Security Configuration

Model: S5900-24S4T2Q

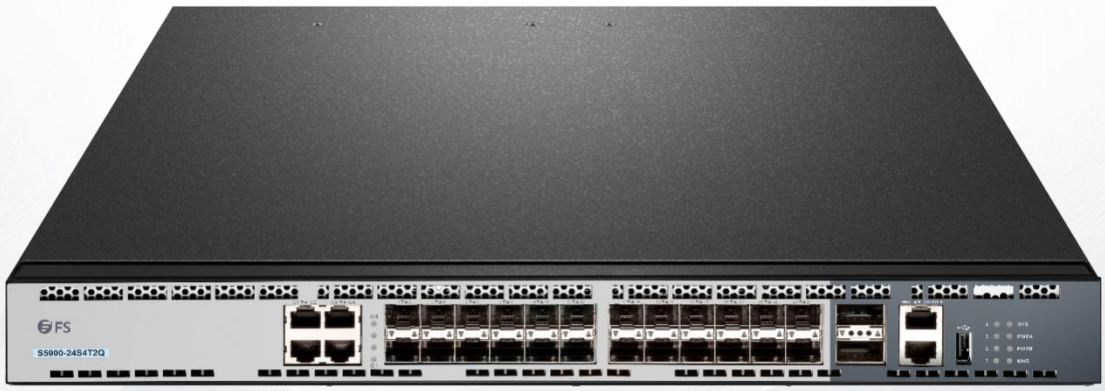

Table of Contents

1. AAA Configuration

1.1 AAA Overview

Access control is the way to control access to the network and services. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

1.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the chapter "Configuring Authentication."

- Authorization—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.
As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, refer to the chapter "Configuring Authorization."

- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting fg interfaces. For information about configuring accounting using AAA, refer to the chapter "Configuring Accounting."

1.1.2 Benefits of Using AAA

AAA provides the following benefits:
- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- Multiple backup systems

1.1.3 AAA Principles

- AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

1.1.4 Method Lists

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, Cisco IOS software selects the next authentication method in the method list. This process continues until there is successful

communication with a listed authentication method or the other software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authenticate u failsatany point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted. The following figures shows a typical AAA network configuration that includes four security servers: R1 and R2 ure RADIUS servers, and T1 and T2 are TACACS+ servers.

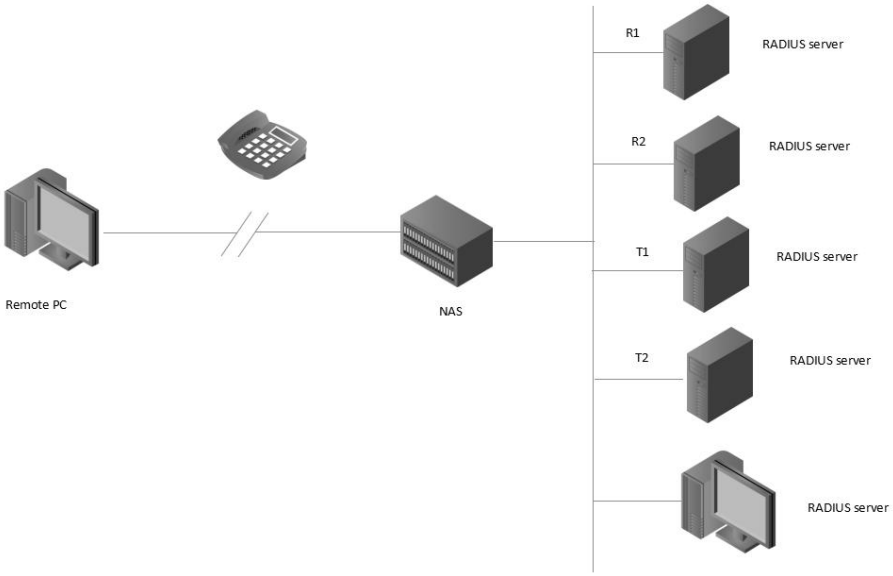

Figure 1-1 Typical AAA Network Configuration

Suppose the system administrator has defined a method list where R1 will be contacted first for authentication information, then R2, T1, T2, and finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session will be terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

1.2 AAA Configuration Process

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack.

1.2.1 Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

- If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.
- (Optional) Configure authorization using the aaa authorization command.
- (Optional) Configure accounting using the aaa accounting command.

1.3 AAA Configuration Process List

- Configuring Login Authentication Using AAA
- Configuring PPP Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- AAA authentication username-prompt

- AAA authentication password-prompt
- Establishing Username Authentication
- Enabling Password

1.4 AAA Authentication Configuration Task

To configure AAA authentication, perform the following configuration processes:
(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
(2) Define the method lists for authentication by using an AAA authentication command.
(3) Apply the method lists to a particular interface or line, if required.

To configure AAA authentication, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
(2) Define the method lists for authentication by using an AAA authentication command.
(3) Apply the method lists to a particular interface or line, if required.

1.4.1 Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

Command	Purpose
format	Ethernet
line [console | vty] Une.umber [ending-line-number\	Enters line configuration mode for the lines to which you want to apply the authentication list.
login authentication (default | list-name\	Applies the authentication list to a line or set of lines.

The list-name is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the 7ACACS+ server returns an error, enter the following command:
aaa authentication login default group radius

Note:
Because the none keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

The following table lists the supported login authentication methods.:

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses named server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
line	Uses the line password for authentication.

local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

(1) Login Authentication Using Enable Password

Use the aaa authentication login command with the enable method keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:
aaa authentication login default enable

(2) Login Authentication Using Line Password

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:
aaa authentication login default line

Before you can use a line password as the login authentication method, you need to define a line password.

(3) Login Authentication Using Local Password

Use the aaa authentication login command with the local method keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:
aaa authentication login default local

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

(4) Login Authentication Using Group RADIUS

Use the aaa authentication login command with the group radius method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:
aaa authentication login default group radius

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

1.4.2 Enabling Password Protection at the Privileged Level

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

Use the following command in global configuration mode:

Command	Purpose
aaa authentication enable default method i [method2...]	Enables user ID and password checking for users requesting privileged EXEC level

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

The following table lists the supported enable authentication methods.

Keyword	Description
enable	Uses the enable password for authentication.

group name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.
group radius	Uses the list of all RADIUS hosts for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

1.4.3 Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

Configuring a Login Banner

To configure a banner that will be displayed whenever a user logs in (replacing the default message for login), use the following commands in global configuration mode:

Command	Purpose
aaa authentication banner delimiter text-string delimiter	Creates a personalized login banner.

Configuring a Failed-Login Banner

To configure a message that will be displayed whenever a user fails login (replacing the default message for failed login), use the following commands in global configuration mode:

Command	Purpose
aaa authentication fail-message delimiter text-string delimiter	Creates a message to be displayed when a user fails login.

Instruction
To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

1.4.4 AAA Authentication Username-prompt

To change the text displayed when users are pro mptedto entera username, use the aaa authentication username-prompt command inglobal configuration mode. To return to the default username prompt text, use the no form of this command, username：
The aaa authentication username-prompt command does not change any dialog that is supplied by a remote TACACS+ server.

Use the following command to configure in global configuration mode：

Command	Purpose
aaa authentication username-prompt text-string	String of text that will be displayed when the user is prompted to enter an username.

1.4.5 AAA Authentication Password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command in global configuration mode. To return to the default password prompt text, use the no form of this command.

password：
The aaa authentication password-prompt command does not change any dialog that is supplied by a remote TACACS+ server. Use the following command to configure in global configuration mode：

Command	Purpose
aaa authentication password-prompt text-string	String of text that will be displayed when the user is prompted to enter a password.

1.4.6 Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:
- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
- To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and "no escape" situations

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration:

Use the no form of this command to delete a username.
username name (nopassword | password password \ password encryption-type encrypted-password}
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-rotary rotary-group-number\
username name [callback-line [tty | aux] line-number [ending-line-number\\
username name [noescape] [nohangup]
username name [privilege level]
username name [user-maxlinks number]
no username name

1.4.7 Enabling Password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode.

To remove the password requirement, use the no form of this command.

enable password {[encryption-type] encrypted-password} [level level]
no enable password [level level]

1.5 AAA Authentication Configuration Example

RADIUS Authentication Example

This section provides one sample configuration using RADIUS.

The following example shows how to configure the switch to authenticate and authorize using RADIUS:
aaa authentication login radius-login group radius local
aaa authorization network radius-network radius line vty
login authentication radius-login

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:
- The aaa authentication login radius-login radius local command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authentication ppp radius-ppp radius command configures the software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.
- The aaa authorization network radius-network radius command command queries RADIUS for network authorization, address assignment, and other access lists.
- The login authentication radius-login command enables the radius-login method list for line 3.

1.6 AAA Authentication Configuration Task List

- Configuring EXEC Authorization using MA

1.7 AAA Authentication Configuration Task

To configure AAA authentication, perform the following configuration processes：

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
(2) Define the method lists for authentication by using an AAA authentication command.

(3) Apply the method lists to a particular interface or line, if required.

1.7.1 Configuring EXEC Authorization Using AAA

Use the aaa authorization command to enable authorization

Use aaa authorization exec command to run authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.

Use line configuration command login authorization to apply these lists. Use the following command in global configuration mode:

Command	Purpose
aaa authorization exec (default | list-name} method1 [method2...]	Establishes global authorization list.
line [console | vty] line-number [ending-line-number\	Enters the line configuration mode for the lines to which you want to apply the authorization method list.
login authorization {default | list-name}	Applies the authorization list to a line or set of lines (in line configuration mode).

The keyword list-name is the character string used to name the list of authorization methods.

The keyword method specifies the actual method during authorization process. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. The system uses the first method listed to authorize users for specific network services; if that method fails to respond, the system selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted. If all specified methods fail to respond, and you still want the system to enter the EXEC shell, you should specify none as the last authorization method in command line.

Use default parameter to establish a default list, and the default list will apply to all interfaces automatically. For example, use the following command to specify radius as the default authorization method for exec:
aaa authorization exec default group radius

Note:
If no method list is defined, the local authorization service will be unavailable and the authorization is allowed to pass.

The following table lists the currently supported EXEC authorization mode:

Keyword	Description
group WORD	Uses a named server group for authorization.
group radius	Uses radius authorization.
local	Uses the local database for authorization.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.

1.8 AAA Authentication Example

1. EXEC local authorization example

```
aaa authentication login default local
aaa authorization exec default local
!
username execl password 0 abc privilege 15
username exec2 password 0 abc privilege 10
```

```
username exec3 nopassword
username exec4 password 0 abc user-maxlinks 10
username exec5 password 0 abc autocommand telnet 172.16.20.1
!
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The aaa authentication login default local command defines the default method list of login authentication. This method list applies to all login authentication servers automatically.
- The aaa authorization exec default local command defines default method list of exec authorization. The method list automatically applies to all users that need to enter exec shell.
- Username is execL login password is abc, EXEC privileged level is 15(the highest level), that is, when userexecl whose privileged level is 15 logs in exec shell, all commands can be checked and performed.
- Username is exec2, login password is abc, EXEC privileged level is 10, that is, when user exec2 whose privileged level is 10 logs in EXEC shell, commands with privileged level less than 10 can be checked and performed.
- Username is exec3, no password is needed for login.
- Username is exec4, login password is abcT the maximum links of the user is 10.
- Username is exec5, login password is abc, user performs telnet 172.16.20.1 immediately when logging in exec shell.

1.9 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA

1.10 AAA Accounting Configuration Task

To configure AAA accounting, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
(2) Define the method lists for accounting by using an AAA accounting command.
(3) Apply the method lists to a particular interface or line, if required.

1.10.1 Configuring EXEC Authorization Using AAA

Use the aaa accounting command to enable AAA accounting.

To create a method list to provide accounting information about all outbound connections made from the network access server, use the aaa accounting connection command.

Command	Purpose
aaa accounting connection (default | list-name} {start-stop | stop-only | none} group groupname	Establishes global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported connection accounting methods:

Keyword	Description
group WORD	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.10.2 Configuring Network Accounting Using AAA

Use the aaa accounting command to enable AAA accounting.

To create a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions, use the aaa accounting network command in global configuration mode.

Command	Purpose
aaa accounting network (default | list-name} {start-stop | stop-only | none} group groupname	Enables global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported network accounting methods:

Keyword	Description
group WORD	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.10.3 AAA Accounting Update

To enable periodic interim accounting records to be sent to the accounting server, use the aaa accounting update command in global configuration mode. To disable interim accounting updates, use the no form ofthis command.

Command	Purpose
aaa accounting update [newinfo] [periodic number]	Enables AAA accounting update.

If the newinfo keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the periodic keyword, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accountingrecord is sent.

When using both the newinfo and periodic keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure the aaa accounting update newinfo periodic number command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the newinfo algorithm.

1.10.4 AAA Accounting Suppress Null-username

To prevent the AAA system from sending accounting records for users whose username string is NULL, use the aaa accounting suppress null-username command in global configuration mode. To allow sending records for users with a NULL username, use the no form of this command.

• aaa accounting suppress null-username

2. Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set.

2.1 AAA Overview

2.1.1 AAA Security Service

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
- AppleTalk Remote Access (ARA)
- NetBIOS Frame Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections
- Switch-to-switch situations. RADIUS does not provide two-way authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

2.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

(1) The user is prompted for and enters a username and password.
(2) The username and encrypted password are sent over the network to the RADIUS server.
(3) The user receives one of the following responses from the RADIUS server:
a. ACCEPT—The user is authenticated.
b. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
c. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
d. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:
Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

Connection parameters, including the host or client IP address, access list, and user timeouts.

2.2 RADIUS Configuration Step

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the aaa authentication global configuration command to define method lists for RADIUS authentication. For more information about using the aaa authentication command, refer to the "Configuring Authentication" chapter.
- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the

"Configuring Authentication" chapter.

The following configuration tasks are optional:

- You may use the aaa authorization global command to authorize specific user functions. For more information about using the aaa authorization command, refer to the chapter "Configuring Authorization."
- You may use the aaa accounting command to enable accounting for RADIUS connections. For more information about using the aaa accounting command, refer to the chapter "Configuring Accounting."

2.3 RADIUS Configuration Task List

- Configuring Switch to RADIUS Server Communication
- Configuring Switch to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

2.4 RADIUS Configuration Task

2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider.

A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

Command	Purpose
radius-server host ip-address [auth-port porf-nu/T7ber] [acct-port portnumber\	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key string	Specifies the shared secret text string used between the router and a RADIUS server.

To configure global communication settings between the router and a RADIUS server, use the following radius-server commands in global configuration mode:

Command	Purpose
radius-server retransmit retries	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
radius-server timeout seconds	Specifies for how many se c onds aswitc h waitsfoe a reply to a RADIUS request before retransmitting the request.
radius-server deadtime minutes	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

2.4.2 Configuring Switch to RADIUS Server Communication

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26).

Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use.

For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

Command	Purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the aaa authentication command, specifying RADIUS as the authentication method. For more information, refer to the chapter "Configuring Authentication."

2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the aaa authorization command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the aaa accounting command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

2.5 RADIUS Configuration Examples

2.5.1 RADIUS Authentication and Authorization Example

The following example shows how to configure the router to authenticate and authorize using RADIUS:
aaa authentication login use-radius group radius local

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:
aaa authentication login use-radius radius local configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, use-radius is the name of the method list, which specifies RADIUS and then local authentication.

RADIUS Authentication, Authorization, and Accounting Example

The following example shows a general configuration using RADIUS with the AAA command set:
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password Along Password
aaa authentication login admins radius local
line vty 1 16
login authentication admins

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:
radius-server host command defines the IP address of the RADIUS server host.
radius-server key command defines the shared secret text string between the network access server and the RADIUS server host.
aaa authentication login admins group radius local command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP;
login authentication admins command applies the "admins" method list for login authentication.

2.5.2 RADIUS Application Example

The following example shows how to define the general configuration through the AAA command set:
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd username root password AlongPassword aaa authentication login admins radius local line vty 1 16
login authentication admins

In the example above, each command line has its own meaning. See the following content:
The command radius-server host defines the IP address of the RADIUS server.
The command radius-server key defines the shared pin between the network access server and the RADIUS server.
The command aaa authentication login admins radius local defines the authentication method list admins, which first specifies RADIUS as the authentication method and then uses the local authentication if the RADIUS server does not respond.
The command login authentication admins specify the method list admins as the login authentication method.

3. Web Authentication Configuration

The section describes the concept of web authentication and configuration and usage of the Web authentication.

3.1 AAA Overview

3.1.1 AAA Security Service

The web authentication of the switch is a connection control mode as PoE and 802.1 x. When you use the Web authentication, the login and logout operations can be successfully performed through the interaction of the browser and the builtin portal server of the switch. During the operations of login and logout, no other client software need be installed.

1) Device role

The roles that the network devices take during the Web authentication are shown in Figure 3-1:

- Client It is a user computer that accesses network through the switch. The user computer need be configured the network browser, the function of DHCP client and the function to originate DNS query.
- DHCP server: It is to distribute the IP address for users.
- AAA server: It is to save user right information and to charge users for their network access.
- Switch: It is a switch having web authentication. It is to control the access right of users and works as an agent between users and AAA server.

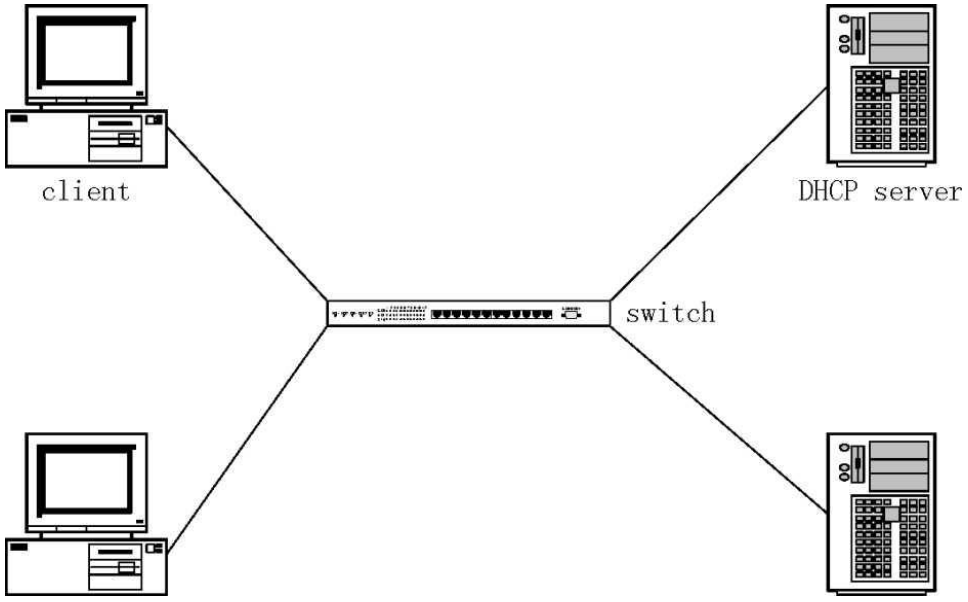

Figure 3-1 Web authentication network

2) Authentication flow

According to different configuration strategies, the Web authentication flow of the switch may relate to protocols such as DHCP and DNS. Its typical flow is shown in Figure 3-2. The Web authentication flow generally contains the following steps:

(1) The DHCP server sends a DHCP confirmation request to a user through the switch after the user originates the process of DHCP address distribution. The switch then identifies and records the user.
(2) The user accesses any Website through the browser (Write down the domain name, not the IP address, in the host part of the url column in the browser), which activates the DNS request of the user computer.
(3) The DNS server returns the user a request response. The switch captures the request response message and changes the resolved address to the address of the built-in portal server in the switch.
(4) The DHCP confirmation process continues after the browser captures DNS resolution. The switch returns the corresponding authentication page according to different authentication methods after the switch receives the request.
(5) The user submits the authentication request; the switch authenticates the user through the AAA server after the switch receives information submitted by the user; if the authentication succeeds, the AAA server will be notified to start charging; the switch gives the user the network access right and returns the user a page that the authentication is successful; meanwhile, the switch also returns a keep alive page, which periodically sends the user online notification to the switch.
(6) The user sends the logout request to the switch through the browser. The switch then notifies the AAA server to stop charging, and withdraws the network access right from the user.
(7) In the period between successful user authentication and logout, the switch periodically detects the user online notification. If the notification is not received in the present time, the switch considers that the user abnormally logs off, notifies the AAA

server to stop charging and withdraws the network access right from the user.

The above steps may vary a little with configuration strategies and user's operations. For example, if user directly accesses the portal server of the switch before the authentication is approved, DNS-related processes will not be enabled.

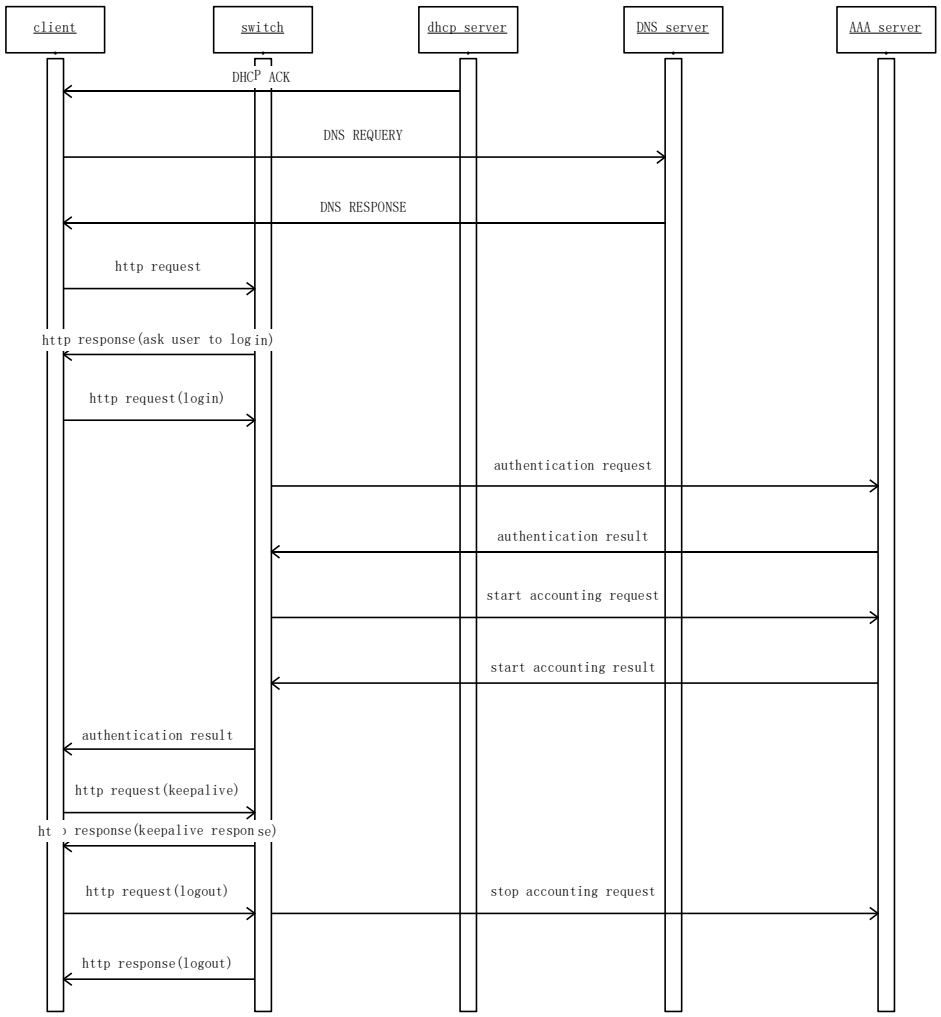

Figure 3-2 web authentication flow

3.1.2 AAA Security Service

(1) Planning the authentication mode

Two authentication modes are provided to control user's access:
Username/password authentication mode: In this mode, the switch identifies the user through the username and password, and notifies the AAA server to start charging according to username; user needs to enter the username and password through the browser.

VLAN ID authentication mode: In this mode, the switch identifies the user through the VLAN ID the user belongs to, and notifies the AAA server to start charging according to VLAN ID; user only requires to confirm corresponding operations on the Web page before accessing the network.

Different operation strategies adopt different authentication modes. The supported maximum number of users that simultaneously access the network varies with the authentication mode. For the username/password authentication mode, the switch supports simultaneously accessed users as many as its performance permits. For the VLAN ID authentication mode, the maximum number of simultaneously accessed users equals the number of VLAN that the switch supports.

(2) Planning network topology

The switch takes the routing interface as a unit to set the authentication attribute, if the web authentication function is enabled on a routing intelace, network accesues through the routing interface are all controlled by the web authentication, the dhcp server, dns server or aaa server should connect the switch through the interface with web authentication function disabled. figure3-3 shows the relative typical network topology.

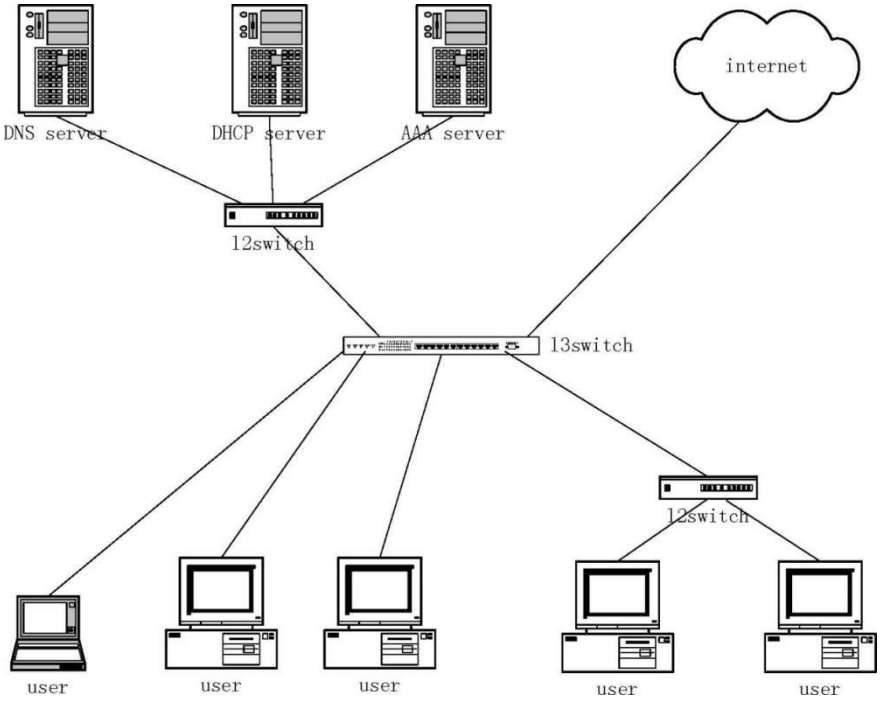

Figure 3-3 Typical network topology

3.2 Configuring Web Authentication

3.2.1 AAA Security Service

(1) Configuring the address of the portal server

Run the following command in global configuration mode to configure the address of the portal server:

Run...	To...
web-auth portal-server A.B.C.D	Configure the IP address of the portal server.

(2) Configuring authentication duration

The parameter authtime determines the maximum time of user's authentication. If the authentication is not approved within the maximum time, the switch terminates the authentication procedure.

Run the following command in global configuration mode to configure the authentication duration (Unit: second):

Run...	To...
web-auth authtime <60-65535>	Configure the authentication duration.

(3) Configuring the transmission period of the online notification

Through the online notification sent by the browser, the switch checks whether the user is online.

Run the following command in global configuration mode to configure the transmission period (unit: second):

Run...	To...
web-auth keep-alive <60-65535>	Configure the transmission period for the online notification.

(4) Configuring the duration to detect the abnormal logout

When the switch does not receive the user online notification from the browser in the set duration, the switch considers that user logs out abnormally.

Run the following command in global configuration mode to configure the duration to detect the abnormal logout:

Run...	To...
web-auth holdtime <60-65535>	Configure the duration to detect user's abnormal logout.

(5) Configuring password for the VLAN ID authentication

When the authentication mode is set to VLAN ID, the switch takes vlan n as the user name, n representing the corresponding VLAN serial number. All user names use the same password.

Run the following command in global configuration mode to configure the password for the VLAN ID authentication:

Run...	To...
web-auth vlan-password <WORD>	Configure the password for the VLAN ID authentication.

3.2.2 Interface Configuration

(1) Configuring authentication mode

The switch provides two authentication modes: username/password and VLAN ID.

Run the following command in interface configuration mode to configure the authentication mode:

Run...	To...
web-auth mode user | vlan-id	Configure the authentication mode.

(2) Configuring authentication method list

Different authentication method lists can be applied on each interface. By default, the authentication method list named default is applied on each interface.

Run the following command in interface configuration mode to configure the authentication method list:

Run...	To...
web-auth authentication WORD	Configure the authentication method list

(3) Configuring the accounting method list

Different accounting method lists can be applied on each interface. By default, the accounting method list named default is applied on each interface.

Run the following command in interface configuration mode to configure the accounting method list:

Run...	To...
web-auth accounting WORD	Configure the accounting method list.

3.2.3 Enabling Web Authentication

If global configuration and interface configuration satisfy the requirements, you can enable the Web authentication on the designated routing switch.

Run the following command in interface configuration mode to enable the Web authentication:

Run...	To...
web-auth enable	Enable the Web authentication.

3.3 Monitoring and Maintaining Web Authentication

3.3.1 Checking the Global Configuration

Run the following command in privileged mode to check the global configuration:

Run...	To...
show web-auth	Check the global configuration.

3.3.2 Checking Interface Configuration

Run the following command in interface configuration mode to check the interface configuration:

Run...	To...
show web-auth interface [vlan | SuperVian]	Check the interface configuration.

3.3.3 Checking User State

Run the following command in privileged mode to check the user state:

Run...	To...
show web-auth user	Check the user state.

3.3.4 Mandatorily Kicking Out Users

Run the following command in global configuration mode to mandatorily kick out a user.

Run...	To...
web-auth kick-out user-IP	Mandatorily kick out a user.

3.4 Web Authentication Configuration Example

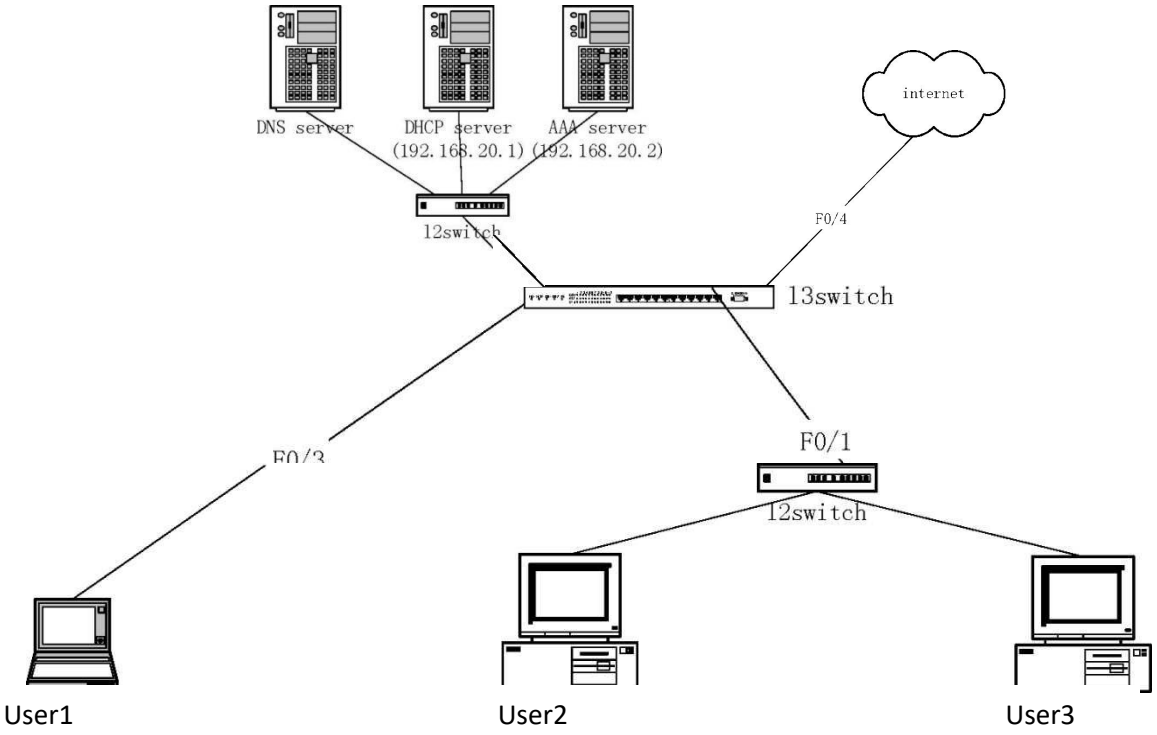

Figure 3-4 Network topology

Global configuration

```
aaa authentication login auth-weba radius
aaa accounting network acct-weba start-stop radius
!
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813 radius-server key 405.10
!
ip dhcpd enable
ip http server
!
vlan 1-4
!
web-auth portal-server 192.168.20.41
web-auth holdtime 3600
web-auth authtime 600
web-auth keep-alive 180
```

Configuration of the layer-2 interface

```
interface FastEthernetO/1
switch port pvid 1
interface FastEthernetO/2
switch port pvid 2

interface FastEthernetO/3
switchport pvid 3
!
interface FastEthernetO/4
switchport pvid 4
```

Configuration of the routing interface

```
interface VLAN1
no ip directed-broadcast
ip helper-address 192.168.20.1 web-auth accounting acct-weba web-auth authentication auth-weba web-auth mode vlan-id
web-auth enable
!
```

```
interface VLAN2
ip address 192.168.20.41 255.255.255.0 no ip directed-broadcast
!
interface VLAN3
no ip directed-broadcast
ip helper-address 192.168.20.1 web-auth accounting acct-weba web-auth authentication auth-weba web-auth mode user
web-auth enable
!
interface VLAN4
no ip directed-broadcast
```