2.2 Lab 2: Local AAA Configuration

2.2.1 Introduction

2.2.1.1 About This Lab

Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.

AAA provides the following functions:

- Authentication: verifies whether users are permitted to access the network.
- Authorization: authorizes users to use particular services.
- Accounting: records the network resources used by users.

Users can use one or more security services provided by AAA. For example, if a company wants to authenticate employees that access certain network resources, the network administrator only needs to configure an authentication server. If the company also wants to record operations performed by employees on the network, an accounting server is needed.

In summary, AAA authorizes users to access specific resources and records user operations. AAA is widely used because it features good scalability and facilitates centralized user information management. AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.

In this lab activity, you will configure local AAA to manage and control resources for remote Telnet users.

2.2.1.2 Objectives

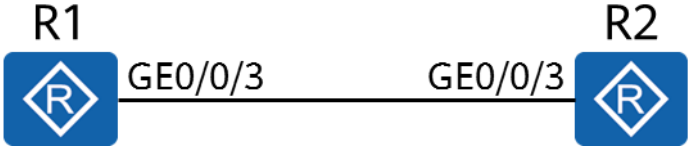
Upon completion of this task, you will be able to:

- Learn how to configure local AAA
- Learn how to create a domain
- Learn how to create a local user
- Understand domain-based user management

2.2.1.3 Networking Topology

R1 functions as a client, and R2 functions as a network device. Access to the resources on R2 needs to be controlled. Therefore, you need to configure local AAA authentication on R1 and R2 and manage users based on domains, and configure the privilege level for authenticated users.

Figure 2-1 Lab topology for local AAA configuration



2.2.2 Lab Configuration

2.2.2.1 Configuration Roadmap

1. Configure an AAA scheme.
2. Create a domain and apply the AAA scheme to the domain.
3. Configure local users.

2.2.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name R1 and R2.

The details are not provided here.

Configure IP addresses for R1 and R2.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
```

Step 2 Configure an AAA scheme.

Configure authentication and authorization schemes.

```
[R2-aaa]aaa
Enter the AAA view.
[R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
Create an authentication scheme named datacom.
[R2-aaa-authen-datacom]authentication-mode local
Set the authentication mode to local authentication.
[R2-aaa-authen-datacom]quit
[R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
Create an authorization scheme named datacom.
[R2-aaa-author-datacom]authorization-mode local
Set the authorization mode to local authorization.
[R2-aaa-author-datacom]quit
```

A device functioning as an AAA server is called a local AAA server, which can perform authentication and authorization, but not accounting.

The local AAA server requires a local user database, containing the user name, password, and authorization information of local users. A local AAA server is faster and cheaper than a remote AAA server, but has a smaller storage capacity.

Step 3 Create a domain and apply the AAA scheme to the domain.

```
[R2]aaa
[R2-aaa]domain datacom
```

The devices manage users based on domains. A domain is a group of users and each user belongs to a domain. The AAA configuration for a domain applies to the users in the domain. Create a domain named datacom.

```
[R2-aaa-domain-datacom]authentication-scheme datacom
The authentication scheme named datacom is used for users in the domain.
[R2-aaa-domain-datacom]authorization-scheme datacom
The authorization scheme named datacom is used for users in the domain.
```

Step 4 Configure local users.

Create a local user and password.

```
[R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.
```

If the user name contains a delimiter of at sign (@), the character string before the at sign is the user name and the character string following the at sign is the domain name. If the value does not contain the at sign, the entire character string represents the user name and the domain name is the default one.

Configure the parameters for the local user, such as access type and privilege level.

```
[R2-aaa]local-user hcia@datacom service-type telnet
```

The **local-user service-type** command configures the access type for a local user. After you specify the access type of a user, the user can successfully log in only when the configured access type is used. If the access type is set to telnet, the user cannot access the device through a web page. Multiple access types can be configured for a user.

```
[R2-aaa]local-user hcia@datacom privilege level 3
```

The privilege level of the local user is specified. Only commands within the specified privilege level or a lower level are available for a user.

Step 5 Enable the telnet function on R2.

```
[R2]telnet server enable
The Telnet server function is enabled on the device. This function is enabled by default on some devices.
[R2]user-interface vty 0 4
[R2-ui-vty0-4]authentication-mode aaa
```

The **authentication-mode** command configures an authentication mode for accessing the user interface. By default, the user authentication mode of the VTY user interface is not configured. An authentication mode must be configured for the login interface. Otherwise, users will not be able to log in to the device.

Step 6 Verify the configuration.

Telnet R2 from R1.

```
<R1>telnet 10.0.12.2
  Press CTRL_] to quit telnet mode
  Trying 10.0.12.2 ...
  Connected to 10.0.12.2 ...

Login authentication


Username:hcia@datacom
Password:
<R2>
```

R1 has logged in to R2.

Display the online users on R2.

```
[R2]display users
  User-Intf    Delay    Type  Network Address    AuthenStatus    AuthorcmdFlag
  129 VTY 0    00:02:43 TEL   10.0.12.1              pass
  Username : hcia@datacom
```

----End

2.2.3 Verification

The details are not provided here.