Golden ISO (GISO) upgrades to a version that has a predefined list of software maintenance update (SMUs) with a single operation. However, to update to the same version with a different set of SMUs requires a two-step process. This two-step process can be avoided using the `install update replace` functionality to replace the currently active version with the full package including the image and SMUs from the newly added GISO.

For information about the functionality and configuration, see *Customize Installation using Golden ISO* chapter in the System Setup and Software Installation Guide for NCS5000 Series Routers, IOS XR 6.5.x.

NRSSVR Process Infra Hardening on Repeated Configuration Commits

This feature provides resolution to prevent RDSFS process crash, and memory leakage at Name Registration Service (NRS) and Replicated Data Services File System (RDSFS) Server due to *large number of configuration commits*. To achieve this, nrs_purge API is enhanced to purge the NRS handles for files that are already deleted. This resolution provides significant improvements in the following aspects:

- Enables a large number of configuration commits, without any issues
- Ensures lower memory consumption for NRS server and RDSFS processes.
- Prevents the need to reload the router when it has to recover from the following scenarios:
  - Continuous restarting or crashing of RDSFS processes
  - Not being able to commit any configurations

Enhancements to Programmability

Cisco IOS XR supports programmability of `OC NI`, `OC local routing`, `OC-MPLS`, `OC-RSVP-SR`, `OC-RPL` and `OC-BGP-Policy` OpenConfig data models for configuration and operational data.

For more information about YANG data models and configuration, see *Using Data Models* chapter in *Programmability Configuration Guide for Cisco NCS 5000 Series Routers*

Behavior Change Introduced in this release

Deprecated Commands

- From this release onwards the **interface tunnel-te** *tunnel-id* **path-option pref {dynamic|explicit} segment-routing** command is deprecated. Configure Segment Routing Traffic Engineering (SR-TE) using the **segment-routing traffic-eng** command.

  For more information on the SR-TE commands and configurations, see the *Segment Routing Command Reference* and *Segment Routing Configuration Guide for Cisco NCS 5000 Series Routers*.

RPKI Prefix Validation

Starting from Cisco IOS XR Release 6.5.1, origin-as validation is disabled by default, you must enable it per address family.

See Configure BGP Prefix Validation

Hardware Features Introduced in Cisco IOS XR Software Release 6.5.1

There is no new hardware introduced in this release.

Hardware Enhancements Introduced in Cisco IOS XR Software Release 6.5.1

This release introduces following hardware enhancements:

- Support for 1GE SFP optics modules for single-fiber bidirectional applications on the NCS 5001 and NCS 5002 routers:
  - GLC-BX-D, GLC-BX-U
  - GLC-BX40-D-I, GLC-BX40-DA-I, GLC-BX40-U-I
  - GLC-BX80-D-I, GLC-BX80-U-I

  The bidirectional SFP optics modules operate on a single strand of standard SMF. The communication over a single strand of fiber is achieved by separating the transmission wavelength of the two devices.

  Refer to the Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet for descriptions and specifications.

Caveats

Caveats describe unexpected behavior in Cisco IOS XR Software releases. Severity-1 caveats are the most critical caveats; severity-2 caveats are less critical.

Cisco IOS XR Caveats

Bug ID	Headline
CSCvj73245	YANG framework detected the fatal condition Backend processing failed for cdp netconf request
CSCvk71334	Failed to obtain hardware interface key for BVI interface after series of 10+ reloads
CSCvk75964	Install Fails if GISO build tool is used from 6.5.x

Caveats Specific to the NCS 5000 Routers

There are no caveats in this release.

Bug ID	Headline
CSCvi77491	Both PI and PD license UNREGISTERED after HwModuleLocRP0Reload

Upgrading Cisco IOS XR Software

Cisco IOS XR Software is installed and activated from modular packages, allowing specific features or software patches to be installed, upgraded, or downgraded without affecting unrelated processes. Software packages can be upgraded or downgraded on all supported card types, or on a single card (node).

Before starting the software upgrade, use the **show install health** command in the admin mode. This command validates if the statuses of all relevant parameters of the system are ready for the software upgrade without interrupting the system.

The upgrade document is available along with the software images.

Cisco Software Manager (CSM) application provides an intuitive user interface to manage Cisco IOS XR installations, with pre-installation and post-installation checks and reports. CSM helps manage the process of software maintenance upgrades (SMUs) and service packs (SPs) on devices that run the Cisco IOS XR Software.

For information on how to use CSM, see Cisco Software Manager User Guide.

Note After upgrading to the latest release, the upgraded CHA FPD fails to activate on some of the RSP-880 TR/SE , A99-RSP TR/SE and RP2 cards even after RSP or RP is reloaded. The issue is observed in Cisco IOS XR 32-bit and Cisco IOS XR 64-bit image. The **show hw-module fpd** command output from the Cisco IOS XR 64-bit image displays the device status as **Reload Req**. However, there is no functionality impact seen during the normal operation of the router.

Please install the following SMUs and force upgrade CHA FPDs:

- AA14628 and AA14630

Related Documentation

The most current Cisco Network Convergence System 5000 Series documentation is located at this URL:

http://www.cisco.com/c/en/us/support/routers/network-convergence-system-5000-series/tsd-products-support-series-home.html

The document containing Cisco IOS XR System Error Messages (SEM) is located at this URL:

https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

Production Software Maintenance Updates (SMUs)

A production SMU is a SMU that is formally requested, developed, tested, and released. Production SMUs are intended for use in a live network environment and are formally supported by the Cisco TAC and the relevant development teams. Software bugs identified through software recommendations or Bug Search Tools are not a basis for production SMU requests.

For information on production SMU types, refer the Production SMU Types section of the IOS XR Software Maintenance Updates (SMUs) guide.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.