

TACACS+ over IPv6

An IPv6 server can be configured to be used with TACACS+.

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

Information About TACACS+ over IPv6

The Terminal Access Controller Access-Control System (TACACS+) security protocol provides centralized validation of users. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your devices are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are inacl, outacl, prefix, and route.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

TACACS+ Over an IPv6 Transport

An IPv6 server can be configured to use TACACS+. Both IPv6 and IPv4 servers can be configured to use TACACS+ using a name instead of an IPv4 or IPv6 address.

How to Configure TACACS+ over IPv6

Configuring the TACACS+ Server over IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tacacs server** *name*
4. **address ipv6** *ipv6-address*
5. **key** [**0** | **7**] *key-string*
6. **port** [*number*
7. **send-nat-address**
8. **single-connection**
9. **timeout** *seconds*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**tacacs server** *name* **Example:** `Device(config)# tacacs server server1`	Configures the TACACS+ server for IPv6 and enters TACACS+ server configuration mode.
Step 4	**address ipv6** *ipv6-address* **Example:** `Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5`	Configures the IPv6 address of the TACACS+ server.
Step 5	**key** [**0**	**7**] *key-string* **Example:**	Configures the per-server encryption key on the TACACS+ server.

	Command or Action	Purpose
	`Device(config-server-tacacs)# key 0 key1`	
Step 6	**port** [*number* **Example:** `Device(config-server-tacacs)# port 12`	Specifies the TCP port to be used for TACACS+ connections.
Step 7	**send-nat-address** **Example:** `Device(config-server-tacacs)# send-nat-address`	Sends a client's post-NAT address to the TACACS+ server.
Step 8	**single-connection** **Example:** `Device(config-server-tacacs)# single-connection`	Enables all TACACS packets to be sent to the same server using a single TCP connection.
Step 9	**timeout** *seconds* **Example:** `Device(config-server-tacacs)# timeout 10`	Configures the time to wait for a reply from the specified TACACS server.

Specifying the Source Address in TACACS+ Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 tacacs source-interface** *type number*

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.

	Command or Action	Purpose
Step 3	**ipv6 tacacs source-interface** *type number* **Example:** `Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0`	Specifies an interface to use for the source address in TACACS+ packets.

Configuring TACACS+ Server Group Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server tacacs+** *group-name*
4. **server name** *server-name*
5. **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server tacacs+** *group-name* **Example:** `Device(config)# aaa group server tacacs+ group1`	Groups different TACACS+ server hosts into distinct lists and distinct methods.
Step 4	**server name** *server-name* **Example:** `Device(config-sg-tacacs+)# server name server1`	Specifies an IPv6 TACACS+ server.
Step 5	**server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]	Configures the IPv6 address of the private TACACS+ server for the group server.

	Command or Action	Purpose
	Example: `Device(config-sg-tacacs+)# server-private 2001:DB8:3333:4::5 port 19 key key1`	

Configuration Examples for TACACS+ over IPv6

Example: Configuring TACACS+ Server over IPv6

```
Device# show tacacs

           Tacacs+ Server:          server1
           Server Address:          FE80::200:F8FF:FE21:67CF
             Socket opens:          0
            Socket closes:          0
            Socket aborts:          0
            Socket errors:          0
         Socket Timeouts:           0
  Failed Connect Attempts:          0
       Total Packets Sent:          0
       Total Packets Recv:          0
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

Related Documents

Related Topic	Document Title
Configuring PPP interfaces	PPP Configuration in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T.
Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices	*Cisco IOS Dial Technologies Command Reference*
Lists of IOS Security Commands	*Cisco IOS Security Command Reference*
Configuring PPP authentication using AAA	Configuring PPP Authentication Using AAA in the Configuring Authentication module in the *Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T.
Configuring RADIUS Authentication	Configuring RADIUS module in the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported 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
RFC 1661	*Point-to-Point Protocol (PPP)*
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*
RFC 2759	*Microsoft PPP CHAP Extensions, Version 2*

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/techsupport

Feature Information for TACACS+ 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 TACACS+ over IPv6

Feature Name	Releases	Feature Information
TACACS+ over IPv6	Cisco IOS XE Release 3.2S	TACACS+ over IPv6 is supported. The following commands were introduced or modified: **aaa group server tacacs+**, **address ipv6 (TACACS+)**, **ipv6 tacacs source-interface**, **key (TACACS+)**, **port (TACACS+)**, **send-nat-address**, **server name (IPv6 TACACS+)**, **server-private (TACACS+)**, **single-connection**, **tacacs server**, **timeout (TACACS+)**.