# IPv6 Network Management Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 920 Series)

**First Published:** 2014-07-28

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS


CHAPTER 1 **SNMP over IPv6** 1

Finding Feature Information 1

Information About SNMP over IPv6 1

SNMP over an IPv6 Transport 1

How to Configure SNMP over IPv6 2

Configuring an SNMP Notification Server over IPv6 2

Configuration Examples for SNMP over IPv6 4

Examples: Configuring an SNMP Notification Server over IPv6 4

Additional References 5

Feature Information for SNMP over IPv6 6

CHAPTER 2 **IPv6 CNS Agents** 7

Finding Feature Information 7

Information About IPv6 CNS Agents 7

CNS Agents 7

CNS Configuration Agent 8

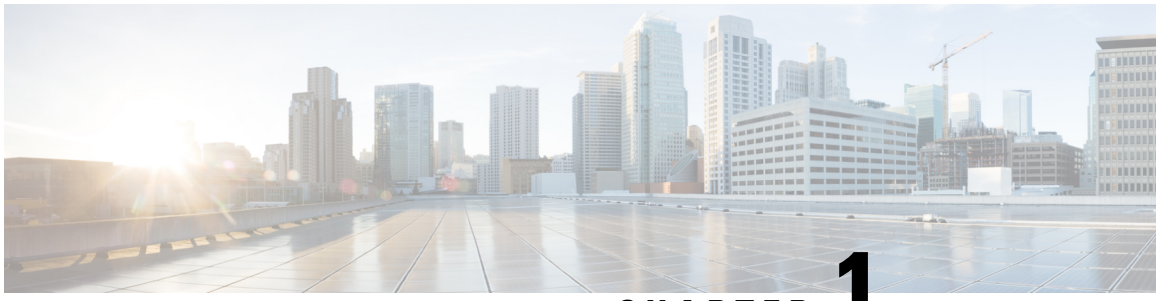
CNS Event Agent 8

CNS EXEC Agent 8

CNS Image Agent 8

Additional References for IPv6 IOS Firewall 9

Feature Information for IPv6 CNS Agents 9



CHAPTER 1

# SNMP over IPv6

Simple Network Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can perform SNMP queries and receive SNMP notifications from a device running IPv6.


- Finding Feature Information, on page 1
- Information About SNMP over IPv6, on page 1
- How to Configure SNMP over IPv6, on page 2
- Configuration Examples for SNMP over IPv6, on page 4
- Additional References, on page 5
- Feature Information for SNMP over IPv6, on page 6


# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

# Information About SNMP over IPv6

## SNMP over an IPv6 Transport

Simple Network Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can perform SNMP queries and receive SNMP notifications from a device running IPv6 software. The SNMP agent and related MIBs have been enhanced to support IPv6 addressing. This feature uses the data encryption standard (3DES) and advanced encryption standard (AES) message encryption.

# How to Configure SNMP over IPv6

## Configuring an SNMP Notification Server over IPv6

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the device. Optionally, you can specify one or more of the following characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.
- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

You can configure one or more community strings. To remove a specific community string, use the **no snmp-server community** command.

The **snmp-server host** command specifies which hosts will receive SNMP notifications, and whether you want the notifications sent as traps or inform requests. The **snmp-server enable traps** command globally enables the production mechanism for the specified notification types (such as Border Gateway Protocol [BGP] traps, config traps, entity traps, and Hot Standby Router Protocol [HSRP] traps).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
4. **snmp-server engineID remote** {*ipv4-ip-address* | *ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
5. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list* ] {*acl-number* | *acl-name*}]
6. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
7. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*} ]
8. **snmp-server enable traps** [*notification-type*] [**vrrp**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server community** *string* [**view** *view-name*] [**ro** \| **rw**] [**ipv6** *nacl*] [*access-list-number*]<br>**Example:**<br>`Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2` | Defines the community access string. |
| **Step 4** | **snmp-server engineID remote** {*ipv4-ip-address* \| *ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*<br>**Example:**<br>`Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6` | (Optional) Specifies the name of the remote SNMP engine (or copy of SNMP). |
| **Step 5** | **snmp-server group** *group-name* {**v1** \| **v2c** \| **v3** {**auth** \| **noauth** \| **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list* ] {*acl-number* \| *acl-name*}]<br>**Example:**<br>`Device(config)# snmp-server group public v2c access ipv6 public2` | (Optional) Configures a new SNMP group, or a table that maps SNMP users to SNMP views. |
| **Step 6** | **snmp-server host** {*hostname* \| *ip-address*} [**vrf** *vrf-name*] [**traps** \| **informs**] [**version** {**1** \| **2c** \| **3** [**auth** \| **noauth** \| **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]<br>**Example:**<br>`Device(config)# snmp-server host host1.com 2c vrf trap-vrf` | Specifies the recipient of an SNMP notification operation.<br>• Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications. |
| **Step 7** | **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** \| **v2c** \| **v3** [**encrypted**] [**auth** {**md5** \| **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** \| **3des** \| **aes** {**128** \| **192** \| **256**}} *privpassword*] {*acl-number* \| *acl-name*} ]<br>**Example:**<br>`Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2` | (Optional) Configures a new user to an existing SNMP group.<br>**Note** You cannot configure a remote user for an address without first configuring the engine ID for that remote host. This is a restriction imposed in the design of these commands; if you try to configure the user before the host, you will receive a warning message, and the command will not be executed. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **snmp-server enable traps** [*notification-type*] [**vrrp**]<br>**Example:**<br>`Device(config)# snmp-server enable traps bgp` | Enables sending of traps or informs, and specifies the type of notifications to be sent.<br>• If a value for the *notification-type* argument is not specified, all supported notification will be enabled on the device.<br>• To discover which notifications are available on your device, enter the **snmp-server enable traps ?** command. |

# Configuration Examples for SNMP over IPv6

## Examples: Configuring an SNMP Notification Server over IPv6

The following example permits any SNMP to access all objects with read-only permission using the community string named public. The device also will send Border Gateway Protocol (BGP) traps to the IPv4 host 172.16.1.111 and IPv6 host 3ffe:b00:c18:1::3/127 using SNMPv1 and to the host 172.16.1.27 using SNMPv2c. The community string named public will be sent with the traps.

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 172.16.1.27 version 2c public
Device(config)# snmp-server host 172.16.1.111 version 1 public
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

### Example: Associate an SNMP Server Group with Specified Views

In the following example, the SNMP context A is associated with the views in SNMPv2c group GROUP1 and the IPv6 named access list public2:

```
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
access ipv6 public2
```

### Example: Create an SNMP Notification Server

The following example configures the IPv6 host as the notification server:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group public v2c access ipv6 public2
Device(config)# snmp-server host host1.com 2c vrf trap-vrf
Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6
```

```
public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

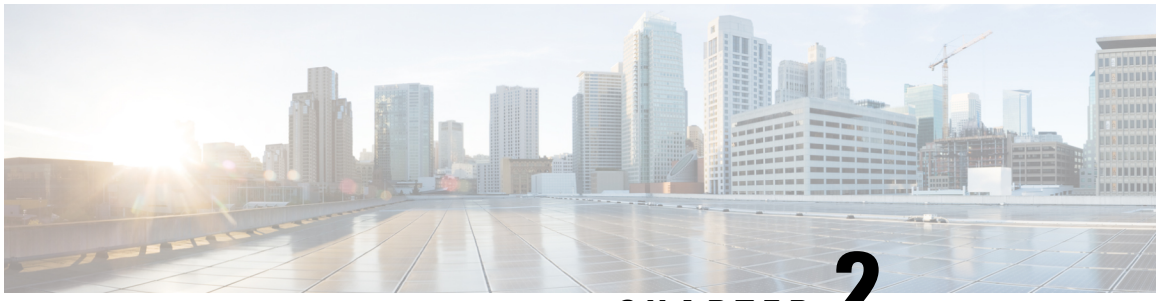
# Feature Information for SNMP over IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 1: Feature Information for SNMP over IPv6***

| Feature Name | Releases | Feature Information |
|---|---|---|
| SNMP over IPv6 | Cisco IOS XE Release 3.13.0S | This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D). |



CHAPTER 2

# IPv6 CNS Agents

IPv6 addressing is supported in the Cisco Networking Services (CNS) subsystem. CNS is a foundation technology for linking users to networking services and provides the infrastructure for the automated configuration of large numbers of network devices. The document describes CNS agents supported in IPv6.


- Finding Feature Information, on page 7
- Information About IPv6 CNS Agents, on page 7
- Additional References for IPv6 IOS Firewall, on page 9
- Feature Information for IPv6 CNS Agents, on page 9


# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

# Information About IPv6 CNS Agents

## CNS Agents

IPv6 addressing is supported in the Cisco Networking Services (CNS) subsystem. CNS is a foundation technology for linking users to networking services, and it provides the infrastructure for the automated configuration of large numbers of network devices. Many IPv6 networks are complex, with many devices, and each device must be configured individually. When standard configurations do not exist or have been modified, the time involved in initial installation and subsequent upgrading is considerable. ISPs need a method for sending out partial configurations to introduce new services.

To address all these issues, CNS was designed to provide "plug-and-play" network services using a central directory service and distributed agents. CNS features include CNS agents and a flow-through provisioning structure. CNS flow-through provisioning uses the CNS configuration and event agents to provide an automated workflow, eliminating the need for an onsite technician.

IPv6 addressing supports the CNS agents described in the following sections:

## CNS Configuration Agent

The CNS configuration agent is involved in the initial configuration and subsequent partial configurations on a Cisco device. The configuration agent uses a CNS configuration engine to provide methods for automating initial Cisco device configurations, incremental configurations, and synchronized configuration updates, and the configuration engine reports the status of the configuration load as an event to which a network monitoring or workflow application can subscribe.

## CNS Event Agent

The CNS event agent provides a transport connection to the CNS event bus for all other CNS agents. No event can be sent to the device by the configuration engine until the CNS event agent is operational and has successfully built a connection between the configuration engine and the device.

The event agent uses a CNS configuration engine to provide methods for automating initial Cisco device configurations, incremental configurations, and synchronized configuration updates.

## CNS EXEC Agent

The CNS EXEC agent allows a remote application to execute a CLI command in EXEC mode on a Cisco device by sending an event message that contains the command.

## CNS Image Agent

Administrators maintaining large networks of Cisco devices need an automated mechanism to load image files onto large numbers of remote devices. Network management applications are useful to determine which images to run and how to manage images received from the Cisco online software center. Other image distribution solutions do not scale to cover thousands of devices and cannot distribute images to devices behind a firewall or using Network Address Translation (NAT). The CNS image agent enables the managed device to initiate a network connection and request an image download allowing devices using NAT, or behind firewalls, to access the image server.

The CNS image agent can be configured to use the CNS event bus. To use the CNS event bus, the CNS event agent must be enabled and connected to the CNS event gateway in the CNS Configuration Engine. The CNS image agent can also use an HTTP server that understands the CNS image agent protocol. Deployment of CNS image agent operations can use both the CNS event bus and an HTTP server.

# Additional References for IPv6 IOS Firewall

### Related Documents

| Related Topic | Document Title |
|---|---|
| Security commands | • *Cisco IOS Security Command Reference: Commands A to C*<br>• *Cisco IOS Security Command Reference: Commands D to L*<br>• *Cisco IOS Security Command Reference: Commands M to R*<br>• *Cisco IOS Security Command Reference: Commands S to Z* |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS IPv6 features | *Cisco IOS IPv6 Feature Mapping* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for IPv6 CNS Agents

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 2: Feature Information for IPv6 CNS Agents***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 CNS Agents | Cisco IOS XE Release 3.13.0S | This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D). |