Configuring Second-Tier Authentication

Overview of Second-Tier Password Authentication

A normal user has permission only to enter execution mode to view configuration information. A normal user cannot enter configuration mode to modify the configuration.

A second-tier password allows a normal user to pass second-tier authentication and perform all administrator tasks. The Second-Tier Password Authentication feature is disabled by default.

A second-tier password can be used for both local and remote authentication. If user management is configured with local authentication, the second-tier password is also authenticated with local authentication. If user management is configured with remote authentication, the second-tier password is also authenticated with remote authentication.

With local authentication configured, if a normal user logs in to the privileged mode, the device prompts the user for the password. A normal user needs to enter a second-tier password for successful authentication. With remote authentication configured, if a normal user logs in to the privileged mode, the device automatically uses the configured username and second-tier password for successful authentication.

Configure Second-Tier Password Authentication

To configure second-tier password 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	[**no**] **username privilege-auth** **Example:** `Device(config)# username privilege-auth`	Enables authentication. Use the **no username privilege-auth** to disable authentication.
Step 4	**username change-privilege-pwd** {**0** | **7**} *password* **Example:** `Device(config)# username change-privilege-pwd 4 123`	Configures the password for second-tier password authentication. If the password is selected as 0, it indicates that the password is in plain text. If you select 7, the password is in cipher text. You must use the corresponding plain text for authentication.
Step 5	[**no**] **username privilege-auth-remote-user** *username* **Example:** `Device(config)# username privilege-auth-remote-user test`	Configures the username for second-tier password authentication. Use the **no username privilege-auth-remote-user** *username* to remove the username.

Monitor Second-Tier Authentication

Use the following command to monitor second-tier authentication.

Table 1: Command to Monitor Second-Tier Authentication

Command	Purpose
show username privilege-auth	Displays the second-tier password authentication configuration.

Configuration Example: Configuring Second-Tier Authentication

The following example shows how to create a normal user with username and password as **test/test**:

```
Device> enable
Device# configure terminal
Device(config)# username test privilege 0 password 0 test
```

The following example shows how to log in as a normal user if second-tier password authentication is not configured:

```
Device> enable
Device# configure terminal
```

```
Device(config)# quit
Username:test
Password:****
```

The following example shows how to configure a username for second-tier password authentication (it defaults to local authentication, and the authentication is optional):

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth-remote-user test
```

The following example shows how to configure a password for second-tier password authentication. (When a user enters privileged mode, the password is required.)

```
Device> enable
Device# configure terminal
Device(config)# username change-privilege-pwd 0 123456
Please input your login password : ****
Change password successfully.
```

The following example shows the error message when the wrong password is entered:

```
Device> enable
Please input password : ****
Password is error.
Device>
```