

Per VRF for TACACS Servers

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.

- Prerequisites for Per VRF for TACACS Servers, on page 1
- Restrictions for Per VRF for TACACS Servers, on page 1
- Information About Per VRF for TACACS Servers, on page 1
- How to Configure Per VRF for TACACS Servers, on page 2
- Configuration Examples for Per VRF for TACACS Servers, on page 5
- Additional References, on page 6
- Feature Information for Per VRF for TACACS Servers, on page 7

Prerequisites for Per VRF for TACACS Servers

- TACACS+ server access is required.
- 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 enabled globally on the router before per VRF for a TACACS+ server is configured.

Information About Per VRF for TACACS Servers

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 XE Release 2.2, this functionality was available only on RADIUS servers.

How to Configure Per VRF for TACACS Servers

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

Procedure

	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:**	Configures a VRF table and enters VRF configuration mode.

	Command or Action	Purpose
	`Router (config)# ip vrf cisco`	
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.
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:**	Configures the VRF reference of a AAA TACACS+ server group.

	Command or Action	Purpose
	`Router (config-sg-tacacs+)# ip vrf forwarding cisco`	
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.

To maintain stable and reliable AAA accounting operations, adhere to the following recommendations:

Avoid combining generic and named TACACS+ server groups. Do not combine the generic TACACS+ group with named TACACS+ server groups within the same AAA accounting configuration. Instead, specify only the named group that includes the configured servers with source-interface bindings. This practice ensures that Cisco IOS XE initiates TACACS+ accounting connections directly to the named group, utilizing the correct source-interface and routing configurations, thereby preventing fallback issues and broken AAA operations.

```
Example:
aaa accounting system default
action-type start-stop
group ISE_SERVERS
```

In this example, the generic TACACS+ group is omitted from the list.

Verify named TACACS+ server group parameters- Ensure that the named TACACS+ server group is configured with all necessary parameters, such as ip vrf forwarding and ip tacacs source-interface. These parameters are critical for guaranteeing proper packet routing and successful communication with the TACACS+ servers.

Caution Enabling debug CLI can cause performance degradation on the router. Use of **debug** commands for large number of sessions is not recommended.

SUMMARY STEPS

1. **enable**
2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

DETAILED STEPS

Procedure

	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

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

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 Per VRF for TACACS+ Servers

Feature Name	Releases	Feature Information
Per VRF for TACACS+ Servers	Cisco IOS XE Release 2.2	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. In Cisco IOS XE Release 2.2, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **ip tacacs source-interface**, **ip vrf forwarding (server-group)**, **server-private (TACACS+)**.