

# Cisco Prime Network Services Controller Release Notes, Release 3.5.1b

---

**First Published:** 2020-06-29

## Cisco Prime Network Services Controller Release Notes

This document describes the features, limitations, and bugs for the Prime Network Services Controller, Release 3.5.1b.

### Prime Network Services Controller Overview

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services. For the latest release updates and overview, see the corresponding [data sheet](#).

Cisco Prime Network Services Controller is the primary management element for Cisco Nexus 1000VE Switches and Services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000VE switches and services deliver a highly secure multitenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Cisco Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. is built on an information-model architecture in which each managed device is represented by its subcomponents (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG security services.



---

**Note** Starting with Cisco PNSC Release 3.4.2a, Cisco Adaptive Security Appliance (ASA 1000V), Cisco Cloud Services Router (CSR), Citrix NetScaler VPX, Citrix NetScaler, and KVM Hypervisor, and Microsoft HyperV platforms are not supported.

---

#### Hypervisor Support

The Prime Network Services Controller platform supports multiple VM Managers through their APIs and through tight integration with Nexus 1000VE Virtual Supervisor Modules (VSMs) and Virtual Ethernet Modules (VEMs).

#### Cisco Dynamic Fabric Automation Integration Support

Cisco Dynamic Fabric Automation (DFA) delivers fabric optimization, management, and automation capabilities under Cisco Unified Fabric. Prime Network Services Controller plays a critical role in the Cisco DFA solution

with L4-7 services integration. Prime Network Services Controller integrates with Cisco Data Center Network Manager (DCNM) to support the managed resources and services in a VMware vSphere environment.

### **Consistent and Efficient Security Policies**

Prime Network Services Controller uses security profiles for template-based configuration of security policies. A security profile is a collection of security policy sets and integrated policies and rules that can be predefined and applied on demand at the time of virtual machine instantiation. This profile-based approach significantly simplifies authoring, deployment, and management of security policies, including dense multi-tenant environments, while enhancing deployment agility and scaling. Security profiles also help reduce administrative errors and simplify audits.

The XML API for Prime Network Services Controller facilitates integration with northbound network provisioning tools for programmatic network and security provisioning and management of Cisco VSG (VSG) and ASA 1000V. The option of programmatic control of those virtual appliances can greatly simplify operational processes and reduce infrastructure management costs.

### **Nondisruptive Administration Model**

By providing visual and programmatic controls, Prime Network Services Controller can enable the security operations team to author and manage security policies for virtualized infrastructure and enhance collaboration with the server and network operations teams. This nondisruptive administration model helps ensure administrative segregation of duties to reduce errors and simplify regulatory compliance and auditing:

- Security administrators can author and manage security profiles and manage VSG instances. Security profiles are referenced in Nexus 1000VE port profiles.
- Network administrators can author and manage port profiles, and manage Nexus 1000VE switches. Port profiles with referenced security profiles are available in VMware vCenter through the Nexus 1000VE VSM programmatic interface with VMware vCenter.
- Server administrators can select an appropriate port profile in VMware vCenter when instantiating a virtual machine.

### **Efficient Management for Easier Scalability**

Prime Network Services Controller implements an information-model architecture in which each managed device, such as VSG or Cisco ASA 1000V, is represented by the device's object-information model. This model-based architecture helps enable the use of:

- Stateless managed devices—Security policies (security templates) and object configurations are abstracted into a centralized repository and used as templates against any virtual device type.
- Dynamic device allocation—A centralized resource management function manages pools of devices that are commissioned (deployed) in service and a pool of devices that are available for commissioning. This approach simplifies large-scale deployments because managed devices can be preinstantiated and then configured on demand, and devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools.
- Scalable management—A distributed management-plane function is implemented using an embedded agent on each managed device that helps enable greater scalability.

## **New Features and Enhancements**

No new features were introduced in Cisco Prime Network Services Controller, release 3.5.1b.

## Limitations and Usage Guidelines

This section lists the usage guidelines and limitations for the Cisco Prime Network Services Controller (PNSC):

- Starting with PNSC release 3.5.1b with VMware ESXi 6.7u2, you can not instantiate VSG through PNSC.
- We recommend you to use Firefox version 69.0.3 or later for PNSC. Configuration changes in PNSC do not reflect automatically for Google Chrome and Windows IE, and require manual refresh.
- Cisco PNSC release 3.5.1b does not support functionality to create port profiles. Use VSM CLI to create port profiles.
- Starting with PNSC release 3.5.1b, Org changes for a tenant is not supported. Use VSM CLI for Org changes for a tenant.
- Cisco PNSC release 3.5.1b does not support user defined policy rule conditions. Network, VM, and VZone Attribute Type cover all the required expressions for the filter conditions.

## Requirements Overview

The following topics identify the primary requirements for installing and using Prime Network Services Controller.

### System Requirements

Requirement	Description
<b>Prime Network Services Controller Virtual Appliance</b>	
Four virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk space	<p>220 GB on shared NFS or SAN, configured on two disks as follows:</p> <ul style="list-style-type: none"> <li>• Disk 1—20 GB</li> <li>• Disk 2—200 GB</li> </ul> <p>• With InterCloud functionality, 220 GB on shared NFS or SAN, and configured on two disks as follows:</p> <ul style="list-style-type: none"> <li>• Disk 1—20 GB</li> <li>• Disk 2—200 GB</li> </ul> <p>• Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows:</p> <ul style="list-style-type: none"> <li>• Disk 1—20 GB</li> <li>• Disk 2—20 GB</li> </ul>

Requirement	Description
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix

## Hypervisor Requirements

Prime Network Services Controller is a multi-hypervisor virtual appliance that can be deployed on VMware vSphere.

See the [VMware Compatibility Guide](#) to confirm that VMware supports your hardware platform.

Requirement	Description
<b>VMware</b>	
VMware vSphere	6.5.0, 6.7 U1, 6.7 U2, 6.7 U3
VMware vCenter	6.5 U2, 6.7 U1, 6.7 U2, 6.7 U3

## Web-Based GUI Client Requirements

Requirement	Description
Operating system	Either of the following: <ul style="list-style-type: none"> <li>• Microsoft Windows</li> <li>• Apple Mac OS</li> </ul>
Browser	Any of the following: <ul style="list-style-type: none"> <li>• Google Chrome 32.0 or later (recommended)</li> <li>• Internet Explorer 10.0 or later</li> <li>• Mozilla Firefox 26.0 or later</li> </ul>
Flash player	Adobe Flash Player plugin 11.9 or later

## Firewall Ports Requiring Access

If Prime Network Services Controller is protected by a firewall, the following ports on the firewall must be open so that clients can contact Prime Network Services Controller.

Port	Description
22	TCP/SSH
80	HTTP
443	HTTPS
843	Adobe Flash

## Performance and Scalability

The following table lists the performance and scalability data for Prime Network Services Controller when using VMware.

Item	Scalability Numbers
Endpoints ( VSGs)	511
Hypervisors	600
Locales	256
Object groups	65536
Orgs	2048
Policies	4096
Policy sets	2048
Rules	16384
Security profiles	2048
Tenants	256
Managed VMs	6000
Users	260
Zones	8192

## Hypervisor Support

The following table identifies features that differ with regard to hypervisor support in Prime Network Services Controller Release 3.5.1b. Features that are not listed are supported by all hypervisors.

<b>Feature and Device Support</b>	<b>VMware vSphere ESXi 5.5, 6.0, 6.5a, and 6.7u1</b>
<b>Feature Support</b>	
Automatic deployment of network services	Supported

<b>Feature and Device Support</b>	<b>VMware vSphere ESXi 5.5, 6.0, 6.5a, and 6.7u1</b>
VM Attribute support	Supported: <ul style="list-style-type: none"> <li>• Cluster Name</li> <li>• Guest OS Full</li> <li>• Name</li> <li>• Hypervisor Name</li> <li>• Parent Application Name</li> <li>• Port Profile Name</li> <li>• Resource Pool</li> <li>• VM DNS Name</li> <li>• VM Name</li> </ul>
<b>Device Support</b>	
For detailed information about device support, see <a href="#">Cisco Prime Network Services Controller Supported Devices</a> .	
VSG	Supported

## Prime Network Services Controller Upgrade Matrix

The following table lists the supported upgrade paths for Prime Network Services Controller.



**Note** Please make sure to have 5GB of space free in bootflash directory before proceeding with upgrade process.

**Table 1: PNSC Upgrade Path**

Initial Version	Intermediate State(s)	Final Version
2.0.3	2.1 to 3.0.2g to 3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
2.1	3.0.2 to 3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
3.0.2	3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
3.2.1d	3.4.1d to 3.5.1a	3.5.1b
3.2.2b	3.4.1d to 3.5.1a	3.5.1b
3.4.1b	3.4.1d to 3.5.1a	3.5.1b
3.4.1c	3.4.1d to 3.5.1a	3.5.1b

Initial Version	Intermediate State(s)	Final Version
3.4.1d	3.5.1a	3.5.1b
3.4.2a	3.5.1a	3.5.1b
3.4.2b	3.4.2d	3.5.1b
3.4.2c	3.5.1a	3.5.1b
3.4.2d	N/A	3.5.1b
3.5.1a	N/A	3.5.1b

## Important Notes

The following topics provide important information for using Prime Network Services Controller.

### Cloned Linux Virtual Machines

When Linux virtual machines are cloned, new MAC addresses are assigned. This causes a MAC address mismatch between the VM settings and the Linux Guest OS. If you encounter this situation, the following message is displayed:

```
The Guest OS either does not contain interface configuration for the VM NICs or the
interfaces are explicitly disabled.
```

For information on how to resolve the MAC address mismatch, see the [VMware Knowledge Base](#).

### Editing Firewall Interfaces

We recommend that you do not edit the data interfaces of compute or edge firewalls. Changing the data interface via the Prime Network Services Controller GUI stops communication between the Cisco Nexus 1000VE VEM link and the firewall, and thereby stops vPath traffic.

If you change the data interfaces of compute or edge firewalls via the Prime Network Services Controller GUI, make the appropriate configuration changes on the Cisco Nexus 1000VE.

### Searching with Special Characters

Searching for organization names does not work if the organization names include special characters, such as \$.

### User Account Password Expiration

When adding a user account, the administrator can choose to expire the account password and select the date on which it expires. When the expiration date is reached, the account is disabled and the user cannot log in to Prime Network Services Controller until a user with administrator privileges extends the expiration date.

## Workflow for Automatically Deploying Network Services

Prime Network Services Controller enables you to automatically deploy compute firewall and load balancer network services by preparing the required networks, defining organizational profiles by configuring service automation policies, and assigning the organizational profiles to the required organization in the tenant hierarchy.

The following table identifies the tasks required to configure Prime Network Services Controller for automatic network service deployment, the related documentation, and the minimum role required for each task.

Task	Related Documentation	Role Required
<p>1. Confirm that the following prerequisites are met:</p> <ul style="list-style-type: none"> <li>• Prime Network Services Controller has been installed and is accessible from VMware.</li> <li>• In Prime Network Services Controller, VMware vCenter has been added as a VM Manager.</li> <li>• The Prime Network Services Controller Device Adapter has been installed and is registered with Prime Network Services Controller.</li> </ul>	<i>Cisco Prime Network Services Controller 3.5.1b Installation Guide.</i>	admin
2. Import service images. Supported service devices are VSG compute firewalls .	<a href="#">Importing Service Images, on page 8</a>	admin
3. Configure Management, HA, and vPath networks and subnetworks at root.	<a href="#">Configuring Networks for Network Service Deployment, on page 9</a>	admin
4. Create the policies and profiles for the network services.	<a href="#">Adding a Device Profile, on page 10</a>	admin
5. Create organizational (Org) profiles and add service automation definitions to each profile.	<a href="#">Configuring an Org Profile for Automatic Service Deployment, on page 11</a>	admin
6. In Tenant Management, create the organization where the network services will be deployed and assign an Org profile.	<a href="#">Creating an Organization and Assigning an Org Profile, on page 12</a>	admin or tenant-admin
7. Add a network to the organization to deploy the network service.	<a href="#">Deploying a Network Service, on page 12</a>	tenant-admin
8. Configure additional policies and profiles as needed.	<a href="#">Configuring Additional Policies and Profiles for Network Services, on page 13</a>	tenant-admin
9. Removing an automatically deployed compute firewall network service.	<a href="#">Deleting an Automatically Deployed Compute Firewall Service, on page 13</a>	tenant-admin

## Importing Service Images

enables you to import service images that you can then use to instantiate a device or service VM.

After you import an image, automatically places the file in the correct location and populates the Images table.



**Before you begin**

Confirm that the service images are available for importing into .

**Procedure**

- 
- Step 1** Choose **Resource Management > Resources > Images**.
- Step 2** Click **Import Service Image**.
- Step 3** In the Importing Service Image Dialog box:
- a) Enter a name and description for the image you are importing.
  - b) In the Type field, choose the type of image to import.
  - c) In the Version field, enter a version number that you want to assign to the image.
  - d) In the Import area, provide the following information, and then click **OK**:
    - Protocol to use for the import operations: FTP, SCP, or SFTP.
    - Hostname or IP address of the remote host with the images.
    - Account username and password for the remote host.
    - Absolute image path and filename, starting with a slash (/).
- 

**Configuring Networks for Network Service Deployment**

To automatically deploy network services, you must configure the following networks with subnetworks at the root level:

- A management network—This network provides IP addresses for the automatically deployed services.
- A vPath service network—This network is required for deploying compute firewall network services.
- An HA network—This network is required for deploying compute firewall network services in HA mode.

The following guidelines apply when creating networks for automated network service deployment:

- You must use the same Distributed Virtual Switch (DVS) port group for all networks.
- The port group must be accessible from Prime Network Services Controller.

**Procedure**

- 
- Step 1** Choose **Resource Management > Managed Resources > root**.
- Step 2** In the Networks tab, click **Add**.
- Step 3** To add a management network, provide the following information and click **OK**:
- a) Enter the network name and description.
  - b) In the Role field, choose **Management**.
  - c) In the VM Manager area, choose the VMM and the port group.

- Step 4** To add an HA network to support compute firewall services in HA mode, provide the following information and click **OK**:
- Enter the network name and description.
  - In the Role field, choose **HA**.
  - In the VM Manager area, choose the VMM and the port group.
- Step 5** To add a vPath service network, provide the following information and click **OK**:
- Enter the network name and description.
  - In the Role field, choose **Service\_Vpath**.
  - In the VM Manager area, choose the VMM and the same port group that you chose for the management network.
- Step 6** For each management and vPath network, add a subnetwork as follows:
- Choose the network and click **Add** in the Subnetworks area.
  - In the Add Subnetwork dialog box, enter the netmask, gateway, and name for the subnetwork.
  - In the IP Address Range area, click **Add** and enter the starting and ending IP addresses for the IP address range for the subnetwork.
  - Click **OK** to accept your changes.

## Adding a Device Profile

A device profile is a set of custom security attributes and device policies. Adding a device profile enables you to specify the DNS and NTP servers that the service device is to use in addition to SNMP, syslog, and authentication policies.

### Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Device Profiles**.
- Step 2** Click **Add Device Profile**.
- Step 3** In the General tab in the Add Device Profile dialog box:
- Enter the profile name and description.
  - If required, select the time zone.
  - Add a DNS server and domain.
  - Add an NTP server.
  - For the SNMP, Syslog, and Auth policies, either use the default policy, select another existing policy, or create a new policy.
  - In the Policy Engine Logging field, indicate whether logging is enabled or disabled.
- Step 4** In the Advanced tab, specify the fault, core file, and log file policies to use for the for the Prime Network Services Controller policy agent, and then click **OK**.

## NTP Behavior Post PNSC Upgrade

NTP service does not come up on the terminal when PNSC is upgraded from the previous releases to Release 3.4.1d or later. To access the NTP service, you need to re-login into the same terminal or start a new terminal.

## Configuring an Org Profile for Automatic Service Deployment

A network service automation policy specifies the profiles, image, and credentials to be used when deploying a network service. Depending on the type of service, different options are available. For each Org profile, you can create a definition for each network service type: compute firewall and load balancer.

### Procedure

- Step 1** Choose **Tenant Management > root > Profile Name > Create** and enter a name for the Org profile.
- Step 2** Choose **Resource Management > Managed Resources > root > Service Deployment > Org Profile > profile** where *profile* is the profile you created in the first step.
- Step 3** To enable automatic deployment of the service, check the **Enable Automation** check box.
- Step 4** Click **Compute Firewall Service** or **Load Balancer Service** to deploy that service using this Org profile.
- Step 5** In the Network Service dialog box, provide the information as described in the following table, and then click **OK**. Different fields are available depending on the type of service.

**Note** You must set the Admin state to *enable* to deploy the service.

Field	Description
<b>Properties</b>	
Admin State	Whether the Administrative state of the network service is enabled or disabled. You must choose <b>enable</b> to deploy the service.
HA Mode	(Compute firewall only) Whether the service should operate in standalone or active standby mode.
Deployment Size	(Compute firewall only) Size of the deployment: small, medium, or large. For more information, see the online help.
Enable License	(Load balancer only) Check the check box to use an existing license for the service.
Feature License	(Load balancer only) Choose the license to use for the service.
<b>Profiles</b>	
Device Config Profile	The device configuration profile to use for the service.
<b>Access</b>	
Login User	User account for administrative access.
Login Password	User password for administrative access.
Confirm Password	Confirming password entry.

Field	Description
<b>VM Image Table</b>	
<i>image</i>	Choose the service image to use to deploy the network service.

## Creating an Organization and Assigning an Org Profile

After you configure the service automation policies for an Org profile, create the tenant or other organization on which you want to deploy the network service. Creating the organization includes assigning the Org profile that will be used to automatically deploy network services.

### Before you begin

Determine the level in the hierarchy where the organization that will be configured to automatically deploy network services will reside.

### Procedure

- Step 1** Choose **Tenant Management > root** and navigate to the level where you want to add the organization that will deploy network services using the Org profile. For example, to assign an Org profile to a tenant, click **Create Tenant** at the root level. Similarly, to assign an Org profile at the Application level, navigate to the VDC and click **Create Application**.
- Step 2** In the Create dialog box, enter a name for the organization and, from the **Profile** drop-down list, choose the Org profile to assign to the organization.
- Step 3** Click **OK**.

## Deploying a Network Service

After you create the organization where network services will be deployed and assign an Org profile, you can deploy the network service. To deploy the network service, create a network on the organization.

The following guidelines apply when deploying a network service:

- Only one compute firewall service can be automatically instantiated for an organization by adding a Layer 2 network with any role.
- Only one load balancer service can be automatically instantiated for an organization by adding a Layer 2 network with the role Service\_LB.

### Before you begin

- For a compute firewall network service, confirm that Management and vPath networks have been configured at root.

**Procedure**

- 
- Step 1** Choose **Resource Management > Managed Resources > root > tenant** or **tenant > org**.
- Step 2** In the Networks tab, create the network for the service to be deployed, being sure to choose the correct role for the service.  
The network service is then automatically deployed. To monitor progress, choose **Resource Management > Managed Resources > root > tenant** or **tenant > org** and click the **Network Services** tab.
- 

**Configuring Additional Policies and Profiles for Network Services**

After deploying a network service, you might need to apply new policies and profiles to the network service. To apply new policies and profiles to a specific, deployed network service, create the policies and profiles at the same organizational level as the deployed service. For example, if a compute firewall network service has been deployed for a VDC, create the new policies and profiles at the VDC level.

**Deleting an Automatically Deployed Compute Firewall Service**

You cannot delete an automatically deployed compute firewall by deleting the network of a specific client. However, you can delete an automatically deployed compute firewall service from the Managed Resources Network Services tab in Prime Network Services Controller.



- 
- Note** If you delete the vPath network from root, it will remove all compute firewalls from all tenants and subordinate organizations.
- 

**Procedure**

- 
- Step 1** Choose the organization in which the network service has been deployed (**Resource Management > Managed Resources > root > tenant > org**).
- Step 2** Click the **Network Services** tab.
- Step 3** Choose the automatically deployed compute firewall service and click **Delete**.
- 

**Using the Bug Search Tool**

This topic explains how to use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

**Procedure**

- 
- Step 1** Go to <http://tools.cisco.com/bugsearch>.
- Step 2** In the Log In screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.

**Note** If you do not have a Cisco.com username and password, you can register for them at <http://tools.cisco.com/RPF/register/register.do>.

**Step 3** To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.

**Step 4** To search for bugs in the current release:

- a) In the Search For field, enter Cisco Prime Network Services Controller and press **Enter**. Leave the other fields empty.
- b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

**Tip** To export the results to a spreadsheet, click the **Export Results to Excel** link.

## Open Bugs

There are no open bugs for Cisco Prime Network Services Controller, Release 3.5.1b.

## Resolved Bugs

The following table lists the resolved bugs in Prime Network Services Controller, Release 3.5.1b.

Bug ID	Description
<a href="#">CSCvg34973</a>	NSC: Core in resource-mgr-svc_res_enterpriseAG

## Related Documentation

### Prime Network Services Controller

The Prime Network Services Controller documentation is available on [Cisco.com](#) at the following URL:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-services-controller/tsd-products-support-series-home.html>

### Cisco Nexus 1000VE Series Switch Documentation

The Cisco Nexus 1000VE documentation is available on [Cisco.com](#) at the following URL:

<https://www.cisco.com/c/en/us/support/switches/nexus-1000ve/series.html>

### Cisco Prime Data Center Network Manager Documentation

The Cisco Prime Data Center Network Manager (DCNM) documentation is available on [Cisco.com](#) at the following URL:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/tsd-products-support-series-home.html>

### Cisco Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway (VSG) documentation is available on [Cisco.com](#) at the following URL:

<http://www.cisco.com/c/en/us/support/switches/virtual-security-gateway/tsd-products-support-series-home.html>

## Accessibility Features in Prime Network Services Controller

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact [accessibility@cisco.com](mailto:accessibility@cisco.com).

### 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.

---

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 NON-INFRINGEMENT 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](http://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)

© 2020 Cisco Systems, Inc. All rights reserved.