Contents

1 Configuring TACACS

1.1 Introduction

1.1.1 Overview

Terminal Access Controller Access Control System (TACACS) is a distributed authentication, authorization and accounting (AAA) protocol based on the client/server architecture. TACACS+ has enhanced functions on the basis of the TACACS protocol, to provide the authentication, authorization and accounting services for users. This following describes TACACS+.

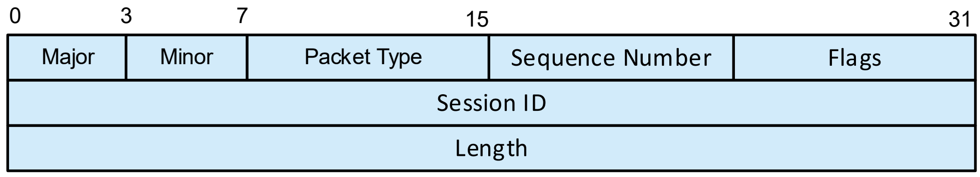
Both TACACS+ and Remote Authentication Dial-In User Service (RADIUS) are capable of providing AAA security services. Compared with RADIUS, TACACS+ has the following advantages:

- It is implemented based on the Transmission Control Protocol (TCP) and provides more reliable network transmission.
- TACACS+ encrypts both packet bodies and passwords to boost security.
- Authentication is separated from authorization. The authentication server and authorization server can be deployed separately in remote deployment.
- TACACS+ supports authorization and accounting on configuration commands.

1.1.2 Principles

1. TACACS+ Packet

Figure 1-1 TACACS+ Packet Structure



Fields contained in the TACACS+ packet structure shown in Figure 1-1 are described in Table 1-1.

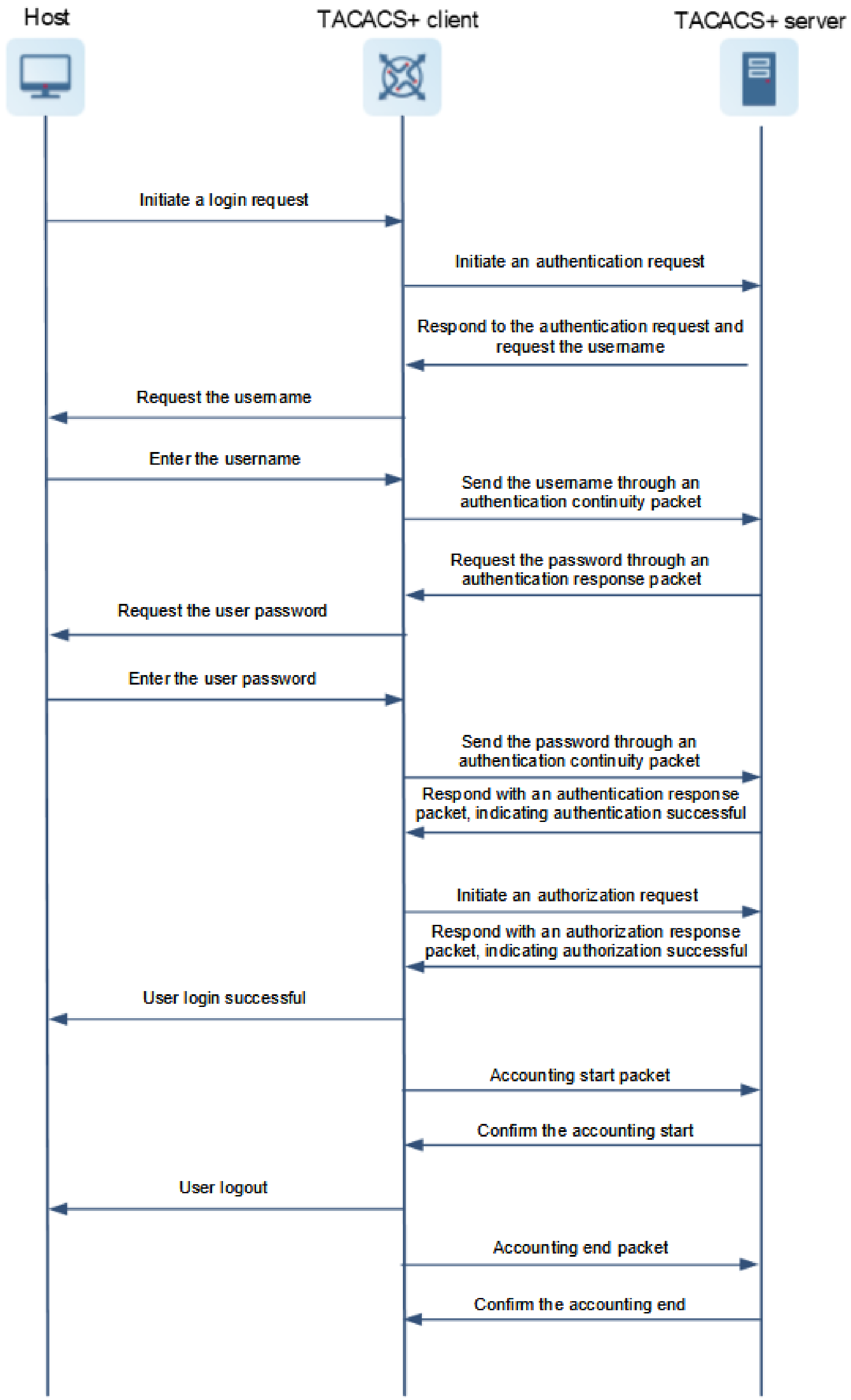
Table 1-1 Description of Fields Contained in a TACACS+ Packet

Field	Length	Description
Major Version	4 bits	Major TACACS+ version
Minor Version	4 bits	Minor TACACS+ version
Packet Type	1 byte	Packet type. The options are as follows: **0x01**: Indicates an authentication packet. **0x02**: Indicates an authorization packet.

Field	Length	Description
		0x03: Indicates an accounting packet.
Sequence Number	1 byte	Sequence number of a data packet in the current session (The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of each subsequent data packet increases by one. The client sends data packets only with an odd sequence number and TACACS+ Daemon sends data packets only with an even sequence number.)
Flags	1 byte	Whether the data packet is encrypted
Session ID	4 bytes	TACACS+ session ID
Length	4 bytes	Body length of a TACACS+ data packet (excluding the header)

2. Packet Exchange Process

Figure 1-1 TACACS+ Packet Exchange Flowchart


Host
TACACS+ client
TACACS+ server
Initiate a login request
Initiate an authentication request
Respond to the authentication request and request the usemame
Request the usemame
Enter the username
Send the usemame through an authentication continuity packet
Request the password through an authentication response packet
Request the user password
Enter the user password
Send the password through an authentication continuity packet
Respond with an authentication response packet, indicating authentication successful
Initiate an authorization request
Respond with an authorization response packet, indicating authorization successful
User login successful
Accounting start packet
Confirm the accounting start
User logout
Accounting end packet
Confirm the accounting end

As shown in Figure 1-1, the TACACS+ protocol basically involves the authentication, authorization, and accounting processes. The network access server (NAS) requests security services from the TACACS+ server as a TACACS+ client.

(1) Authentication process

a A user initiates a login request to the NAS.

b After receiving the user request, the NAS sends an authentication start packet to the TACACS+ server to initiate an authentication request.

c The TACACS+ server responds to the authentication request and asks the NAS to provide the username.

d The NAS asks the user terminal to provide the username.

e The user enters the username and sends it to the NAS.

f The NAS sends the username to the TACACS+ server through an authentication continuity packet.

g After receiving the username, the TACACS+ server continues to ask the NAS for the user password.

h The NAS requests the user terminal to provide the password.

i The user enters the password and sends it to the NAS.

j The NAS sends the password to the TACACS+ server through an authentication continuity packet.

k After receiving the password, the TACACS+ server verifies the password and then returns an authentication success message to the NAS.

(2) Authorization process

a The NAS initiates an authorization request to the TACACS+ server.

b The TACACS+ server responds to the authorization request by returning an authorization success message to the NAS.

c After receiving the authorization success message, the NAS allows the user to log in to the NAS and perform operations within the authorized scope.

(3) Accounting process

a The NAS sends an accounting start request to the TACACS+ server.

b After receiving the accounting start request, the TACACS+ server starts accounting and returns an accounting request acceptance message to the NAS.

c If the user logs out, the NAS sends an accounting end request to the TACACS+ server after receiving a user logout message.

d After receiving the accounting end request, the TACACS+ stops accounting and returns an accounting end message.

1.1.3 Protocols and Standards

- RFC 1492: Terminal Access Controller Access Control System

1.2 Configuration Task Summary

TACACS+ configuration includes the following tasks:

- Configuring TACACS+ Basic Features
- (Optional) Configuring TACACS+ Reachability Detection
- (Optional) Configuring a TACACS+ Server Group

1.3 Configuring TACACS+ Basic Features

1.3.1 Overview

This section describes how to configure parameters for the communication between the device and a TACACS+ server to ensure normal communication between them. After the parameters are configured, the device can correctly send AAA authentication, authorization, and accounting requests to the TACACS+ server and give responses.

1.3.2 Restrictions and Guidelines

Configuring TACACS+ basic features only ensures proper communication between the device and a TACACS+ server. To provide AAA security services for users, you still need to reference the TACACS+ server in an AAA method list.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA.

aaa new-model

(4) Configure a TACACS+ server.

tacacs-server host [**oob** [**via Mgmt** *Mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**port** *port-number*] [**test username** *username*] [**idle-time** *idle-time*] [**timeout** *timeout*] [**key** [**0** | **7**] *key*]

No TACACS+ server is configured by default.

You can specify a shared key for a TACACS+ server when configuring the server. If it is not specified, the global shared key will be used.

(5) (Optional) Configure the global shared key for the communication between the device and TACACS+ server.

tacacs-server key [**0** | **7**] *key*

No global shared key is configured for the device and TACACS+ server by default.

(6) (Optional) Configure the source address for TACACS+ packets.

ip tacacs source-interface *interface-type interface-number*

No source address is configured for TACACS+ packets and the address is set by the network layer by default.

You can run this command to specify an outbound interface for packets. After this command is configured, the first IP address of the interface is used as the source address of TACACS+ packets.

(7) (Optional) Configure the timeout duration for the TACACS+ server.

tacacs-server timeout *timeout*

The default timeout duration of a TACACS+ server is **5** seconds in the communication between the device and the TACACS+ server.

1.4 Configuring TACACS+ Reachability Detection

1.4.1 Overview

A TACACS+ server can be only in the reachable or unreachable state. The device will not send authentication, authorization, or accounting requests of access users to an unreachable TACACS+ server unless all servers in the TACACS+ server group are unreachable.

The device maintains the reachability status of each TACACS+ server. The device selects a reachable TACACS+ server preferentially to improve the handling performance of TACACS+ services.

The device actively detects whether a specified TACACS+ server is reachable. After the active detection function is configured for a TACACS+ server, the device periodically sends detection requests (authentication requests or accounting requests) to the TACACS+ server. The active detection interval is **60** minutes when the TACACS+ server is reachable and **1** minute when the TACACS+ server is unreachable.

1.4.2 Restrictions and Guidelines

- To enable active detection for a specified TACACS+ server, perform the following configuration when configuring the TACACS+ server:
  - Configure a test username for the TACACS+ server.
  - Configure at least one tested port (authentication port or accounting port) for the TACACS+ server.
- It is judged that a TACACS+ server is unreachable only when both conditions below are met:
  - The device fails to receive a correct response packet from the TACACS+ server within the specified timeout period.
  - The consecutive transmission count of a request packet sent by the device to the same TACACS+ server reaches the specified timeout count.
- If any of the following conditions is met for an unreachable TACACS+ server, the TACACS+ server is considered reachable:
  - The device receives a correct response from the TACACS+ server.
  - The duration in which the TACACS+ server is unreachable exceeds the time configured using the **tacacs-server deadtime** command and active detection is disabled for the TACACS+ server.
  - The authentication port or accounting port of the TACACS+ server is updated on the device.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the criteria for the device to judge that a TACACS+ server is unreachable.

tacacs-server dead-criteria { **time** *timeout* **tries** *tries-number* | **time** *timeout* | **tries** *tries-number* }

The criteria for the device to judge that a TACACS+ server is unreachable are that the server timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

(4) (Optional) Configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

tacacs-server deadtime *deadtime*

Even if a TACACS+ server is unreachable, the device still sends requests to the TACACS+ server by default.

If active detection is enabled for a TACACS+ server, the time parameter configured by the **tacacs-server deadtime** command does not take effect on the TACACS+ server.

1.5 Configuring a TACACS+ Server Group

1.5.1 Overview

One or more TACACS+ servers can be added to each TACACS+ server group, which provides AAA services for users as a whole.

1.5.2 Restrictions and Guidelines

- TACACS+ security services are a type of AAA services and need to be used in combination with the AAA features. TACACS+ provides security services for users as one method in an AAA method list.
- When configuring the authentication, authorization, and accounting method lists, you can specify server groups separately for them.
- In a user-defined server group, you can only specify and apply servers in the default server group.
- TACACS+ server groups support virtual routing and forwarding (VRF) instances. When a server group in a specified VRF instance is used, the source address used by the device to communicate with a remote server must be obtained from the VRF instance. If you run the **ip tacacs+ source-interface** command to specify the source interface for request packets, the IP address obtained from this source interface takes priority over that found in the VRF instance.
- The name of a server group cannot be set to the predefined keyword **tacacs+**.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a TACACS+ server group.

aaa group server tacacs+ *group-name*

No TACACS+ server group is configured by default.

You can group TACACS+ servers so that authentication, authorization, and accounting can be completed by different server groups.

(4) Add a server to the TACACS+ server group.

server { *ipv4-address* | *ipv6-address* }

No server is added to a TACACS+ server group by default.

(5) (Optional) Specify a VRF instance for the TACACS+ server group.

ip vrf forwarding *vrf-name*

No VRF instance is specified for a TACACS+ server group by default.

The VRF instance configured for a TACACS+ server group must use a valid name configured using the **vrf definition** command in global configuration mode.

(6) Configure an MGMT port to be used by the TACACS+ server group.

ip oob [**via Mgmt** *mgmt-number*]

No MGMT port to be used by a TACACS+ server group is configured by default.

(7) (Optional) Configure the function of carrying the **nas-ip** attribute in packets.

nas-ip { *ipv4-address* | *ipv6-address* }

Packets do not carry the **nas-ip** attribute by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

⚠ **Notice**

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 TACACS+ Monitoring

Command	Purpose
show tacacs	Displays the interaction between the device and each TACACS+ server.
debug tacacs+	Debugs TACACS+.

1.7 Configuration Examples

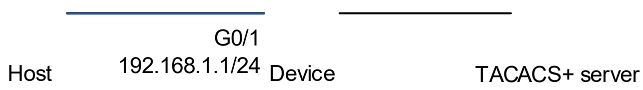
1.7.1 Configuring TACACS+ for Login Authentication

1. Requirements

A TACACS+ server needs to be used for authentication of login users.

2. Topology

Figure 1-1 Topology of Login Authentication Using TACACS+



3. Notes

- Configure device information and add login users on the TACACS+ server.
- Enable AAA security services on the device.
- Configure TACACS+ server information on the device.
- Configure a TACACS+ authentication method list.
- Apply the TACACS+ authentication methods to a specific line.

4. Procedure

(1) Configure device information and add login users on the TACACS+ server. The configuration is omitted here. For details, see the TACACS+ server configuration manual.

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure a TACACS+ server (the IP address of the TACACS+ server is set to 192.168.1.3 and the shared key is set to **sharekey** here).

```
Device(config)# tacacs-server host 192.168.1.3 key sharekey
```

(4) Configures an authentication method list.

```
Device(config)# aaa authentication login tacacs-method group tacacs+
```

(5) Apply the authentication methods to a line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication tacacs-method
```

5. Verification

After entering the correct username and password, a user can log in to the device successfully.

```
User Access Verification

Username:hostname1
Password:password1



Device#
```

6. Configuration Files

```
!
```

```
aaa new-model
!
aaa authentication login tacacs-method group tacacs+
!
tacacs-server host 192.168.1.3 key 7 $10$275$g8oXDDIPVeA=$
!
line console 0
line vty 0 4
 login authentication tacacs-method
!
```

7. Common Errors

The shared key configured on the device is inconsistent with that used by the TACACS+ server.

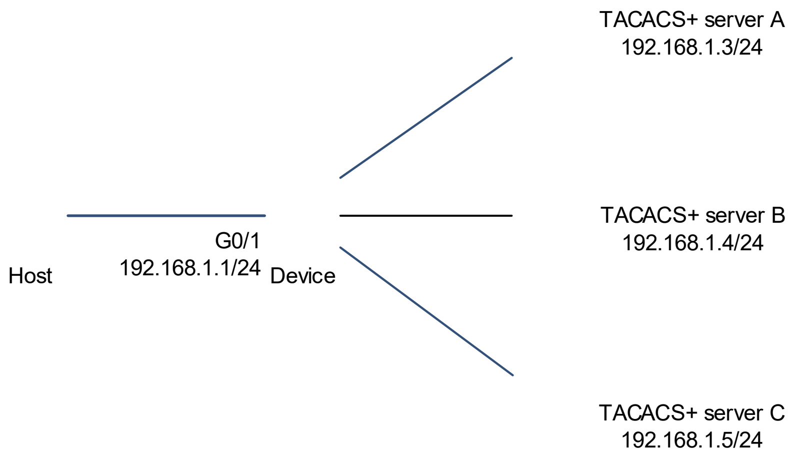
1.7.2 Configuring Separated Authentication, Authorization and Accounting by Using TACACS+

1. Requirements

The user authentication, authorization, and accounting services need to be separately completed by different TACACS+ server groups.

2. Topology

Figure 1-1 Topology of Separated Authentication, Authorization, and Accounting of TACACS+



3. Notes

- Configure device information and add login users on the TACACS+ server.
- Enable AAA security services on the device.
- Configure TACACS+ servers on the device and add them to different TACACS+ server groups.
- Configure TACACS+ authentication, authorization, and accounting method lists.
- Apply the TACACS+ authentication, authorization, and accounting methods to a specific line.

4. Procedure

(1) Configure device information and add login users on the TACACS+ server. The configuration is omitted here. For details, see the TACACS+ server configuration manual.

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure TACACS+ server A and add it to TACACS+ server group **tacacs1**. (The IP address of TACACS+ server A is set to 192.168.1.3 and the shared key is set to **sharekey** here.)

```
Device(config)# tacacs-server host 192.168.1.3 key sharekey
Device(config)# aaa group server tacacs+ tacacs1
Device(config-gs-tacacs+)# server 192.168.1.3
Device(config-gs-tacacs+)# exit
```

(4) Configure server groups **tacacs2** and **tacacs3** by referring to the steps of configuring server group **tacacs1**.

```
Device(config)# tacacs-server host 192.168.1.4 key sharekey
Device(config)# aaa group server tacacs+ tacacs2
Device(config-gs-tacacs+)# server 192.168.1.4
Device(config-gs-tacacs+)# exit
Device(config)# tacacs-server host 192.168.1.5 key sharekey
Device(config)# aaa group server tacacs+ tacacs3
Device(config-gs-tacacs+)# server 192.168.1.5
Device(config-gs-tacacs+)# exit
```

(5) Configure an authentication method list to use server group **tacacs1**, an authorization method list to use server group **tacacs2**, and an accounting method list to use server group **tacacs3**.

```
Device(config)# aaa authentication login tacacs-method group tacacs1
Device(config)# aaa authorization exec radius-method group tacacs2
Device(config)# aaa accounting exec radius-method start-stop group tacacs3
```

(6) Apply the authentication methods, authorization methods, and accounting methods to a line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication tacacs1
Device(config-line)# authorization exec tacacs2
Device(config-line)# accounting exec tacacs3
```

5. Verification

After entering the correct username and password configured on TACACS+ server A, a user can log in to the device successfully.

```
User Access Verification

Username:hostname1
Password:password1



Device#
```

After login, the user has only the privilege level granted by TACACS+ server B and can only run commands under this privilege level.

After the user logs out, accounting information of the user can be queried on TACACS+ server C. For details about how to query accounting information, see the TACACS+ server configuration manual.

6. Configuration Files

```
!
aaa new-model
!
aaa accounting exec radius-method start-stop group tacacs3
aaa authorization exec radius-method group tacacs2
aaa authentication login radius-method group tacacs1
!
tacacs-server host 192.168.1.3 key 7 $10$275$g8oXDDIPVeA=$
tacacs-server host 192.168.1.4 key 7 $10$275$g8oXDDIPVeA=$
tacacs-server host 192.168.1.5 key 7 $10$275$g8oXDDIPVeA=$
!
!
aaa group server tacacs+ tacacs1
 server 192.168.1.3
!
aaa group server tacacs+ tacacs2
 server 192.168.1.4
!
aaa group server tacacs+ tacacs3
 server 192.168.1.5
!
line console 0
line vty 0 4
 accounting exec tacacs3
 authorization exec tacacs2
 login authentication tacacs1
!
```

7. Common Errors

- The shared key configured on the device is inconsistent with that used by the TACACS+ server.
- Undefined servers are added to a server group.

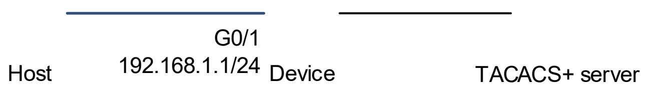
1.7.3 Configuring Reachability Detection

1. Requirements

TACACS+ reachability detection needs to be configured to identify unreachable TACACS+ servers.

1. Topology

Figure 1-1 Topology of TACACS+ Reachability Detection



2. Notes

- Configure the global criteria for judging that a TACACS+ server is unreachable.
- Configure an IP address for the TACACS+ server and configure active detection parameters.

3. Procedure

Configure the global criteria for judging that a TACACS+ server is unreachable as follows: The consecutive timeout count is **5** and the timeout duration is **120** seconds.

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 120 tries 5
```

Set the IP address of the TACACS+ server to 192.168.1.3, detection username to **test**, detection interval to **90** minutes.

```
Device(config)# tacacs-server host 192.168.1.3 test username test idle-time 90
```

4. Verification

Disconnect the network communication between the device and the server with the IP address 192.168.1.3. Initiate TACACS+ authentication through the device. After 120 seconds, run the **show tacacs** command to check that the server status is "Dead".

```
Hostname# enable
Hostname# show tacacs server
Tacacs+ Server : 192.168.1.3/49
state: Dead
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 1

Tacacs capability:
    mgmt enable: true
    vrf enable: true
```

5. Configuration Files

```
!
tacacs-server host 192.168.1.3 test username test idle-time 90
tacacs-server dead-criteria time 120 tries 5
!
```