Contents

1 Configuring RADIUS

1.1 Introduction

1.1.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed authentication, authorization and accounting (AAA) protocol based on the client/server architecture. It works with AAA to provide AAA security services for users.

When providing AAA security services, a network device serves as a RADIUS client to provide user information to the RADIUS server to initiate security service requests. The remote RADIUS server stores user information and network service information, and provides security services for users by responding to requests from the RADIUS client.

RADIUS is usually applied in networks that have high security requirements and allow remote user access. As a completely open protocol, many systems (such as UNIX, Windows 2000, and Windows 2008) support the installation of RADIUS as a system component. Therefore, the RADIUS server becomes the most widely used security server.

1.1.2 Principles

1. Basic Concepts

- Client/server mode

  RADIUS uses the client/server mode and consists of RADIUS clients and the RADIUS server.

  - As the initiator of RADIUS requests, a RADIUS client usually runs on a network access server (NAS). It provides user information for the RADIUS server, and receives and processes responses from the RADIUS server, for example, accepting or rejecting user access, and requesting user-specific information.
  - The RADIUS server maintains the IP addresses and shared key of RADIUS clients as well as configured user information, and provides authentication, authorization, and accounting services by responding to requests from RADIUS clients. One RADIUS server usually corresponds to multiple RADIUS clients.

- Shared key

  A shared key is a string shared between a RADIUS client and the server. It is used to encrypt and decrypt user passwords during RADIUS packet transmission and generate packet verification fields, in an effort to ensure RADIUS communication security.

- RADIUS server group

  Security methods used in AAA security services are based on server groups. Likewise, RADIUS provides AAA security services based on RADIUS server groups. One security method corresponds to one RADIUS server group and one or more RADIUS severs can be configured in each RADIUS server group.

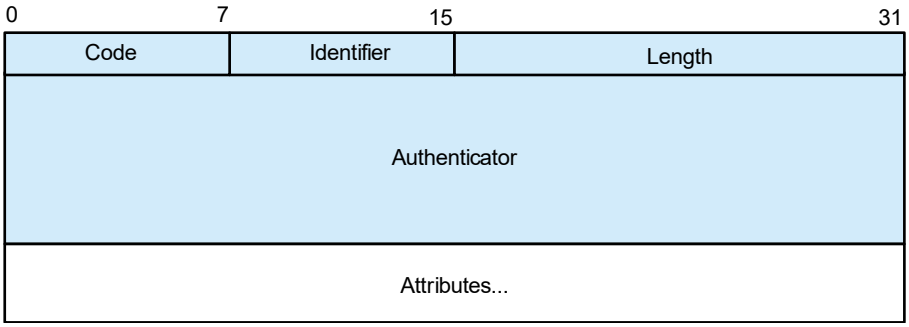
  If multiple RADIUS servers are configured in a RADIUS server group, when a device fails to communicate with the first RADIUS server or the first RADIUS server is unreachable, the device automatically attempts

to communicate with the second RADIUS server, and so on. The attempt lasts till the communication succeeds or the communication with all RADIUS servers fails.

2. RADIUS Packet

- Packet structure

Figure 1-1 Structure of a RADIUS Packet



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

Table 1-1 Description of Fields Contained in a RADIUS Packet

Field	Length	Description	Remarks
Code	1 byte	Identifies the packet type.	Values corresponding to common packet types and their meanings are as follows: **1**: Access-Request **2**: Access-Accept **3**: Access-Reject **4**: Accounting-Request **5**: Accounting-Response **11**: Access-Challenge
Identifier	1 byte	Matches a request with a response packet.	Request packets and response packets of the same type have the same identifier value.
Length	2 bytes	Indicates the length of a RADIUS packet.	The value is the sum of the lengths of the **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes** fields. If the length of a received packet is greater than the value of **Length**, the content beyond the value of **Length** is ignored as filling information. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
Authenticator	16	Verifies packets and	N/A

Field	Length	Description	Remarks
	bytes	encrypts and decrypts user passwords.	
Attributes	Variable length	Carries authentication, authorization, and accounting information.	This field usually contains multiple attributes and each attribute is represented in the type, length, value (TLV) format.

- RADIUS attributes

  RADIUS attributes carry authentication, authorization, and accounting information, and each attribute is represented in the TLV format, as described in Table 1-2.

Table 1-2Description of RADIUS Attribute Fields

Field	Length	Description
Type	1 byte	Attribute type
Length	1 byte	Total length of an attribute (TLV)
Value	Variable length	Attribute description

Table 1-3RADIUS Attribute List

Attribute No.	Attribute Name	Attribute No.	Attribute Name
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit

Attribute No.	Attribute Name	Attribute No.	Attribute Name
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

- Introduction to RADIUS attributes

  This section describes some of the important attributes.

  - Attribute 31

    When a RADIUS client sends a request packet to the RADIUS server, information is filled in attribute 31 (**Calling-Station-ID**) to identify the user to be authenticated. The MAC address of a user is often used as the attribute content. For example, in IEEE 802.1X authentication, the device uses the MAC address of the device where the IEEE 802.1X client resides as the attribute content.

    Different RADIUS servers have different requirements for the format of the MAC address in attribute 31. Therefore, ensure that the MAC address format used by RADIUS clients is the same as that used by the server. Currently, the following three MAC address formats are supported.

Table 1-4 Supported Formats of the MAC Address in Attribute 31

MAC Address Format	Description
ietf	Standard format specified in the Internet Engineering Task Force (IETF) standard (RFC3580). It uses hyphens (-) as the separator, for example, 00-D0-F8-33-22-AC.
normal	Dotted hexadecimal format using dots (.) as the separator, for example, 00d0.f833.22ac.
unformatted	Default format with no separator, for example, 00d0f83322ac.

- Attribute 26

  Attribute 26 (**Vendor-Specific**) is also called a private attribute, which allows device vendors to define attributes. Device vendors can define multiple attributes in the TLV format in attribute 26. Table 1-5 lists private attributes supported by Orion_B26Q products.

Table 1-5 List of Orion_B26Q Private Attributes

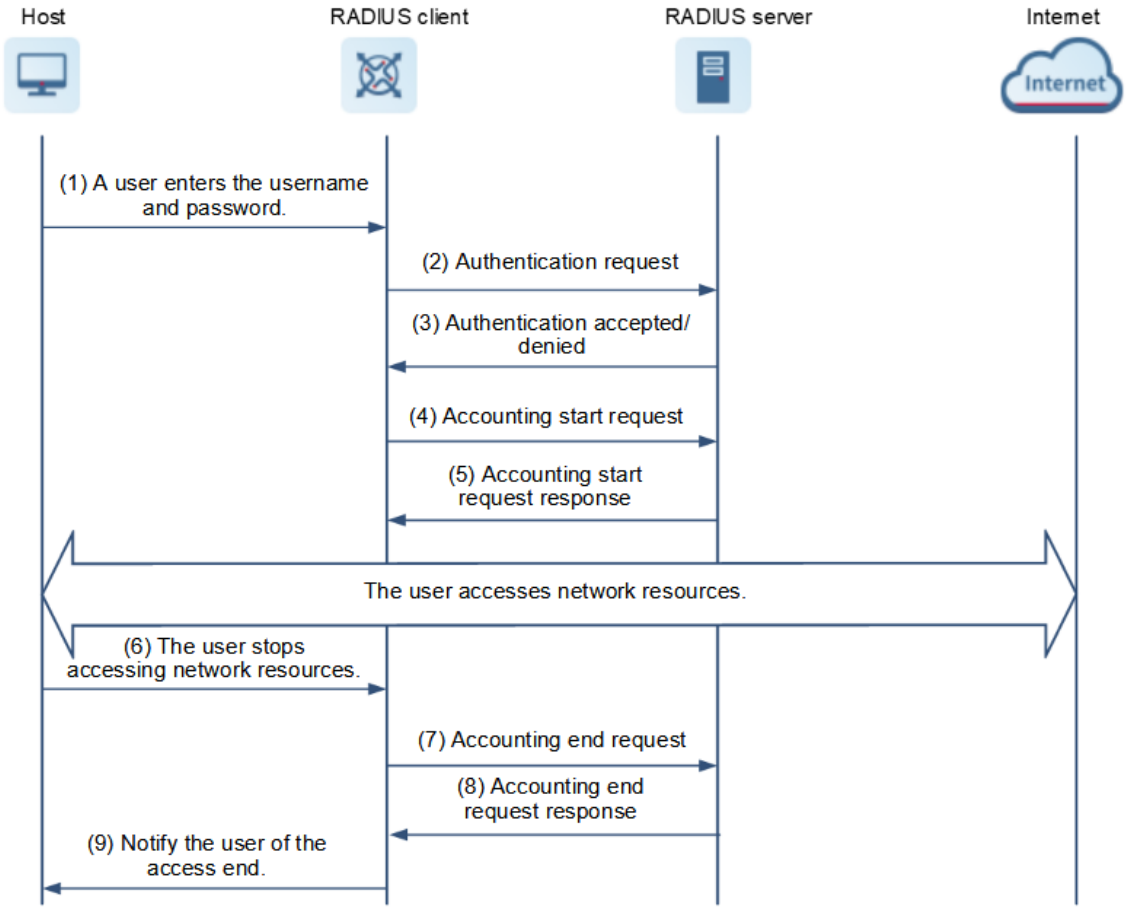
ID	Function	Type	Extended Type
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	VLAN-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	IPv6-multicast-address	79	79

ID	Function	Type	Extended Type
27	IPv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

3. RADIUS Authentication, Authorization, and Accounting

RADIUS provides authentication, authorization, and accounting for users. The interaction process is shown in Figure 1-1.

Figure 1-1RADIUS Authentication, Authorization, and Accounting Process



- RADIUS authentication and authorization process

a A user enters the username and password and sends them to a RADIUS client.

b After receiving the username and password, the RADIUS client sends an authentication request packet to the RADIUS server. The password in the authentication request packet is encrypted.

c After receiving the authentication request, the RADIUS server checks whether the username and password are legitimate. If yes, the RADIUS server accepts the authentication request and delivers authorization information of the user. If no, the RADIUS server rejects the authentication request.

- RADIUS accounting process

dIf the RADIUS server returns an authentication success message in the user authentication process, the RADIUS client sends an accounting start request packet to the RADIUS server.

eThe RADIUS server returns an accounting start response packet and starts accounting.

fWhen stopping accessing network resources, the user sends a disconnection request to the RADIUS client.

gThe RADIUS client sends an accounting end request packet to the RADIUS server.

hThe RADIUS server returns an accounting end response packet and stops accounting.

iThe user is disconnected from the network and cannot access network resources.

4. RADIUS Packet Retransmission Upon Timeout

After sending a packet to the RADIUS server, a RADIUS client uses a timer to test whether the RADIUS server responds within the specified time. If the RADIUS server does not respond within the specified time, the RADIUS client retransmits the packet. The following timeout and retransmission parameters need to be configured:

- RADIUS server timeout duration

  The response time of a RADIUS server depends on its performance and the network environment. Configure a proper timeout duration based on the actual situation.

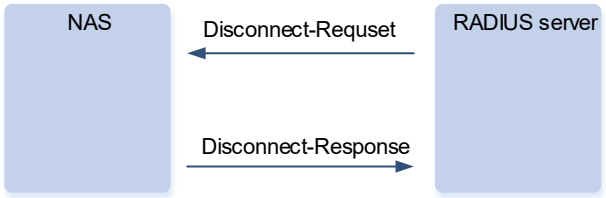
- Retransmission count
- Whether accounting update packets need to be retransmitted

5. RADIUS Forcible Logoff

Users can go offline actively. In addition, the RADIUS server can send messages to force authenticated users offline.

RADIUS forcible logoff is a user logoff management method defined in the protocol of Dynamic Authorization Extensions to RADIUS. The NAS and RADIUS server exchange Disconnect-Messages (DMs) to force authenticated users offline. The protocol of Dynamic Authorization Extensions to RADIUS enables NASs from different vendors to be compatible with RADIUS servers in user logoff processing.

Figure 1-1DM Interaction of Dynamic Authorization Extensions to RADIUS



The DM interaction between a RADIUS server and the NAS is as follows:

(1) The RADIUS server actively sends a Disconnect-Request message to port UDP3799 of the NAS to initiate a user logoff request.

(2)The NAS searches for the user based on the user session information and username carried in the Disconnect-Request message and logs off the user.

(3)The NAS sends the logoff result to the RADIUS server through a Disconnect-Response message.

1.1.3 Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Configuration Task Summary

RADIUS configuration includes the following tasks:

(1)Configuring RADIUS Basic Features

(2)Configuring a RADIUS Server Group

(3)(Optional) Configuring RADIUS Attributes Select at least one of the following tasks to configure.

- Configure the Attribute Format
- _
- Configuring Compatibility with Devices of Other Vendors

(4)(Optional) Configuring RADIUS Reachability Detection

(5)(Optional) Configuring the DSCP Value for RADIUS Packets

(6)(Optional) Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server

(7)(Optional) Configuring the Accounting-On Function

(8)(Optional) Configuring the Accounting Packet Copying Function

1.3 Configuring RADIUS Basic Features

1.3.1 Overview

This section describes how to configure parameters for the communication between a network device and a RADIUS 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 RADIUS server and give responses.

1.3.2 Restrictions and Guidelines

- Before configuring RADIUS, ensure that the network communication between the device and the RADIUS server is in good condition.
- Before configuring RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

1.3.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure a RADIUS remote server.

radius-server host [**oob** [**via Mgmt** *Mgmt_number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

No RADIUS remote server is configured by default.

If a RADIUS server is not added to a RADIUS server group, the device uses the global routing table when communicating with the RADIUS server. Otherwise, the device uses the virtual routing and forwarding (VRF) routing table of the RADIUS server group.

(4)Configure a shared key for the communication between the device and the RADIUS server.

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

No shared key for the communication between the device and the RADIUS server is configured by default.

A shared key is the basis for correct communication between the device and the RADIUS server. The same shared key must be configured on them both to ensure normal communication between them.

(5)(Optional) Configure the source address for RADIUS packets.

ip radius source-interface *interface-type interface-number*

The source IP address of RADIUS packets is set by the network layer by default.

After this command is configured, the device uses the first IP address of the interface specified in the command as the source address of RADIUS packets. Ensure that the communication between the configured address and the RADIUS server is normal. Specifying the source IP address for packets to be sent to the RADIUS server can reduce the NAS information maintenance workload on the RADIUS server.

(6)(Optional) Configure the source UDP port to be used by the device to send RADIUS packets.

radius-server source-port *source-port*

The source UDP port used by the device to send RADIUS packets is a random packet by default.

(7)(Optional) Configure the waiting time, after which the device retransmits a RADIUS request packet.

radius-server timeout *timeout*

The default waiting time before the retransmission of a RADIUS packet is **5** seconds.

(8)(Optional) Configure the accounting update packet retransmission function for Web-authenticated users.

radius-server account update retransmit

The accounting update packet retransmission function is enabled for Web-authenticated users by default.

The configuration does not affect users of other authentication types.

1.4 Configuring a RADIUS Server Group

1.4.1 Overview

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

1.4.2 Restrictions and Guidelines

- RADIUS security services are a type of AAA services and need to be used in combination with AAA features. RADIUS provides security services for users as one method in an AAA method list.
- When configuring the authentication 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.
- RADIUS server groups support 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 radius 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 **radius**.

1.4.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure a RADIUS server group.

aaa group server radius *group-name*

No RADIUS server group is configured by default.

You can group RADIUS servers so that authentication and accounting can be completed by different server groups.

(4)Add a server to the RADIUS server group.

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

No server is added to a RADIUS server group by default.

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

ip vrf forwarding *vrf-name*

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

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

(6) (Optional) Configure an MGMT port to be used by the RADIUS server group.

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

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

1.5 Configuring RADIUS Attributes

1.5.1 Overview

RADIUS attributes are used to carry authentication, authorization, and accounting information to be used in packet interaction. You can configure the attribute format, private attribute processing method, and vendor compatibility.

1.5.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configure the Attribute Format
-
- Configuring Compatibility with Devices of Other Vendors

1.5.3 Configure the Attribute Format

1. Overview

This section describes how to configure the attribute format to be used in encapsulation and parsing.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure RADIUS attributes. Configure at least one of the tasks.

- Configure the format of the MAC address used in attribute 31 (**Calling-Station-ID**).

  radius-server attribute 31 mac format { **3hyphen** | **ietf** | **normal** | **unformatted** | { { **colon-split** | **dot-split** | **hyphen-split** } { **mode1** | **mode2** } [**lowercase** | **uppercase**] } }

  The MAC address used in attribute 31 uses the unformatted pattern.

  Some RADIUS servers (mainly used for IEEE 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the format of MAC addresses used in attribute 31 to the IETF format.

- Configure the encapsulation format for the **NAS-Port-ID** attribute.

  radius-server attribute nas-port-id format { **mode**1 | **normal** | **port-vid** | **qinq** }

  The default encapsulation format of the **NAS-Port-ID** attribute is the normal format.

  Use this command to configure the encapsulation format for the **NAS-Port-ID** attribute applicable to 802.1Q in 802.1Q (QinQ) scenarios or non-QinQ scenarios.

- Configure the parsing mode for the **Class** attribute.

  radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** | **unit bit/s** | **unit byte/s** }

  The function of parsing the rate limit configuration from the **Class** attribute of RADIUS packets is disabled by default.

Configure this command if a server needs to deliver the rate limit value by using the **Class** attribute.

- Configure whether RADIUS authentication request packets carry a specified attribute.

  radius-server authentication attribute *type* { **package** | **unpackage** }

  According to the RFC standard, attributes that must be carried in authentication requests are carried by default, attributes that do not need to be carried are not carried by default, and other attributes are in the unset state by default.

- Configure whether RADIUS accounting request packets carry a specified attribute.

  radius-server account attribute *type* { **package | unpackage** }

  According to the RFC standard, attributes that must be carried in accounting requests are carried by default, attributes that do not need to be carried are not carried by default, and other attributes are in the unset state by default.

1.5.4 Configuring Orion Private Attributes

1. Overview

Vendors can define private attributes to implement some features that are not supported by the standard RADIUS protocol. You can configure the methods used by devices to process private attributes based on the actual environment. Private attributes configured in this section are all Orion_B26Q private attributes.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure Orion_B26Q private attributes. Configure at least one of the tasks.

- Configure the device to set the private attribute **port-priority** delivered by the server to the class of service (CoS) value of an interface.

  radius set qos cos

  The device sets the private attribute **port-priority** delivered by the server to the differentiated services code point (DSCP) value by default.

- Configure the device to support the **CUI** attribute.

  radius support cui

  The function of supporting the **CUI** attribute by RADIUS is disabled by default.

1.5.5 Configuring Compatibility with Devices of Other Vendors

1. Overview

In actual deployment environments, Orion_B26Q devices may interconnect to RADIUS servers of other vendors. Private attributes defined by different vendors are different. It is necessary to enable compatibility with the configuration of devices of other vendors.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure compatibility with devices of other vendors. Configure at least one of the tasks.

- Configure whether RADIUS authentication request packets carry the private attributes of a specified vendor.

  radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

  Authentication request packets do not carry private attributes of other vendors by default.

- Configure whether RADIUS accounting request packets carry the private attributes of a specified vendor.

  radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

  Accounting request packets do not carry private attributes of other vendors by default.

- Configure RADIUS to parse private attributes of Cisco, Huawei, and Microsoft devices carried in packets.

  radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

  RADIUS parses private attributes of Cisco, Huawei, and Microsoft devices carried in packets by default.

- Enable the function of not differentiating private vendor IDs during RADIUS packet parsing.

  radius vendor-specific extend

  RADIUS identifies only Orion_B26Q private vendor ID during packet parsing by default.

- Configure the mode of parsing private attributes.

  radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

  RADIUS parses private attributes of Cisco, Huawei, and Microsoft devices carried in packets by default.

  If the server is a Orion_B26Q application server, the RADIUS private attribute type needs to be configured to achieve compatibility.

1.6 Configuring RADIUS Reachability Detection

1.6.1 Overview

A RADIUS 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 RADIUS server unless all servers in the RADIUS server group are unreachable.

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

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

1.6.2 Restrictions and Guidelines

- To enable active detection for a specified RADIUS server, perform the following configuration when configuring the RADIUS server:

- Configure a test username for the RADIUS server.
- Configure at least one tested port (authentication port or accounting port) for the RADIUS server.

- It is judged that a RADIUS server is unreachable only when both conditions below are met:
  - The device fails to receive a correct response packet from the RADIUS server within the specified timeout duration.
  - The number of times that the device sends request packets to the same RADIUS server consecutively reaches the specified timeout count.
- If any of the following conditions is met for an unreachable RADIUS server, the RADIUS server is considered reachable.
  - The device receives correct responses from the RADIUS server.
  - The duration in which the RADIUS server is unreachable exceeds the time configured using the **radius-server deadtime** command, and active detection is disabled for the RADIUS server.
  - The authentication port or accounting port of the RADIUS server is updated on the device.

1.6.3 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 RADIUS server is unreachable.

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

The criteria for judging that a RADIUS server is unreachable are that the timeout duration is 60 seconds and the consecutive timeout count is 10 by default.

If a RADIUS server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS server is unreachable.

(4)Configure active detection and set the IP address, authentication port, or accounting port for the remote RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] *

No active detection is configured by default.

(5)(Optional) Configure the number of times that the device sends requests to a RADIUS server consecutively before confirming that the RADIUS server is unreachable.

radius-server retransmit *retransmit-times*

The device sends requests to a RADIUS server three times consecutively before confirming that the RADIUS server is unreachable by default.

(6)(Optional) Configure the duration for the device to stop sending request packets to an unreachable RADIUS server.

radius-server deadtime *deadtime*

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

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

1.7 Configuring the DSCP Value for RADIUS Packets

1.7.1 Overview

DSCP is in the type of service (ToS) field of the IP header and is used to identify the packet transmission priority.

A larger DSCP value indicates a higher packet priority. The default DSCP value of RADIUS packets is **0**. You can configure the DSCP value for RADIUS packets to change the transmission priority of RADIUS packets.

1.7.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the DSCP value for RADIUS packets.

radius dscp *dscp-value*

The default DSCP value of RADIUS packets is **0**.

1.8 Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server

1.8.1 Overview

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively. You can configure the units of data flows and data packets to be sent to a RADIUS server based on the actual network situation.

1.8.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the units of data flows and data packets to be sent to a RADIUS server.

radius data-flow-format { { **data byte** | **data giga-byte** | **data kilo-byte** | **data mega-byte** } | { **packet giga-packet** | **packet kilo-packet** | **packet mega-packet** | **packet one-packet** } } *

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively.

1.9 Configuring the Accounting-On Function

1.9.1 Overview

The accounting-on function is used to notify a RADIUS server of the device restart. After the device is restarted, online users are forced offline. However, the RADIUS server does not perceive the device restart and does not log off the users. As a result, the users encounter an exception when initiating re-authentication. Therefore, it is necessary to enable the accounting-on function.

1.9.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the function of sending accounting-on packets upon device restart.

radius-server accounting-on enable

The function of sending accounting-on packets upon device restart is enabled by default.

1.10 Configuring the Accounting Packet Copying Function

1.10.1 Overview

RADIUS accounting packets are sent to one server specified in the accounting method list by default. After this function is enabled, the device copies accounting packets and sends the packets to all servers in a server group.

1.10.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the function of copying and sending accounting packets to servers in a specified group.

radius-sever accounting-copy *group*

The function of copying and sending RADIUS accounting packets is disabled by default.

1.11 Monitoring

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

Run the **clear** commands to clear information.

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

Notice

Running the **clear** commands may lose vital information and thus interrupt services.

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

Table 1-1 RADIUS Monitoring

Command	Purpose
show radius parameter	Displays global parameters of a RADIUS server.
show radius server	Displays the configuration of a RADIUS server.
show radius vendor-specific	Displays the configuration of the RADIUS private attribute type.
show radius auth statistics	Displays RADIUS authentication statistics.
show radius radius acct statistics	Displays RADIUS accounting statistics.
show radius group	Displays the configuration of a RADIUS server group.
show radius attribute	Displays RADIUS standard attributes.
show radius-server accounting-copy	Displays the configuration of copying and sending the accounting packets.
debug radius detail	Debugs RADIUS packets.
debug radius extend event	Debugs the function of Dynamic Authorization Extensions to RADIUS.
debug radius extend detail	Debugs packets of Dynamic Authorization Extensions to RADIUS.
debug radius extend error	Prints information related to packets of Dynamic Authorization Extensions to RADIUS for debugging.

1.12 Configuration Examples

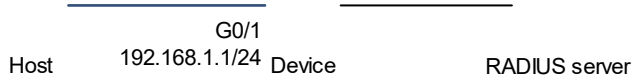
1.12.1 Configuring RADIUS Authentication, Authorization, and Accounting

1. Requirements

A RADIUS server needs to be used for authentication, authorization, and accounting of login users.

2. Topology

Figure 1-1 Topology of RADIUS Authentication, Authorization, and Accounting



3. Notes

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

4. Procedure

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

(2)Enable AAA security services.

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

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

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

(4)Configure the authentication, authorization, and accounting method lists.

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

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

```
Device(config)# line vty 0 4
Device(config-line)# login authentication radius-method
Device(config-line)# authorization exec radius-method
Device(config-line)# accounting exec radius-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#
```

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

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

6. Configuration Files

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

7. Common Errors

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

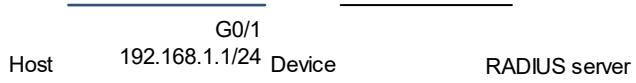
1.12.2 Configuring RADIUS Reachability Detection

1. Requirements

RADIUS reachability detection needs to be configured to identify unreachable RADIUS servers.

2. Topology

Figure 1-1 Topology of RADIUS Reachability Detection



3. Notes

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

4. Procedure

Configure the global criteria for judging that a RADIUS 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 RADIUS server to 192.168.1.3, detection username to **test**, and detection interval to **90** minutes, and disable the server authentication port detection.

```
Device(config)# radius-server host 192.168.1.3 test username test ignore-acct-
port idle-time 90
```

5. Verification

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

```
Hostname# enable
Hostname# show radius server

Server IP:    192.168.1.3
Accounting Port:  1813
Authen  Port:     1812
mom     flag:     1
Test Username:    test
Test Idle Time:   1 Minutes
Test Ports:       Authen and Accounting
Server State:     Dead
    Current duration 1254s, previous duration 2918s
    Dead: total time 1257s, count 1
    Statistics:
        Authen: request 22, timeouts 81
        Author: request 22, timeouts 81
        Account: request 23, timeouts 83
```

6. Configuration Files

```
!
radius-server host 192.168.1.3 test username test ignore-acct-port idle-time 90
key 7 $10$275$g8oXDDIPVeA=$
radius-server dead-criteria time 120 tries 5
!
```