Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.7.x

First Published: 2021-12-11

Last Modified: 2022-06-25

Read Me First



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco vEdge Device, Cisco SD-WAN Release 20.7.x

Note 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.

These release notes accompany the Cisco SD-WAN Release 20.7.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco vEdge devices.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.7.x.

For release information about Cisco SD-WAN Controllers, refer to Release Notes for Cisco SD-WAN Controllers, Cisco SD-WAN Release 20.7.x

What's New for Cisco SD-WAN Release 20.7.x

This section applies to Cisco vEdge devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco SD-WAN Release 20.7.1

Feature	Description
Cisco SD-WAN Getting Started	
Day 0 WAN Interface Automatic IP Detection using ARP	This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process.
Certificate Revocation	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.

Feature	Description
DigiCert Migration	This feature replaces the Symantec Certificate Authority (CA) server with Digicert Certificate Authority server for signing the controller device certificates on Cisco SD-WAN controllers including Cisco vSmart Controller, Cisco vBond Orchestrator, and Cisco vManage. You can protect, verify, and authenticate the identities of organizations and domains using these certificates.
Systems and Interfaces	
TCP/UDP Endpoint tracker and Dual Endpoint Static route tracker for Cisco vEdge devices	This feature enables you to configure the TCP/UDP individual Endpoint static route tracker and to configure tracker group with IPv4, TCP/UDP Dual Endpoint static route trackers for service VPNs to enhance the reliability of the probes.
VRRP Interface Tracking for Cisco vEdge Devices	This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco vEdge devices. Starting this release, you can configure it through Cisco vManage feature template.
Co-Management: Granular Role-Based Access Control for Feature Templates	This feature introduces greater granularity in assigning role-based access control (RBAC) permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Policies	
Configure Default AAR and QoS Policies	This feature is an enhancement to the centralized and localized policies feature. This feature allows you to configure default application-aware routing (AAR) and quality of service (QoS) policies on Cisco IOS XE devices.
High Availability	
Disaster Recovery User Password Change	This feature lets you change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.
Cloud OnRamp	
Cisco CXP Gateway Support for Internet Exit through Service VPN Interfaces	This feature adds support for enabling SaaS in service VPN interfaces in Gateway sites.
Support for Cisco VM Image Upload in qcow2 Format	This feature allows you to upload a virtual machine image to Cisco vManage in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.

Feature	Description
Packet Capture for Cloud onRamp Colocation Clusters	This feature lets you capture packets at either the physical interface level (PNIC) or the virtual interface level (VNIC) on a CSP device of a colocation cluster. You can capture packets on one or more PNICs or VNICs on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format and therefore helps in application analysis, security, and troubleshooting.
Cisco SD-WAN Monitor and Maintain	
Additional Diagnostics Information Added to Admin-Tech File	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	This feature enables you to upload an admin-tech file directly from Cisco vManage when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests (SRs) from Cisco vManage. This streamlines the steps required for working with TAC to troubleshoot a problem.
Resource Monitoring on Cisco SD-WAN Controllers and Cisco vEdge Devices	With this feature, you can configure usage watermarks for resources such as CPU, memory, and disk on Cisco SD-WAN controllers and Cisco vEdge devices. In addition, on Cisco vManage servers, you can configure watermarks to monitor disk read and write speeds. Devices poll the resource usage and notify events to Cisco vManage. Cisco vManage raises alarms to alert you to changes in resource usage, or disk read or write speed so that you can take any necessary corrective action.
Software Upgrade Using a Remote Server	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco vManage, and add locations of software images on the remote server to the Cisco vManage software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.
Enhanced Cisco vManage User Interface for a Consolidated Monitoring View	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all monitoring components have been organized into pill buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu so that you can easily locate these features.

Feature	Description
Cisco SD-WAN Command Reference	
OMP CLI Enhancements	This feature displays detailed information about OMP and TLOC routes on Cisco vSmart Controllers and Cisco vEdge devices. The following commands are enhanced to display received and advertised peering sessions for OMP. show omp routes show omp tlocs

Software and Hardware Behavior Changes in Cisco SD-WAN Release 20.7.1

Behavior Change	Link to Updated Documentation
Angle brackets (< or >) are converted to their HTML equivalents in Cisco SD-WAN Manager feature templates.	A note on special characters is updated in the Feature Templates section.
New error message added for buffer pool.	TMD_SYSLOG_BUFFER_POOL_LOW
Admin-Tech file enhancement	Upload an Admin-Tech File to a TAC Case
Update to cloud-init configuration file	A note on cloud-init configuration file is added in the Create vEdge Cloud VM Instance on KVM section.
When generating a bootstrap configuration file for a Cisco vEdge device, you can now choose an option to generate a file for a Cisco vEdge device using Cisco Catalyst SD-WAN Release 20.4.x or earlier.	Generate a Bootstrap Configuration File

Software and Hardware Behavior Changes in Cisco SD-WAN Release 20.7.2

Behavior Change	Link to Updated Documentation
The vedge-cloud medium device allows 7 SLAs to configure from Cisco vSmart Controller.	A table on maximum SLA classes supported is updated in the SLA Classes section.
Update to cloud-init configuration file	A note on cloud-init configuration file is added in the Create vEdge Cloud VM Instance on KVM section.
In the Cisco SD-WAN overlay, you can have a maximum of 512 multicast enabled Cisco vEdge devices per VPN.	A note on the overlay scalability is added in the PIM Scalability Information section.
Secure Internet Gateway (SIG) tracker monitor statistics are no longer reset at every Domain Name System (DNS) cache timeout interval. SIG tracker monitor statistics are now reset every two hours. A SIG tracker allows you to track the health of your SIG tunnels.	A note is added in the Create Automatic Tunnels Using SIG Feature Template section.

Behavior Change	Link to Updated Documentation
When generating a bootstrap configuration file for a Cisco vEdge device, you can now choose an option to generate a file for a Cisco vEdge device using Cisco Catalyst SD-WAN Release 20.4.x or earlier.	Generate a Bootstrap Configuration File

Important Notes, Known Behavior, and Workaround

- Starting from Cisco SD-WAN Release 20.5.1, Cloud onRamp for IaaS isn't supported for Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.5.1. However, Cloud onRamp for IaaS is supported with AWS as the cloud provider for Cisco vEdge Cloud Routers using Cisco SD-WAN Release 20.4.1 and earlier. Cloud onRamp for IaaS is also supported with Microsoft Azure as the cloud provider for Cisco vEdge Routers using Cisco SD-WAN Release 20.3.1 and earlier.
- For information about upgrade paths, see Cisco vManage Upgrade Paths.

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Bugs for Cisco SD-WAN Release 20.7.2

This section details all fixed and open bugs for this release. These are available in the Cisco Bug Search Tool through the Resolved Bug Search.

Resolved Bugs for Cisco SD-WAN Release 20.7.2

Identifier	Headline
CSCvz64630	Enhancement request to restrict access to GDB tool for non root users. i.e. restrict to 0700
CSCwa08989	Interested traffic(FTP/SIP/ICMP...) can't be forwarded properly after vEdge device rebooting.
CSCwa32952	Cisco vEdge device access controlled via TACACS+ prevents user from performing certain configurations
CSCwa78885	20.8: vEdge2k crashed due to kernel panic while generated admin-tech from Cisco vManage
CSCwb04644	SNMPD crash seen on running Snmpwalk - 20.6.2 Cisco vEdge device5K
CSCwa24992	ZBFW zone-pair (service to service) not working as expected.

Identifier	Headline
CSCwa17427	20.7.1: Gige 0/4 on Cisco vEdge device100 not transmitting or receiving traffic after a reboot
CSCvz42160	Device not rebooting after an intentional crash
CSCwb03242	Cisco vEdge device routing table did not remove deleted default route
CSCvz87934	Cisco vEdge device marking the routes as invalid in OMP when the control policy is changed.
CSCwa51818	Cisco vEdge device-5000 not able to configure more than 4 SLA's
CSCwa58714	Loopback interface not reachable when the gateway set to the virtual vrrp ip
CSCwa84507	Hardware Random Number generation shouldn't include TPM RNG until mutexing occurrs
CSCvy57380	Endpoint Tracker stays down when ip address changed from dhcp to static
CSCwa59201	Cisco vEdge device5k TPM failure resulting TLOC disable
CSCvy27321	Cisco vEdge device interface tracker reporting down status in vdebug constantly while on the CLI its up.

Open Bugs for Cisco SD-WAN Release 20.7.2

Identifier	Headline
CSCwb58618	Cisco vEdge device Sig Autotunnels:Error parsing JSON response for locations and 409 Response received.
CSCwb06217	After failover Existing primary vedge stops receiving traffic and forwarding - 20.6.2
CSCwa23852	Azure Viptela vEdge/vSmart VHD image doesn't prompt initial admin password wizard
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Bugs for Cisco SD-WAN Release 20.7.1

This section details all fixed and open bugs for this release. These are available in the Cisco Bug Search Tool through the Resolved Bug Search.

Resolved Bugs for Cisco SD-WAN Release 20.7.1

Bug ID	Description
CSCvy90538	vedge 20.5 on KVM/ESXI SRIOV: Throughput degradation observed with Qos configs and 1400B traffic
CSCvz43474	OMPD crash seen on vEdge2k doing an assert while doing best path calculation operation.

Bug ID	Description
CSCvz46516	sit_regression; speedtest.py- test_speedtest_2edges: Failed to start iperf client
CSCvy98507	vEdge crash due to Zebra process failure
CSCvx65749	vEdge: we should see an error message on vdebug when system buffer pool is depleting
CSCvy80654	edge router maintains persistent connections to vbond
CSCvv57641	c/vEdge "show omp routes|tlocs received|advertise detail" must show received or advertised not both
CSCvz42885	Packet drops due to QoS Policy after upgrading from 20.3.3 to 20.6.0.101
CSCvx71152	Cisco vEdge 5000 unable to form control connections with controller - Stuck in Challenge -> Timeout

Open Bugs for Cisco SD-WAN Release 20.7.1

Bug ID	Description
CSCwa36262	Vedge 1000 after upgrading to 20.6.1 Error: application communication failure is seen
CSCwa32952	vEdge access controlled via TACACS+ prevents user from performing certain configurations
CSCvz20061	vEdge: OSPF route isn't removed from routing table.
CSCwa25457	Cisco ISR 1000 6G/Vedge 5K: BFD sessions take long time to come up after clearing omp sessions
CSCwa23074	core.fpX.usec found on Vedge1000 after running stress test
CSCwa23852	Azure Cisco SD-WAN vEdge/vSmart VHD image doesn't prompt initial admin password wizard
CSCwa51818	vedge-5000 not able to configure more than 4 SLA's
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Supported Devices

For device compatibility information, see Cisco SD-WAN Device Compatibility.

Redesign of Cisco vManage GUI

From Cisco vManage Release 20.7.1, Cisco vManage GUI is redesigned and offers a new visual display. This section presents a comparative summary of the significant changes between older Cisco vManage releases and Cisco vManage Release 20.7.1 and later.

Changes in Monitor and Tools Menus

Cisco vManage Release 20.7.1 includes the following changes:

- The **Dashboard** menu is removed, and all submenus that were earlier accessible from the **Dashboard** menu are now part of the **Monitor** menu.
- The **Monitor** page provides a real-time user interface with a consolidated view of the monitoring information for the components and services of a Cisco SD-WAN overlay network.
- Using the pill buttons on the **Monitor** page, you can navigate to monitoring information for specific components or services of a Cisco SD-WAN overlay network.
- The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu are now part of the **Tools** menu so that you can easily locate these features.

Figure 1: Dashboard Menu in Cisco vManage Release 20.6.1 and Earlier

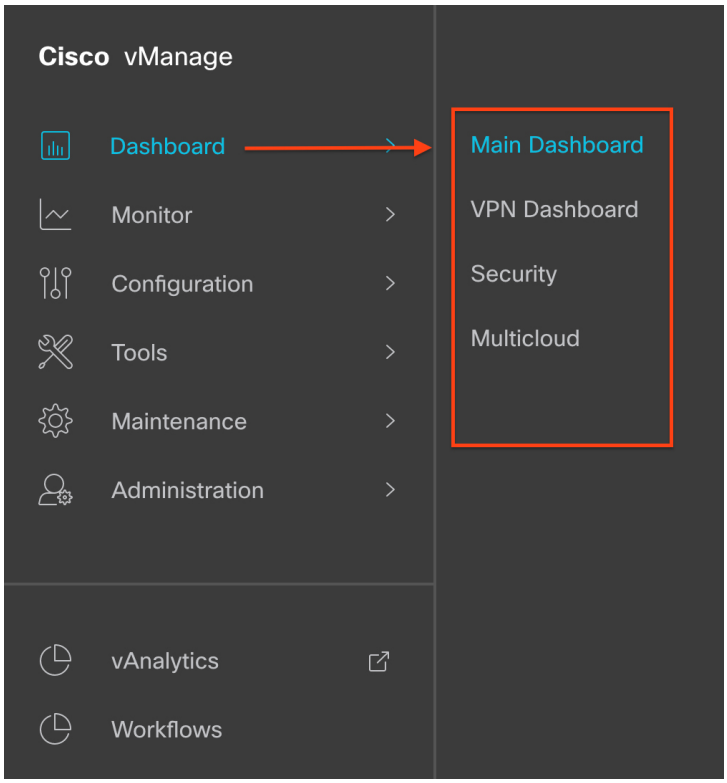


Figure 2: Monitor Menu in Cisco vManage Release 20.7.1 and Later

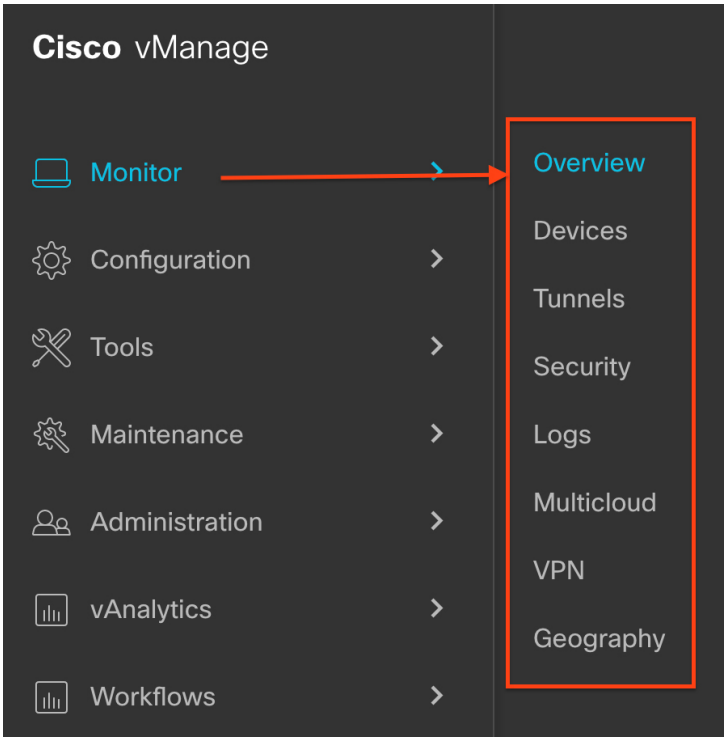


Figure 3: Tools Menu in Cisco vManage Release 20.7.1 and Later

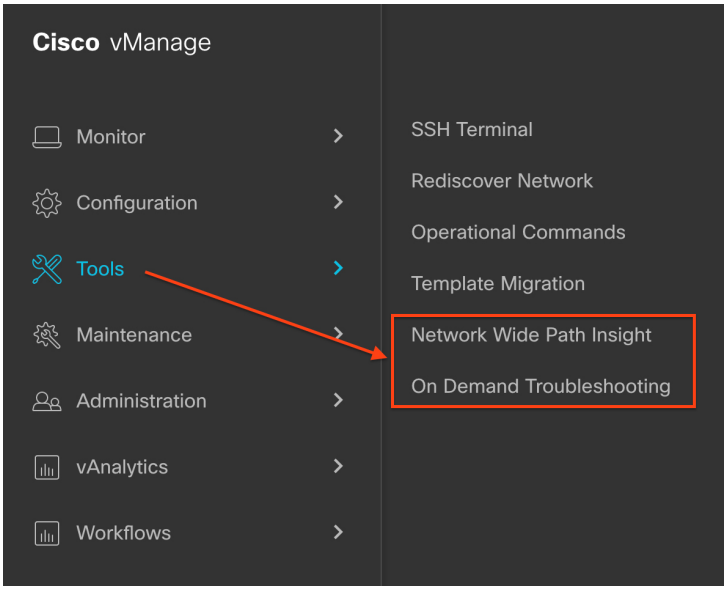
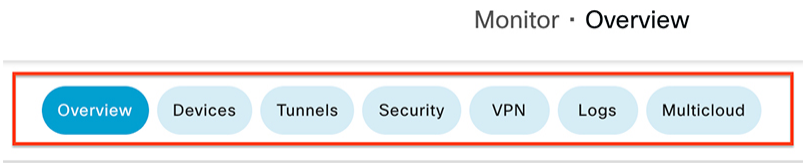


Figure 4: Pill Buttons in Monitor Window in Cisco vManage Release 20.7.1 and Later



Support for Web Content Accessibility Guidelines (WCAG) 2.0 Standard

Cisco vManage Release 20.7.1 supports Web Content Accessibility Guidelines (WCAG) 2.0 standard for the AA conformance level, with the following limitations:

- You cannot exit from SSH terminal using the keyboard.
- Cisco SD-WAN Manager cannot skip repetitive navigation links.
- Data charts on Cisco SD-WAN Manager use colors as the only visual means of conveying information, which is not compliant with WCAG 2.0.
- Some text elements as well as non-text elements in Cisco SD-WAN Manager do not meet the color contrast ratio as defined in WCAG 2.0.

Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.