Per VRF for TACACS+ Servers

First Published: March 1, 2004
Last Updated: June 29, 2010

The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers.

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 for Per VRF for TACACS+ Servers" section on page 8.

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

Contents

Prerequisites for Per VRF for TACACS+ Servers

- TACACS+ server access is required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Experience configuring TACACS+, AAA and per VRF AAA, and group servers is necessary.

Restrictions for Per VRF for TACACS+ Servers

- The VRF instance must be specified before per VRF for a TACACS+ server is configured.

Information About Per VRF for TACACS+ Servers

To configure the Per VRF for TACACS+ Servers feature, the following concept should be understood:

Per VRF for TACACS+ Servers Overview

The Per VRF for TACACS+ Servers feature allows per VRF AAA to be configured on TACACS+ servers. Prior to Cisco IOS Release 12.3(7)T, this functionality was available only on RADIUS servers.

How to Configure Per VRF for TACACS+ Servers

This section contains the following procedures:

Configuring Per VRF on a TACACS+ Server

The initial steps in this procedure are used to configure AAA and a server group, create a VRF routing table, and configure an interface. Steps 10 through 13 are used to configure the per VRF on a TACACS+ server feature:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **interface** *interface-name*
7. **ip vrf forwarding** *vrf-name*
8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*

11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

12. **ip vrf forwarding** *vrf-name*

13. **ip tacacs source-interface** *subinterface-name*

14. **exit**

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	`ip vrf` *vrf-name* **Example:** `Router (config)# ip vrf cisco`	Configures a VRF table and enters VRF configuration mode.
Step 4	`rd` *route-distinguisher* **Example:** `Router (config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF instance.

Step 5	`exit`
	
	Example:
	`Router (config-vrf)# exit`
		Exits VRF configuration mode.

Step 6	`interface` *interface-name* **Example:** `Router (config)# interface Loopback0`	Configures an interface and enters interface configuration mode.
Step 7	`ip vrf forwarding` *vrf-name* **Example:** `Router (config-if)# ip vrf forwarding cisco`	Configures a VRF for the interface.
Step 8	`ip address` *ip-address mask* [**secondary**] **Example:** `Router (config-if)# ip address 10.0.0.2 255.0.0.0`	Sets a primary or secondary IP address for an interface.

Step 9	`exit`
	
	Example:
	`Router (config-if)# exit`
		Exits interface configuration mode.

	Command or Action	Purpose
Step 10	**aaa group server tacacs+** *group-name* **Example:** Router (config)# aaa group server tacacs+ tacacs1	Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **Example:** Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco	Configures the IP address of the private TACACS+ server for the group server.
Step 12	**ip vrf forwarding** *vrf-name* **Example:** Router (config-sg-tacacs+)# ip vrf forwarding cisco	Configures the VRF reference of a AAA TACACS+ server group.
Step 13	**ip tacacs source-interface** *subinterface-name* **Example:** Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
Step 14	**exit** **Example:** Router (config-sg-tacacs)# exit	Exits server-group configuration mode.

Verifying Per VRF for TACACS+ Servers

To verify the per VRF TACACS+ configuration, perform the following steps:

Note The **debug** commands may be used in any order.

SUMMARY STEPS

1. **enable**

2. **debug tacacs authentication**

3. **debug tacacs authorization**

4. **debug tacacs accounting**

5. **debug tacacs packets**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`debug tacacs authentication`
	
	Example:
	`Router# debug tacacs authentication`
		Displays information about AAA/TACACS+ authentication.

Step 3	`debug tacacs authorization`
	
	Example:
	`Router# debug tacacs authorization`
		Displays information about AAA/TACACS+ authorization.

Step 4	`debug tacacs accounting`
	
	Example:
	`Router# debug tacacs accounting`
		Displays information about accountable events as they occur.

Step 5	`debug tacacs packets`
	
	Example:
	`Router# debug tacacs packets`
		Displays information about TACACS+ packets.

Configuration Examples for Per VRF for TACACS+ Servers

This section includes the following configuration example:

Configuring Per VRF for TACACS+ Servers: Example

The following output example shows that the group server **tacacs1** is configured for per VRF AAA services:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Additional References

The following sections provide references related to Per VRF for TACACS+ Servers..

Related Documents

Related Topic	Document Title
Configuring TACACS+	*"Configuring TACACS+"* module.
Per VRF AAA	"Per VRF AAA" module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Per VRF for TACACS+ Servers

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1   Feature Information for Per VRF for TACACS+ Servers

Feature Name	Releases	Feature Information
Per VRF for TACACS+ Servers	12.3(7)T 12.2(33)SRA 1 12.2(33)SXI 12.2(33)SXH 4 12.2(54)SG	The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. This feature was introduced in Cisco IOS Release 12.3(7)T. This feature was integrated into Cisco IOS Release 12.2(33)SRA1. This feature was integrated into Cisco IOS Release 12.2(33)SXI. This feature was integrated into Cisco IOS Release 12.2(33)SXH4. The following commands were introduced or modified: **ip tacacs source-interface**, **ip vrf forwarding (server-group)**, **server-private (TACACS+)**.