



SNMP over IPv6

- [SNMP over IPv6, on page 1](#)
- [SNMP over an IPv6 Transport, on page 1](#)
- [Configuring an SNMP Notification Server over IPv6, on page 1](#)
- [Examples: Configuring an SNMP Notification Server over IPv6, on page 3](#)

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.

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.

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, and entity traps).

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	snmp-server community <i>string</i> [view <i>view-name</i>] [ro rw] [ipv6 nacl] [<i>access-list-number</i>] Example: <pre>Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2</pre>	Defines the community access string.
Step 4	snmp-server engineID remote { <i>ipv4-ip-address</i> <i>ipv6-address</i> } [udp-port <i>udp-port-number</i>] [vrf <i>vrf-name</i>] <i>engineid-string</i> Example: <pre>Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6</pre>	(Optional) Specifies the name of the remote SNMP engine (or copy of SNMP).
Step 5	snmp-server group <i>group-name</i> { v1 v2c v3 { auth noauth priv }} [context <i>context-name</i>] [read <i>read-view</i>] [write <i>write-view</i>] [notify <i>notify-view</i>] [access [ipv6 <i>named-access-list</i>] { <i>acl-number</i> <i>acl-name</i> }] Example: <pre>Device(config)# snmp-server group public v2c access ipv6 public2</pre>	(Optional) Configures a new SNMP group, or a table that maps SNMP users to SNMP views.
Step 6	snmp-server host { <i>hostname</i> <i>ip-address</i> } [vrf <i>vrf-name</i>] [traps informs] [version { 1 2c 3 [auth noauth priv]}] <i>community-string</i> [udp-port <i>port</i>] [<i>notification-type</i>] Example:	Specifies the recipient of an SNMP notification operation. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
	Device(config)# snmp-server host host1.com 2c vrf trap-vrf	
Step 7	<p>snmp-server user <i>username group-name</i> [remote <i>host [udp-port port]</i>] {v1 v2c v3 [encrypted] [auth {md5 sha} <i>auth-password</i>]} [access [ipv6 nacl] [priv {des 3des aes {128 192 256} } <i>privpassword</i>] {<i>acl-number</i> <i>acl-name</i>}]</p> <p>Example:</p> <pre>Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2</pre>	<p>(Optional) Configures a new user to an existing SNMP group.</p> <p>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.</p>
Step 8	<p>snmp-server enable traps [<i>notification-type</i>] [vrrp]</p> <p>Example:</p> <pre>Device(config)# snmp-server enable traps bgp</pre>	<p>Enables sending of traps or informs, and specifies the type of notifications to be sent.</p> <ul style="list-style-type: none"> • If a value for the <i>notification-type</i> argument is not specified, all supported notification will be enabled on the device. • To discover which notifications are available on your device, enter the snmp-server enable traps ? command.

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 SNMP FLASH 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 flash
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
```