



# Release Notes for Cisco 8400 Series Secure Routers, 17.18.1a

---

# Contents

Cisco 8400 Series Secure Routers, Release 17.18.1a .....	3
New software features.....	3
Resolved issues .....	8
Open issues.....	9
Related resources.....	11
Legal information .....	12

## Cisco 8400 Series Secure Routers, Release 17.18.1a

Cisco 17.18.1a is the first release for Cisco 8400 Series Secure Routers in the Cisco IOS XE 17.18.x release series.

The key highlights of this release include these features and enhancements:

- Monitoring & Observability
- SRv6 Enhancements
- Security and SASE enhancements

### New software features

This section provides a brief description of the new software features introduced in this release.

#### New software features in Cisco IOS XE 17.18.2

Product impact	Feature	Description
Ease of Setup	<a href="#">XXXX</a>	From Cisco IOS XE 17.18.2, you can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager .
Upgrade	<a href="#">IPv6 GRE-TP tunnel as protected link support for SRv6 TI-LFA with IS-IS</a>	From Cisco IOS XE 17.18.2, this feature extends IPv6 GRE-TP tunnel as protected link support for SRv6 TILFA with ISIS.
Upgrade	<a href="#">IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with OSPF</a>	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPF.
Upgrade	<a href="#">IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with IS-IS</a>	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with ISIS.
Security	<a href="#">Infrastructure Resiliency</a>	<p>Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.</p> <p>This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release:</p> <ul style="list-style-type: none"><li>• <b>Plain-text and weak credential storage:</b> Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.</li></ul> <p><i>Recommendation:</i> Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-</p>

Product impact	Feature	Description
		<p>SHA-256) or Type 9 (Scrypt) for non-reversible credentials.</p> <ul style="list-style-type: none"> <li>• <b>SSHv1</b> <i>Recommendation:</i> Use SSHv2.</li> <li>• <b>SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption</b> <i>Recommendation:</i> Use SNMPv3 with authentication and encryption (authPriv).</li> <li>• <b>MD5 (authentication) and 3DES (encryption) in SNMPv3</b> <i>Recommendation:</i> Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.</li> <li>• <b>IP source routing based on IP header options</b> <i>Recommendation:</i> Do not use this legacy feature.</li> <li>• <b>TLS 1.0 and TLS 1.1</b> <i>Recommendation:</i> Use TLS 1.2 or later.</li> <li>• <b>TLS ciphers using SHA1 for digital signatures</b> <i>Recommendation:</i> Use ciphers with SHA256 or stronger digital signatures.</li> <li>• <b>HTTP</b> <i>Recommendation:</i> Use HTTPS.</li> <li>• <b>Telnet</b> <i>Recommendation:</i> Use SSH for remote access.</li> <li>• <b>FTP and TFTP</b> <i>Recommendation:</i> Use SFTP or HTTPS for file transfers.</li> <li>• <b>On-Demand Routing (ODR)</b> <i>Recommendation:</i> Use a standard routing protocol in place of CDP-based routing information exchange.</li> <li>• <b>BootP server</b> <i>Recommendation:</i> Use DHCP or secure boot features such as Secure ZTP.</li> <li>• <b>TCP and UDP small servers (echo, chargen, discard, daytime)</b> <i>Recommendation:</i> Do not use these services on</li> </ul>

Product impact	Feature	Description
		<p>network devices.</p> <ul style="list-style-type: none"> <li>• <b>IP finger</b></li> </ul> <p><i>Recommendation:</i> Do not use this protocol on network devices.</p> <ul style="list-style-type: none"> <li>• <b>NTP control messages</b></li> </ul> <p><i>Recommendation:</i> Do not use this feature.</p> <ul style="list-style-type: none"> <li>• <b>TACACS+ using pre-shared keys and MD5</b></li> </ul> <p><i>Recommendation:</i> Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1</p>

## New software features in Cisco IOS XE 17.18.1

**Table 1.** New software features for Cisco 8400 Edge Platform, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	<a href="#">Hosted Edge Services for SD-Routing Devices</a>	Cisco IOS XE 17.18.1a introduces Hosted Edge Services, a new monitoring feature which enables direct management of Cisco IOx applications installed on your SD-Routing edge devices. This feature delivers improved functionalities like tracking resource usage, starting or stopping Cisco IOx applications at a scale directly through Cisco Catalyst SD-WAN Manager.
C8400 Series Secure Routers Licensing	<a href="#">C8000 Series Secure Routers Licensing</a>	C8400 Series Secure Routers supports platform-based licensing, a way of grouping licenses and devices based on platform-classes. A platform class is a hierarchical categorization based on the product family and place in the network. In this platform-based licensing model, Essentials and Advantage licenses are available. License portability is supported across devices within the same platform class and usage of the same license across different modes is also possible.
Licensing Process	<a href="#">Licensing compliance, reporting, and notification enhancements</a>	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Licensing Process	<a href="#">Product Analytics for routers</a>	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when you start your router. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of use	<a href="#">Managing NGFW Policies from Security Cloud Control</a>	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies.

Product impact	Feature	Description
		From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Security	<a href="#">Custom IPS signature sets</a>	From Cisco IOS XE 17.18.1a release, <a href="#">Custom IPS signature sets</a> are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets. This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	<a href="#">Certificate Management on SD-Routing Devices</a>	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Upgrade	<a href="#">MVPN Ingress Replication (IR) over SRv6</a>	This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	<a href="#">SRv6 Path MTU Discovery</a>	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.
Upgrade	<a href="#">SRv6 Flex- Algo with TI-LFA and uLoop Avoidance</a>	From Cisco IOS XE 17.17.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Licensing Process	<a href="#">Product Analytics for routers</a>	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of Use	<a href="#">MAP-T Border Router (BR) Enhancements</a>	The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment.
Ease of Use	<a href="#">Hosted Edge Services for SD-Routing Devices</a>	From Cisco IOS XE 17.18.1a release, Cisco Catalyst SD-WAN Manager supports deployment of IOx applications such as Cyber Vision, Thousand Eyes, UTD, and so on. The support to monitor these applications is introduced through Hosted Edge Services monitoring dashboard which offers a simplified user experience for overseeing IOx container applications across multiple devices. The Hosted Edge Services monitoring dashboard is introduced on Cisco Catalyst SD-WAN Manager version 20.18.x.

Product impact	Feature	Description
Ease of setup	<a href="#">Cisco Secure Routers Swim and Onboarding Tool</a>	Cisco IOS XE 17.18.1a introduces the Cisco Secure Routers Swim and Onboarding tool that helps customers upgrade and onboard Autonomous hardware devices to cloud-hosted or on-premises Catalyst Cisco SD-WAN Manager.
Licensing Process	Licensing compliance, reporting, and notification enhancements	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Ease of use	<a href="#">Managing NGFW Policies from Security Cloud Control</a>	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Security	<a href="#">Custom IPS signature sets</a>	From Cisco IOS XE 17.18.1a release, <a href="#">Custom IPS signature sets</a> are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets. This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	<a href="#">Certificate Management on SD-Routing Devices</a>	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Upgrade	<a href="#">MVPN Ingress Replication (IR) over SRv6</a>	This feature enables the transport of IPv4 Multicast traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	<a href="#">SRv6 Path MTU Discovery</a>	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.
Upgrade	<a href="#">SRv6 Flex-Algo with TI-LFA and uLoop Avoidance</a>	From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Licensing Process	<a href="#">Product Analytics for routers</a>	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.

Product impact	Feature	Description
Ease of Use	<a href="#">MAP-T Border Router (BR) Enhancements</a>	The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment.
Ease of Use	<a href="#">MAP-T Border Router (BR) Enhancements</a>	The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment.

## Resolved issues

This table lists the resolved issues in this specific software release.

**Note:** This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#). To search for a documented Cisco product issue, type in the browser: <bug\_number> site:cisco.com.

## Resolved issues in Cisco IOS XE 17.18.2

**Table 2.** Resolved issues for Cisco 8400 Edge Platform, Release 17.18.2

Bug ID	Description
<a href="#">CSCwr42950</a>	SDWAN On-Demand Tunnels Do Not Expire When UMTS Is Enabled
<a href="#">CSCwq51935</a>	NAT64 static entry removed when command to delete non-existent entry is applied.
<a href="#">CSCwe19394</a>	cEdge: device may boot up into prev_packages.conf due to power outage
<a href="#">CSCwr77958</a>	NWPI not capturing self-generated syslog traffic
<a href="#">CSCwi61730</a>	Cat8500L crash when removing SGT caching on an interface
<a href="#">CSCwq77322</a>	C8500-12X sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet
<a href="#">CSCwr24031</a>	After upgrade to 17.15 for earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured
<a href="#">CSCwr49794</a>	ISR exporters with ETA enabled are generating invalid template data errors in SNA
<a href="#">CSCwq98206</a>	EPBR set interface action get missing after reboot
<a href="#">CSCwr25077</a>	vDaemon crash when initializing DNS channels

## Resolved issues in Cisco IOS XE 17.18.1

**Table 3.** Resolved issues for Cisco 8400 Edge Platform, Release 17.18.1

Bug ID	Description
<a href="#">CSCwn26353</a>	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
<a href="#">CSCwm27749</a>	Speed test download / throughput issue on device seen with IPSEC ESP-NULl transform using Zscaler
<a href="#">CSCwo75657</a>	Maximum control connection not equal to maximum omp sessions
<a href="#">CSCwm72336</a>	CXP with Data Policy redirect-DNS via overlay causes blackhole
<a href="#">CSCwp91064</a>	FTMD zero pointer dereference leading to crash
<a href="#">CSCwo72675</a>	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
<a href="#">CSCwn26353</a>	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
<a href="#">CSCwm27749</a>	Speed test download / Throughput issue on C8200 platform seen with IPSEC ESP-NULl transform using Zscaler
<a href="#">CSCwo75657</a>	Maximum control connection not equal to maximum omp sessions - cEdge
<a href="#">CSCwm72336</a>	CXP with Data Policy redirect-DNS via Overlay causes Blackhole
<a href="#">CSCwp91064</a>	FTMD zero pointer dereference leading to crash
<a href="#">CSCwo72675</a>	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.

## Open issues

This table lists the open issues in this specific software release.

**Note:** This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#). To search for a documented Cisco product issue, type in the browser: <bug\_number> site:cisco.com

## Open issues in Cisco IOS XE 17.18.2

**Table 4.** Open issues for Cisco 8400 Edge Platform, Release 17.18.2

Bug ID	Description
<a href="#">CSCws30834</a>	cedge ignore the keepalive command under the SIG tunnel interface pushed by the vmanage
<a href="#">CSCws13857</a>	Incorrect NAT translation from service-vrf to global for self-generated ICMP 11 (Time Exceeded) packets
<a href="#">CSCwq77458</a>	fman crash after fnf config changes
<a href="#">CSCwr87083</a>	C11xx: Not able to onboard sd-routing devices using generic bootstrap file stored in usb

Bug ID	Description
<a href="#">CSCws12946</a>	Cedge port forward issue with multiple ISP
<a href="#">CSCws18137</a>	Out of sync when CLI Template was attached (missing element: authentication in /ios:native/ios:line/ios:vty[ios:first='0']/ios:login/ios:authentication)
<a href="#">CSCwr76580</a>	strange behavior with the Cisco Umbrella SIG tunnels configured from vManage to Umbrella.
<a href="#">CSCwr30573</a>	TLOC Extension unable to program due to module boot up timing
<a href="#">CSCws25557</a>	Cipher Suites TLS 1.2 for control connections
<a href="#">CSCwr95551</a>	Router crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT
<a href="#">CSCwr08462</a>	[C8500L-8S4X] There seems to be an issue where the NAT router is not responding to ARP requests
<a href="#">CSCwr44921</a>	SDWAN C-Edge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold
<a href="#">CSCwr97784</a>	Slow performance on Netconf RPC on 17.15.2a on stateless static NAT translation
<a href="#">CSCwr88206</a>	FIB table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole
<a href="#">CSCwr84985</a>	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
<a href="#">CSCwq24119</a>	IR1835: Traceback seen when detaching the CN railways customer configs in 17.19
<a href="#">CSCwm97460</a>	17.9 cEdges - Control Connection to vManage is only Attempted over Highest Priority TLOC
<a href="#">CSCwr00088</a>	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
<a href="#">CSCwr55240</a>	C8000v experienced Critical process ompd fault on rp_0_0
<a href="#">CSCwr72709</a>	Router crash in TDM-TDM call when debug voip fpi enabled
<a href="#">CSCwq98154</a>	[XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
<a href="#">CSCwr49475</a>	BFD sessions flapping and not recovering - SYMNAT port not updating to data-plane
<a href="#">CSCwo42664</a>	SD-WAN Edge: Periodic Service Restart May Generate Crash Files
<a href="#">CSCwr64257</a>	Unexpected reload on ftmd SDWAN device
<a href="#">CSCws26373</a>	cEdge experiences an unexpected reboot due to NAT in the data-plane after a policy push
<a href="#">CSCwp97178</a>	v1718/polaris: flapping nat will casue bfd session down with ipsec session shown
<a href="#">CSCwr76176</a>	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
<a href="#">CSCwr77083</a>	C8000v crashed in crypto library

## Open issues in Cisco IOS XE 17.18.1a

**Table 5.** Open issues for Cisco 8400 Edge Platform, Release 17.18.1a

Bug ID	Description
<a href="#">CSCwp01089</a>	EPFR-High latency times are observed on the hub device
<a href="#">CSCwp12196</a>	Device unexpectedly reloads due to memory corruption on a notification queue in FTMD
<a href="#">CSCwq27426</a>	BFD session down due to unencrypted outbound BFD packets despite active IPsec SA
<a href="#">CSCwe19394</a>	Device may boot up into prev_packages.conf due to power outage
<a href="#">CSCwq40026</a>	Unexpected Reboot due to Process FTMD
<a href="#">CSCwp01089</a>	EPFR-High latency times are observed on the hub device (Cisco Catalyst 8500-12X Edge Platform).
<a href="#">CSCwp12196</a>	cEdge router unexpectedly reloads due to memory corruption on a notification queue in FTMD
<a href="#">CSCwq27426</a>	cEdge: BFD session down due to unencrypted outbound BFD packets despite active IPsec SA
<a href="#">CSCwe19394</a>	cEdge: device may boot up into prev_packages.conf due to power outage
<a href="#">CSCwq40026</a>	Unexpected Reboot due to Process FTMD

### Related resources

- [Hardware Installation Guide for Cisco 8400 Series Secure Routers](#)
- [Software Configuration Guide for Cisco 8400 Series Secure Routers](#)
- [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#)

---

## Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2025 Cisco Systems, Inc. All rights reserved.