SNMP Support over VPNs--Context-Based Access Control

Last Updated: June 30, 2011

The SNMP Support over VPNs--Context-Based Access Control feature provides the infrastructure for multiple Simple Network Management Protocol (SNMP) context support in Cisco IOS software and VPN-aware MIB infrastructure using the multiple SNMP context support infrastructure.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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.

Restrictions for SNMP Support over VPNs--Context-Based Access Control

- If you delete an SNMP context using the **no snmp-server context** command, all SNMP instances in that context are deleted.
- Not all MIBs are VPN-aware.

Information About SNMP Support over VPNs--Context-Based Access Control

SNMP Versions and Security

Cisco IOS software supports the following versions of SNMP:

- SNMPv1--Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c--The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.
- SNMPv3--Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 3413 to 3415. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network.

For more information about SNMP Versions, see the " Configuring SNMP Support " module in the *Cisco IOS Network Management Configuration Guide* .

SNMPv1 or SNMPv2 Security

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP version 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP version 3 performs. To configure the SNMP Support over VPNs--Context-Based Access Control feature when using SNMP version 1 or SNMP version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if it comes in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, it is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from snooping a clear

text community string to query the VPN's data. These methods of source address validation are not as secure as using SNMPv3.

SNMPv3 Security

If you are using SNMPv3, the security name should always be associated with authentication or privileged passwords. Source address validation is not performed on SNMPv3 users. To ensure that a VPN's user has access only to context associated to the VPN and cannot see the MIB data of other VPNs, you must configure a minimum security level of AuthNoPriv.

On a provider edge (PE) router, a community can be associated with a VRF to provide source address validation. However, on a customer edge (CE) router, if source address validation is to be provided, you must associate a source address with the community list by using an access control list.

If you are using SNMPv3, the security name or security password of the users of a VPN should be unknown to users of other VPNs. Cisco recommends not to use SNMPv3 nonauthorized users if you need security of management information.

SNMP Notification Support over VPNs

The SNMP Notification Support over VPNs feature allows the sending and receiving of SNMP notifications (traps and informs) using VPN routing and forwarding (VRF) instance tables. In particular, this feature adds support to Cisco IOS software for the sending and receiving of SNMP notifications (traps and informs) specific to individual VPNs.

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high-connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet over IP, Frame Relay, or ATM networks.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (formerly known as CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support for VPNs--Context-Based Access Control feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The associated VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

VPN-Aware SNMP

The SNMP Support for VPNs--Context-Based Access Control feature extends the capabilities of the SNMP Notification Support for VPNs feature and enables SNMP to differentiate between incoming packets from different VPNs.

When the SNMP Support for VPNs--Context-Based Access Control feature is configured, SNMP accepts requests on any configured VRF and returns responses to the same VRF. A trap host also can be associated with a specific VRF. The configured VRF is then used for sending out traps; otherwise, the default routing table is used. You also can associate a remote user with a specific VRF. You also can configure the VRFs from which SNMP should accept requests. Any requests coming from VRFs that are not specified are dropped.

IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VRF instances with SNMP community strings. When a VRF instance is

associated with an SNMP community string, SNMP processes the requests coming in for a particular community string only if the requests are received from the configured VRF. If the community string contained in the incoming packet does not have a VRF associated with it, the community string will be processed only if it came in through a non-VRF interface.

You also can enable or disable authentication traps for SNMP packets dropped due to VRF mismatches. By default if SNMP authentication traps are enabled, VRF authentication traps are also enabled.

VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

The RD is either an autonomous system number (ASN)-relative RD, in which case it comprises an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it comprises an IP address and an arbitrary number.

You can enter an RD in either of these formats:

- 16-bit ASN: your 16-bit number: For example, 101:3.
- 32-bit IP address: your 32-bit number: For example, 192.168.122.15:1.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about other VPN userss on the same networking device.

VPN-aware SNMP requires an agreement between SNMP manager and agent entities operating in a VPN environment on a mapping between the SNMP security name and the VPN ID. This mapping is created by using multiple contexts for the SNMP data of different VPNs through the configuration of the SNMP-VACM-MIB. The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space associated with a user's access type in the context associated with the user of that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values in the context of a VPN:

- In the first phase, the username is authenticated. This phase ensures that the user is authenticated and authorized for SNMP access.
- In the second phase, the user is authorized for the SNMP access requested to the group objects under consideration of the configured SNMP context. This phase is called the access control phase.
- In the third phase, access is made to a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

How to Configure SNMP Support over VPNs--Context-Based Access Control

Configuring an SNMP Context and Associating the SNMP Context with a VPN

Perform this task to configure an SNMP context and to associate the SNMP context with a VPN.

Note

- Only the following MIBs are context-aware. All the tables in these MIBs can be polled:
  - CISCO-IPSEC-FLOW-MONITOR-MIB (Cisco IOS Release 12.4T and later releases)
  - CISCO-IPSEC-MIB (Cisco IOS Release 12.4T and later releases)
  - CISCO-PING-MIB
  - IP-FORWARD-MIB
  - MPLS-LDP-MIB
- Only two SNMP variables in the IP-FORWARD-MIB can be polled: 1.3.6.1.2.1.4.24.3 (ipCidrRouteNumber - Scalar) and 1.3.6.1.2.1.4.24.4.1 (ipCidrRouteEntry - Table).

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server context** *context-name*
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **context** *context-name*
7. **route-target** {**import** | **export** | **both**} *route-target-ext-community*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** ```Router> enable```	Enables privileged EXEC mode. - Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**snmp-server context** *context-name* **Example:** Router(config)# snmp-server context context1	Creates and names an SNMP context.
Step 4	**ip vrf** *vrf-name* **Example:** Router(config)# ip vrf vrf1	Configures a VRF routing table and enters VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** Router(config-vrf)# rd 100:120	Creates a VPN route distinguisher.
Step 6	**context** *context-name* **Example:** Router(config-vrf)# context context1	Associates an SNMP context with a particular VRF. **Note** In Cisco IOS Release 15.0(1)M and later releases, the **context** command is replaced by the **snmp context** command. See the Network Management Command Reference for more information.
Step 7	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** Router(config-vrf)# route-target export 100:1000	(Optional) Creates a route-target extended community for a VRF.

Configuring SNMP Support and Associating an SNMP Context

Perform this task to configure SNMP support and associate it with an SNMP context.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*}]

4. **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*]]

5. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}

6. **snmp-server enable traps** [*notification-type*] [**vrrp**]

7. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]

8. **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*]

9. **snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*][**target-list** *upn-list-name*]

10. **snmp mib target list** *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}

11. **no snmp-server trap authentication vrf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1**	**v2c**	**v3** [**encrypted**] [**auth** {**md5**	**sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des**	**3des**	**aes** {**128**	**192**	**256**}} *privpassword*] {*acl-number*	*acl-name*}] **Example:** `Router(config)# snmp-server user customer1 group1 v1`	Configures a new user to an SNMP group.

	Command or Action	Purpose
Step 4	**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*]] **Example:** Router(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1	Configures a new SNMP group or a table that maps SNMP users to SNMP views. • Use the **context** *context-name* keyword argument pair to associate the specified SNMP group with a configured SNMP context.
Step 5	**snmp-server view** *view-name oid-tree* {**included** | **excluded**} **Example:** Router(config)# snmp-server view view1 ipForward included	Creates or updates a view entry.
Step 6	**snmp-server enable traps** [*notification-type*] [**vrrp**] **Example:** Router(config)# snmp-server enable traps	Enables all SNMP notifications (traps or informs) available on your system.
Step 7	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] **Example:** Router(config)# snmp-server community public view view1 rw	Sets up the community access string to permit access to the SNMP.
Step 8	**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*] **Example:** Router(config)# snmp-server host 10.0.0.1 vrf vrf1 public udp-port 7002	Specifies the recipient of an SNMP notification operation.
Step 9	**snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*][**target-list** *upn-list-name*] **Example:** Router(config)# snmp mib community-map community1 context context1 target-list commAVpn	Associates an SNMP community with an SNMP context, Engine ID, or security name.

Command or Action	Purpose
Step 10 **snmp mib target list** *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*} **Example:** `Router(config)# snmp mib target list commAVpn vrf vrf1`	Creates a list of target VRFs and hosts to associate with an SNMP community.
Step 11 **no snmp-server trap authentication vrf** **Example:** `Router(config)# no snmp-server trap authentication vrf`	(Optional) Disables all SNMP authentication notifications (traps and informs) generated for packets received on VRF interfaces. • Use this command to disable authentication traps only for those packets on VRF interfaces with incorrect community associations.

Configuration Examples for SNMP Support over VPNs-- Context-Based Access Control

Example Configuring Context-Based Access Control

The following configuration example shows how to configure the SNMP Support over VPNs--Context-Based Access Control feature for SNMPv3:

Note   In Cisco IOS Release 15.0(1)M and later releases, the **context** command is replaced by the **snmp context** command. See the Network Management Command Reference for more information.

```
snmp-server context A
snmp-server context B
ip vrf CustomerA
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!
ip vrf CustomerB
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!
interface Ethernet3/1
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 192.168.2.1 255.255.255.0

interface Ethernet3/2
 description Belongs to VPN B
```

```
 ip vrf forwarding CustomerB
 ip address 192.168.2.2 255.255.255.0

snmp-server user CustomerAv3authusr CustomerAv3grpauth v3 auth md5 passwdA
snmp-server user CustomerBv3authusr CustomerBv3grpauth v3 auth md5 passwdB
snmp-server group CustomerAv3grpauth v3 auth context A read CustomerAv3view write
CustomerAv3view notify CustomerAv3view
snmp-server group CustomerBv3grpauth v3 auth context B read CustomerBv3view write
CustomerBv3view notify CustomerBv3view
snmp-server view view1 internet included
snmp-server view view1 internet.6.3.16 included
snmp-server view view1 internet.6.3.17 included
snmp-server view view1 internet.6.3.18 included
snmp-server view CustomerAv3view ipForward included
snmp-server view CustomerAv3view ciscoPingMIB included
snmp-server view CustomerBv3view ipForward included
snmp-server view CustomerBv3view ciscoPingMIB included
snmp-server community public view view1 rw
snmp-server enable traps
snmp-server host 192.168.2.3 vrf CustomerA version 3 auth CustomerAv3authusr udp-port
7002
snmp-server host 192.168.2.4 vrf CustomerB version 3 auth CustomerBv3authusr udp-port
7002
```

The following configuration example shows how to configure the SNMP Support over VPNs--Context-Based Access Control feature for SNMPv1 or SNMPv2:

Note   In Cisco IOS Release 15.0(1)M and later releases, the **context** command is replaced by the **snmp context** command. See the Network Management Command Reference for more information.

```
snmp-server context A
snmp-server context B
ip vrf Customer_A
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!
ip vrf Customer_B
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!
interface Ethernet3/1
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 192.168.2.1 255.255.255.0

interface Ethernet3/2
 description Belongs to VPN B
 ip vrf forwarding CustomerB
 ip address 192.168.2.2 255.255.255.0
snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c
snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB
snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included
snmp-server enable traps
snmp-server host 192.168.2.3 vrf CustomerA commA udp-port 7002
snmp-server host 192.168.2.4 vrf CustomerB commB udp-port 7002
snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
```

```
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Network Management commands	*Cisco IOS Network Management Command Reference*
SNMP configuration	" Configuring SNMP Support " chapter in the *Cisco IOS Network Management Configuration Guide*
SNMP Support for VPNs	SNMP Notification Support for VPNs

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-PING-MIB • IP-FORWARD-MIB • SNMP-VACM-MIB, *The View-based Access Control Model (ACM) MIB for SNMP*	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1441	*Introduction to version 2 of the Internet-standard Network Management Framework*
RFC 1442	*Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC	Title
RFC 1443	*Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1444	*Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1445	*Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1446	*Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1447	*Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1448	*Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1449	*Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1450	*Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 2571	*An Architecture for Describing SNMP Management Frameworks*
RFC 2576	*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

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 Support over VPNs--Context-Based Access Control

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 Support over VPNs--Context-Based Access Control***

Feature Name	Releases	Feature Information
SNMP Support over VPNs--Context-Based Access Control	12.0(23)S 12.2(25)S 12.2(31)SB2 12.2(33)SRA 12.2(33)SXH 12.3(2)T 15.0(1)M 15.0(1)S Cisco IOS XE Release 3.1.0SG	The SNMP Support over VPNs--Context-Based Access Control feature provides the infrastructure for multiple SNMP context support in Cisco IOS software and VPN-aware MIB infrastructure using the multiple SNMP context support infrastructure.

Glossary

MPLS VPN --Multiprotocol Label Switching Virtual Private Network

NMS --Network Management System. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

SNMP --Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

SNMP communities --Authentication scheme that enables an intelligent network device to validate SNMP requests.

SNMPv2c --Version 2c of the Simple Network Management Protocol. SNMPv2c supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

SNMPv3 --Version 3 of the Simple Network Management Protocol. Interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

UDP --User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VRF --A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.