Configuring Remote Authentication

Overview of Remote Authentication

The User Management feature manages all the tasks related to user authentication and authorization. The types of authentication and authorization are dependent on the device they are performed. If authentication and authorization are performed by the device itself, it is called local authentication. If authentication and authorization are performed on an authentication server such as a RADIUS server, it is called remote authentication.

Remote authentications work only if the user login credentials are stored on the authentication server and a connection exists between the device and the authentication server.

Local authentication is used by default.

Remote authentication supports RADIUS authentication and TACACS+ authentication. You can configure both remote authentication and local authentication for a device. However, the remote authentication takes precedence. Moreover, local authentication is attempted only when remote authentication fails.

Configure Remote Authentication

The following sections provide remote authentication configuration information.

Configure Local Authentication

To configure local authentication, perform this procedure.

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**muser local** **Example:** `Device(config)# muser local`	Enables local authentication mode.

Configuring RADIUS Remote Authentication

Configuring RADIUS remote authentication involves the following tasks:

1. Configure the RADIUS remote authentication mode.
2. Configure the RADIUS authentication server.
3. Configure the RADIUS domain configurations.

Configure the RADIUS Remote Authentication Mode

To configure the RADIUS remote authentication mode, perform this procedure.

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	**muser radius** *radius-name* {**pap** | **chap**} [**account** |**local**] **Example:** `Device(config)# muser radius r1 pap`	Enables RADIUS remote authentication.

Configure the RADIUS Authentication Server

To configure the RADIUS authentication server, perform this procedure.

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** **Example:** `Device(config)# aaa`	Enters AAA configuration mode.
Step 4	**radius host** *radius-name* **Example:** `Device(config-aaa)# radius host r1`	Configures the RADIUS server name.
Step 5	{**primary-auth-ip** | **second-auth-ip**} *ip-address auth-port* **Example:** `Device(config-aaa-radius-r1)# primary-auth-ip 192.0.2.1 20`	Configures the RADIUS authentication server address and port details.
Step 6	**auth-secret-key** *key-value* **Example:** `Device(config-aaa-radius-r1)# auth-secret-key 10`	Configures the RADIUS authentication key.
Step 7	**preemption-time** *value* **Example:** `Device(config-aaa-radius-r1)# preemption-time 2`	(Optional) Configures the recovery time to change to the primary server. **Note** The default value is 0. Configuring the default value indicates no changeover.

Configure the RADIUS Domain Configurations

To configure the RADIUS domain configurations, perform this procedure.

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**aaa** **Example:** `Device(config)# aaa`	Enters AAA configuration mode.
Step 4	**domain** *domain-name* **Example:** `Device(config-aaa)# domain r1`	Configures the RADIUS domain name.
Step 5	**radius host binding** *radius-name* **Example:** `Device(config-aaa-domain-r1)# radius host binding r1`	Binds the domain to the RADIUS server.
Step 6	**state active** **Example:** `Device(config-aaa-domain-r1)# state active`	Activates the domain.
Step 7	**state block** **Example:** `Device(config-aaa-domain-r1)# state block`	(Optional) Deactivates the domain.
Step 8	**exit** **Example:** `Device(config-aaa-domain-r1)# exit`	(Optional) Returns to AAA configuration mode.
Step 9	**default domain-name** {**enable** *domain-name* | **disable**} **Example:** `Device(config-aaa)# default domain-name enable domain1`	(Optional) Enables or deletes the default domain. Use the **default domain-name enable** *domain-name* command to enable the default domain. Use the **default domain-name disable** command to delete the default domain.

Configure TACACS+ Remote Authentication

To configure TACACS+ remote authentication, perform this procedure.

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**muser tacacs+** [**author** |**account** |**command-account** |**local**] **Example:** `Device(config)# muser tacacs+`	Enables TACACS+ remote authentication mode. • **author**: Allows login authorization through the TACACS+ server • **account**: Manages login accounting through the TACACS+ server. • **command-account**: Forwards all the command lines to the TACACS+ server through the TACACS+ account packet. • **local**: Allows local authentication when remote authentication fails.
Step 4	[**no**] **tacacs+ encrypt-key** **Example:** `Device(config)# tacacs+ encrypt-key`	(Optional) Enables password encryption. The default password encryption is clear text. Use the **no tacacs+ encrypt-key** command to disable password encryption.
Step 5	**tacacs+ authentication-type** {**ascii** | **chap** | **pap**} **Example:** `Device(config)# tacacs+ authentication-type ascii`	(Optional) Configures an authentication type. The authentication types available are: • ASCII • Password Authentication Protocol (PAP) • Challenge Handshake Authentication Protocol (CHAP) The default is ASCII.
Step 6	**tacacs+** {**primary** | **secondary**} {**server** *ip-address*} [**encrypt-key** *value* | **key** *value* | **port** *port-num* | **timeout** *value*] **Example:** `Device(config)# tacacs+ primary server 192.168.1.10 key 123456`	Configures the TACACS + server.
Step 7	**tacacs+ preemption-time** *value* **Example:** `Device(config)# tacacs+ preemption-time 20`	(Optional) Configures the recovery time to change to the primary server. **Note** The default value is 0. Configuring the default value indicates no changeover.

Monitor Remote Authentication

Use the following commands to monitor remote authentication.

Table 1: Commands to Monitor Remote Authentication

Command	Purpose
show muser	Displays the authentication configuration.
show radius host [**radius-name**]	Displays the RADIUS host configuration.
show domain [*domain-name*]	Displays the domain configuration.
show tacacs+	Displays the TACACS+ configuration.

Configuration Example: Configuring Remote Authentication

The following example shows how to configure the authentication type:

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ authentication-type ascii
Device(config)# end
```

The following example shows how to configure the address and key of the primary authentication server:

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ primary server 192.168.1.10 key 123456
Device(config)# end
```

The following example shows how to configure the address and key of the secondary authentication server (No configuration is required when there is no secondary server.)

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ secondary server 192.168.1.11 key 123456
Device(config)# end
```

The following example shows how to display the TACACS+ configurations:

```
Device> enable
Device# configure terminal
Device(config)# show tacacs+
Primary Server Configurations:
IP address:         : 192.168.1.10
Connection port:    : 49
Connection timeout: : 5
Key:                : 123456
```

```
Secondary Server Configurations:
IP address:         : 192.168.1.11
Connection port:    : 49
Connection timeout: : 5
Key:                : 123456
Device(config)# end
```

The following example shows how to configure TACACS+ to perform remote authentication:

```
Device> enable
Device# configure terminal
Device(config)# muser tacacs+
Device(config)# end
```