Contents

1 Configuring IEEE 802.1X

1.1 Introduction

1.1.1 Overview

In a local area network (LAN) in compliance with the Institute of Electrical and Electronics Engineers (IEEE) 802 standards, users can connect to network devices to access network resources without authentication and authorization. This access mode does not pose obvious security problems in the early enterprise network application environment. However, with the large-scale development of applications such as mobile office and customer premises network (CPN) operation, this uncontrolled behavior brings great security risks. For this, IEEE develops the 802.1X protocol to solve LAN security problems.

IEEE 802.1X is a port-based network access control standard used to provide secure access services for LANs. This protocol complies with the authentication, authorization and accounting (AAA) security management mechanism. It is usually deployed on user access networks to provide port-based user AAA functions for network administrators.

1.1.2 Principles

1. Basic Concepts

- User

  Users usually refer to clients that need to access network resources. In an IEEE 802.1X wired environment, the MAC address and VLAN ID attributes of each user are unique for user differentiation. All other information (such as the account number and IP address) is changeable for users.

- RADIUS

  Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol applied widely to send authentication information between network devices and RADIUS servers. In actual IEEE 802.1X deployment, this protocol can be used to remotely deploy authentication servers.

- Timeout

  Timeout occurs when a device does not receive any response from a client or server within a specified period of time.

  The device needs to exchange packets with clients and servers during authentication. In response to unexpected factors such as network unavailability, a protocol sets the timeout duration for each exchange step. Each role needs to respond within the timeout duration during authentication. Otherwise, an authentication failure may be caused.

- EAP

  Extensible Authentication Protocol (EAP) carries IEEE 802.1X authentication information.

  EAP provides a universal authentication framework, which supports multiple authentication methods, such as the message digest 5 (MD5) authentication, Challenge-Handshake Authentication Protocol (CHAP)

authentication, Password Authentication Protocol (PAP) authentication, and Transport Layer Security (TLS) authentication. Orion_B26Q IEEE 802.1X module supports the MD5, CHAP, PAP, Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol (PEAP-MSCHAP), and TLS authentication methods.

- EAPOL

  EAP over LAN (EAPOL) is the encapsulation of EAP on a LAN.

  EAPOL encapsulates packets based on the media access control (MAC) layer. The type number is 0x888E. The IEEE 802.1X standard assigns a multicast MAC address 01-80-C2-00-00-03 to the protocol to send packets in the initial authentication process. Orion_B26Q authentication clients may use 01-D0-F8-00-00-03 as the multicast destination address at the beginning of authentication.

- EAPOR

  EAP over RADIUS (EAPOR) is the encapsulation of EAP over RADIUS.

  EAP packets are relayed by network devices. A network device encapsulates EAP packets into RADIUS packets over EAPOR and sends the packets to a RADIUS server for authentication.

2. Authentication

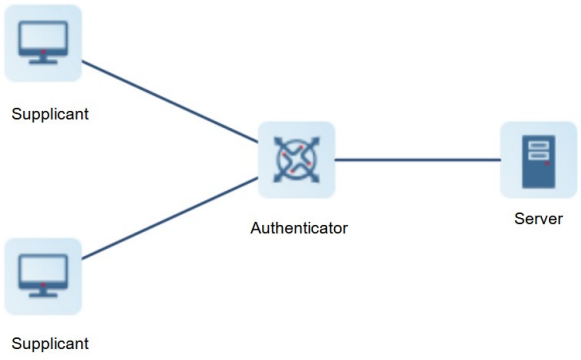
Authentication is a process of verifying user identities and determining whether a user has the legitimate permission to access network resources.

The basic principles of IEEE 802.1X authentication are as follows: A user submits the account and password to an authentication server through a network access server (NAS). The authentication server verifies the account and password. Only users who pass the authentication can obtain network access permissions.

- Authentication roles

  An IEEE 802.1X standard authentication system consists of three roles: supplicant, authenticator, and server, which correspond to the client, NAS, and authentication server (usually RADIUS server) in actual application.

Figure 1-1Authentication Roles



  - Supplicant

    A supplicant is an end user who requests to access network resources. A supplicant is usually a PC.

    A supplicant needs to submit information used for authentication to an authenticator and respond to requests from the authenticator. According to the IEEE 802.1X protocol, a supplicant must run software in compliance with the IEEE 802.1X client standard and the software is responsible for submitting the

account and password during authentication. The most typical software is the IEEE 802.1X client embedded in the operating system (OS). You can also use client software developed by vendors such as Orion_B26Q Supplicant.

- Authenticator

  An authenticator is a NAS that manages supplicants' authentication status and network connection status.

  An authenticator acts as an intermediary between a supplicant and an authentication server. It obtains the account and password used for authentication from a supplicant, and sends them to an authentication server. The authenticator also obtains authentication-related information from the authentication server and sends the information to the supplicant.

- Authentication server

  An authentication server provides the authentication service for users. An authentication server is usually a RADIUS server.

  An authentication server stores legitimate user information and users' authorization information. It checks whether a user is legitimate by verifying the account and password submitted by a supplicant, and manages accounting data submitted by an authenticator. One authentication server can provide the authentication service for multiple supplicants to implement centralized management of users.

- Port type

  There are two types of ports on the device that serves as an authenticator: controlled port and uncontrolled port.

  Users connected to a controlled port can access network resources only after passing authentication. Otherwise, the users can only transmit packets used for authentication. Users connected to an uncontrolled port can access network resources without authentication. The access to network resources needs to be controlled for supplicants and therefore, supplicants need to be connected to controlled ports. Network permission control is not required for authentication servers, and therefore, they need to be connected to uncontrolled ports.

- Authentication process

  A supplicant and an authenticator exchange information through the EAPOL protocol, and an authenticator and an authentication server exchange information through the EAPOR protocol.

  The figure below shows a typical IEEE 802.1X authentication process.

Figure 1-2Authentication Packet Exchange

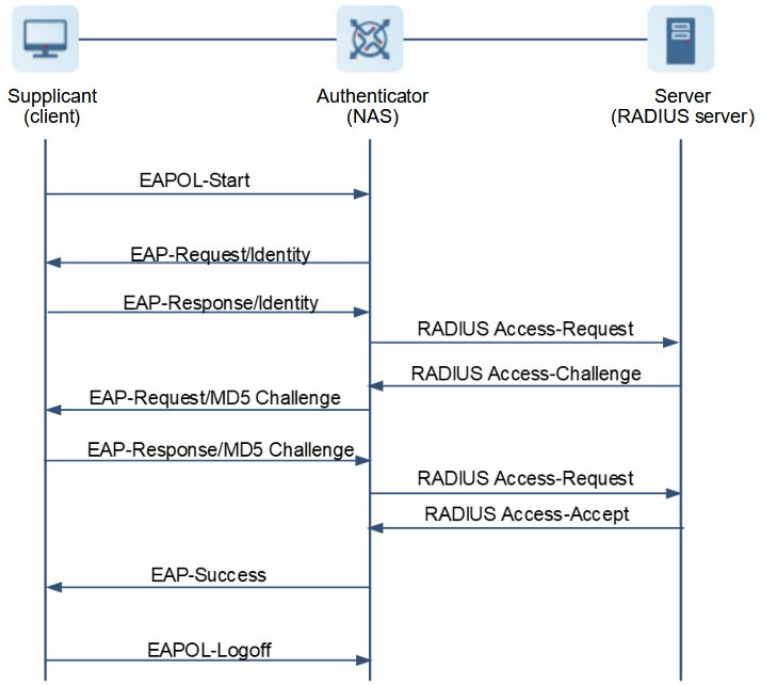


Figure 1-2 shows a typical user-initiated authentication process.

aA user starts the IEEE 802.1X client application on a client and enters the account and password. The client initiates an authentication request to a NAS. So the client sends an authentication request frame (EAPOL-Start) to the NAS.

bAfter receiving the frame, the NAS sends an EAP request frame of the identity type (EAP-Request/Identity) to the client, asking the client to provide the account for authentication.

cAfter receiving the request frame from the NAS, the client sends the account to the NAS through a response frame of the identity type (EAP-Response/Identity).

dAfter receiving the response frame from the client, the NAS retrieves the EAP packet from the frame, encapsulates the EAP packet into a RADIUS packet (RADIUS Access-Request), and sends the packet to an authentication server for processing.

eAfter receiving the Access-Request packet from the NAS, the authentication server parses the account and encrypts the password corresponding to the username by using a randomly generated MD5 Challenge to obtain the encrypted password. The authentication server sends the MD5 Challenge to the NAS through a RADIUS Access-Request packet.

fThe NAS forwards the MD5 Challenge sent by the RADIUS server to the client.

gThe client encrypts the local password by using the received MD5 Challenge and sends the encrypted password to the NAS through an EAP-Response/MD5 packet.

hThe NAS encapsulates the received EAP-Response/MD5 packets into a RADIUS Access-Request packet and sends the packet to the authentication server.

iThe authentication server retrieves the encrypted password from the RADIUS Access-Request packet and compares it with the encrypted password obtained in step e. If they are the same, the authentication server considers the user legitimate and returns an authentication success packet (RADIUS access-Accept) to the NAS.

jAfter receiving the packet, the NAS sends an authentication success frame (EAP-Success) to the client, changes the port status to the authorized state, and allows the user to access the network through the port.

In some special cases (for example, authentication is performed immediately when a user connects to a network), the NAS may actively initiate an authentication request and the step that a user actively initiates a request is skipped.

- User status during authentication

  All users connected to uncontrolled ports can use network resources. Whether users connected to controlled ports can access network resources depends on their authentication status. A user connected to a controlled port cannot access the network when just initiating authentication, and the user is in the unauthorized state. After passing authentication, the user can access the network normally and the status changes to authorized.

  On an IEEE 802.1X-supported network device, all ports are uncontrolled ports by default. You can configure a port as a controlled port to enable all users connected to the port to pass authentication before accessing the network.

  Common user authentication states and behaviors are described as follows:

  - If a user is still in the unauthorized state due to an authentication failure, the user can initiate authentication again.
  - If the network between the NAS and the authentication server is unreachable, a user connected to the NAS is in the unauthorized state.
  - After a user sends an EAPOL-LOGOFF packet, the user transitions from the authorized state to the unauthorized state.
  - When a port on an NAS changes to the LINK-DOWN state, all users connected to the port transition to the unauthorized state.
  - When the NAS is restarted, all users served by the NAS transitions to the unauthorized state.
  - If a client does not support IEEE 802.1X and is connected to a controlled port, the client cannot respond to requests from the NAS and cannot complete authentication. The client is always in the unauthorized state and cannot access network resources.
  - If a client supports IEEE 802.1X but the NAS does not, the NAS does not respond to the EAPOL-Start frame from the client. If the client still receives no response after sending a certain number of EAPOL-Start frames, the client considers the access port as an uncontrolled port and accesses network resources directly.

- Deploying an authentication server

  Orion_B26Q IEEE 802.1X module is compatible with RADIUS servers. RADIUS servers can be used for environment deployment, such as Orion_B26Q SAM/SMP, Microsoft IAS/NPS, and Cisco ACS and Free RADIUS Server. For deployment steps, see the server operation manual.

- Configuring authentication parameters

  To make IEEE 802.1X on an NAS take effect, complete the following configuration:

  kConfigure RADIUS server parameters to ensure the network between the NAS and the RADIUS server is reachable.

lEnsure that the server timeout duration of IEEE 802.1X is greater than that of RADIUS.

mConfigure and apply an AAA method list.

nEnable IEEE 802.1X authentication on the access port.

- Supplicant

  A supplicant refers to IEEE 802.1X-compliant client software installed on a terminal. A user can start the Supplicant software on a terminal and enter the account to initiate authentication.

  If a terminal uses the client embedded in the OS, when the network is available, the terminal automatically displays a dialog box, asking you to enter the account and password for authentication. The implementation and UI operation methods of different client software may be different. You are advised to use Orion_B26Q Supplicant software as the authentication client. If you use other software, see relevant software instructions.

- Going offline

  When stopping accessing network resources, a user can go offline by shutting down the client, disconnecting the network, or logging out of Supplicant.

3. Authorization

Authorization refers to binding specified services to authenticated users, for example, binding an IP address, VLAN, access control list (ACL), quality of service (QoS), available Internet access time range, and available bandwidth. A user is identified by MAC address and VLAN ID (VID). Authorization is actually to add permission information on the basis of MAC address and VLAN ID, such as bound IP address and accessible VLANs.

- IP authorization

  The IEEE 802.1X authentication standard cannot identify IP information. Orion_B26Q IEEE 802.1X module extends the application of IEEE 802.1X and supports MAC+IP binding, which is called IP authorization.

  IP authorization supports four modes:

  - Supplicant authorization: An IP address is provided by Supplicant and this authorization mode needs to be used in combination with Orion_B26Q Supplicant.
  - RADIUS authorization: An IP address is delivered by a RADIUS server to the device after the authentication succeeds.
  - Dynamic Host Configuration Protocol (DHCP) authorization: An authenticated client initiates a DHCP request. After obtaining an IP address, the device binds the IP address with the client's MAC address. DHCP authorization applies to a dynamic IP address environment.
  - Mixed authorization: Authenticated clients select an IP authorization mode based on the sequence of Supplicant authorization, RADIUS authorization, and DHCP authorization, and then the device completes MAC+IP binding. That is, the IP address provided by Supplicant is preferentially used, followed by the IP address assigned by a RADIUS server. The IP address assigned by DHCP is used only when neither of the preceding two IP addresses exists.

- ACL authorization

  ACL authorization means that a server delivers specific ACL services to authenticated users.

  ACL authorization is delivered based on RADIUS attributes and supports standard attributes, Orion_B26Q private attributes, and Cisco private attributes. For details, see the RADIUS server manual.

- Kicking users offline

  Kicking users offline is to force users to go offline. When Orion_B26Q IEEE 802.1X module is used together with Orion_B26Q SAM/SMP, servers can kick online users offline. Then, the users cannot access the network. This function applies to scenarios, in which the Internet access time range needs to be controlled and Internet access charges need to be checked in real time.

4. Accounting

The accounting function is used to audit Internet access behaviors and charges of access users (including auditing the online duration and traffic).

To make the accounting function take effect, configure the accounting function on the device and ensure that the RADIUS server supports the accounting audit function defined in RFC2869.

When a user goes online, the device sends an accounting start packet to the server and the server starts accounting. When the user goes offline, the device sends an accounting end packet to the server, and the server completes an audit and generates an Internet access fee audit list.

Notice

The implementation of the accounting function may vary with servers and not all servers support the accounting function. Therefore, refer to the server usage instructions during actual deployment.

- Accounting start

  After a user passes authentication, the device sends an accounting start packet to the server. After receiving the packet, the server starts the accounting for the user.

  The accounting start packet carries accounting attributes of the user, such as the username and accounting ID.

- Accounting update

  The device periodically sends accounting update packets to the server, making the accounting on the server more real-time.

  The interval for sending accounting update packets can be configured on the device or delivered by the server.

- Accounting end

  After a user logs out, the device sends an accounting end packet to the server. The accounting end packet carries the online duration and traffic of the user. The server generates Internet access records based on the information.

1.1.3 Protocols and Standards

- IEEE802.1X: Port-Based Network Access Control
- RFC2869: RADIUS Extensions

1.2 Configuration Task Summary

IEEE 802.1X configuration includes the following tasks:

(1)Configuring IEEE 802.1X Basic Features

(2)(Optional) Configuring IEEE 802.1X Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Re-authentication
- Configuring Packet Retransmission Parameters
- Configuring the Server Timeout Duration
- Configuring the Quiet Period After an Authentication Failure
- Configuring the Authentication Mode
- Configuring Orion Client Detection

(3)(Optional) Configuring Authorization

(4)(Optional) Configuring MAB. Select any of the following configuration tasks to configure.

- Configuring Single-User MAB
- Configuring Multi-User MAB

(5)(Optional) Configuring MAB Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Username Format for MAB
- Configuring the Username Uppercase/Lowercase for MAB
- Configuring MAB VLAN
- Configuring the MAB Timeout Duration

(6)(Optional) Configuring IAB

(7)(Optional) Configuring the Port Control Mode

(8)(Optional) Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports

(9)(Optional) Configuring the Guest VLAN Function

(10)(Optional) Configuring the Failed VLAN Function

(11)(Optional) Configuring Extended Features. All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Active Authentication
- Configuring a List of Hosts Allowed for Authentication
- Disabling the Virtual Source MAC Address Function
- Configuring Multi-Account Authentication with One MAC Address
- Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface
- Configuring the Function of Initiating Accounting After an IP Address Is Obtained
- Configuring the Priority Order of IEEE 802.1X and MAB
- Configuring the Accounting Update Period
- Configuring Compatibility with H3C Clients and Servers
- Disabling the Global IEEE 802.1X Features

1.3 Configuring IEEE 802.1X Basic Features

1.3.1 Overview

This section describes how to enable 802.1X features to provide basic authentication and accounting services.

1.3.2 Restrictions and Guidelines

- In interface configuration mode, you can enable/disable IEEE 802.1X authentication on the interface.
- Configure RADIUS parameters accurately to ensure that the basic RADIUS communication is proper. Configure an IP address and a protocol communication port for the authentication server as well as the encrypted key used for the communication between the NAS and the RADIUS server.
- The IEEE 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, an error may occur in authentication and accounting.
- IEEE 802.1X uses default method lists by default. To use other method lists, run the **dot1x authentication** and **dot1x accounting** commands to apply the method lists to be used by IEEE 802.1X.
- You can run the **aaa accounting update** command in global configuration mode to enable the accounting update function. The accounting update interval can be configured using the **aaa accounting update periodic** command or delivered by the server. If delivered by the server, the parameter configuration delivered by the server is used preferentially. If the server does not deliver the parameter configuration, the local configuration is used. For details about the accounting update function, see "Configuring AAA" in the *Security Configuration Guide*.
- If IEEE 802.1X is enabled on a port and the number of authenticated users exceeds the maximum number of users supported by port security, port security cannot be enabled. For details about port security, see "Configuring Port Security" in the *Security Configuration Guide*.
- When both port security and IEEE 802.1X are enabled, if the address of port security ages, IEEE 802.1X-authenticated users must be re-authenticated before making further communication.
- Users using static IP addresses or complying with IP+MAC binding can access the network without authentication.
- When Orion_B26Q SAM/SMP software is used together, the accounting function must be configured. Otherwise, the server cannot perceive users going offline.

1.3.3 Prerequisites

Complete required configuration (such as account configuration) on the authentication server to ensure smooth authentication. For details, see the authentication server user manual.

1.3.4 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4)Create an IEEE 802.1X authentication method list and an accounting method list.

aCreate an IEEE 802.1X authentication method list.

aaa authentication dot1x { **default** | *list-name* } { *method* }&<1-4>

No IEEE 802.1X authentication method list is configured by default.

bCreate an IEEE 802.1X accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { *method* }&<1-4>

No IEEE 802.1X accounting method list is configured by default.

(5)(Optional) Configure RADIUS server parameters.

This step is mandatory if the authentication and accounting methods use a RADIUS server.

aConfigure a RADIUS 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 server is configured by default.

bConfigure a shared key for the communication between the device and the RADIUS server.

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

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

(6)Apply the IEEE 802.1X authentication method list and accounting method list.

aApply the IEEE 802.1X authentication method list.

dot1x authentication { **default** | *list-name* }

bApply the IEEE 802.1X accounting method list.

dot1x accounting { **default |** *list-name* }

(7)Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the batch interface configuration mode.

  interface range *interface-type slot-number/interface-number*

(8)Enable IEEE 802.1X authentication.

dot1x port-control auto

1.4 Configuring IEEE 802.1X Parameters

1.4.1 Overview

After IEEE 802.1X basic features are configured, you may need to adjust protocol parameter configuration based on the actual deployment and network status.

1.4.2 Configuration Tasks

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

- Configuring Re-authentication
- Configuring Packet Retransmission Parameters
- Configuring the Server Timeout Duration
- Configuring the Quiet Period After an Authentication Failure
- Configuring the Authentication Mode
- Configuring Orion Client Detection

1.4.3 Configuring Re-authentication

1. Overview

Re-authentication refers that a device periodically requests users to perform re-authentication.

Re-authentication prevents authenticated users from being pretended by other users, and detects whether they are offline, making the accounting more accurate.

2. Restrictions and Guidelines

- After re-authentication is enabled, the device can periodically re-authenticate online users. Re-authentication brings great burden to the server. You are advised to disable this function in the existence of considerable users.
- The re-authentication function can be enabled/disabled, and the re-authentication interval can be configured. In duration-based accounting scenarios, determine the re-authentication interval based on the network scale to ensure reasonable interval and accurate accounting.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable re-authentication.

dot1x re-authentication

The re-authentication function is disabled by default.

(4)(Optional) Configure the re-authentication interval.

dot1x timeout re-authperiod *interval*

The default re-authentication interval is **3600** seconds.

1.4.4 Configuring Packet Retransmission Parameters

1. Overview

A supplicant and an authenticator exchange packets during authentication. Packets need to be retransmitted due to abnormal causes such as timeout. You can configure the retransmission count, retransmission interval, and other parameters based on the actual network conditions.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure packet retransmission parameters. Configure at least one of the tasks.

- Configure the retransmission interval of Request/Identity packets.

  dot1x timeout tx-period *interval*

  The default retransmission interval of Request/Identity packets is **3** seconds.

- Configure the maximum retransmission count of Request/Identity packets.

  dot1x reauth-max *reauth-max-number*

  The default maximum retransmission count of Request/Identity packets is **3**.

- Configure the retransmission interval of Request/Challenge packets.

  dot1x timeout supp-timeout *interval*

  The default retransmission interval of Request/Challenge packets is **3** seconds.

- Configure the maximum retransmission count of Request/Challenge packets.

  dot1x max-req *max-req-number*

  The default maximum retransmission count of Request/Challenge packets is **3**.

1.4.5 Configuring the Server Timeout Duration

1. Overview

This section describes how to configure the server timeout duration of the IEEE 802.1X protocol.

2. Restrictions and Guidelines

- Both the IEEE 802.1X and RADIUS protocols have their own server timeout parameters. Ensure that the server timeout duration of IEEE 802.1X is greater than that of RADIUS. For details about the server timeout parameter of RADIUS, see "Configuring RADIUS" in the *Security Configuration Guide*.
- In an environment with poor server performance, you are advised to set the server timeout duration to a larger value.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the server timeout duration.

dot1x timeout server-timeout *server-timeout*

The default server timeout duration is **5** seconds.

1.4.6 Configuring the Quiet Period After an Authentication Failure

1. Overview

After the quiet period after an authentication failure is configured, a user who fails the authentication needs to wait for a period of time before initiating another authentication. The purpose is to prevent malicious users from conducting frequent authentication to crack passwords in a brute force manner or launch denial of service (DoS) attacks.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the quiet period after an authentication failure.

dot1x timeout quiet-period *quiet-period*

The default quiet period after an authentication failure is **10** seconds.

1.4.7 Configuring the Authentication Mode

1. Overview

Authentication servers and authentication clients may support different authentication modes. You need to select an appropriate authentication mode based on the authentication modes supported by authentication servers and clients. Currently, CHAP, EAP, and PAP authentication modes are supported.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the authentication mode.

dot1x auth-mode { **chap** | **eap** | **pap** }

The default authentication mode is EAP.

1.4.8 Configuring Orion Client Detection

1. Overview

This section describes how to configure Orion_B26Q client detection to detect whether clients are online.

2. Restrictions and Guidelines

Orion_B26Q client detection applies only to Orion_B26Q clients. You are advised to enable this function when Orion_B26Q clients are used.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable online Orion_B26Q client detection.

dot1x client-probe enable

Online Orion_B26Q client detection is disabled by default.

(4)(Optional) Configure Orion_B26Q client detection parameters. Configure at least one of the tasks.

- Configure the Orion_B26Q client detection interval.

  dot1x probe-timer interval *interval*

  The default client detection interval is **20** seconds.

- Configure the Orion_B26Q client detection duration.

  dot1x probe-timer alive *alive-time*

  The default Orion_B26Q client detection duration is **250** seconds.

1.5 Configuring Authorization

1.5.1 Overview

- IP authorization

  IP authorization aims to restrict authenticated users to using specified IP addresses to access the network, and prevent IP address embezzlement.

- Non-Orion_B26Q client filtering

  This function aims to restrict clients to using Orion_B26Q Supplicant for authentication, so as to obtain the anti-proxy, SMS, and other functions provided by Orion_B26Q Supplicant.

- 2nd-generation Orion_B26Q Supplicant deployment

  2nd-generation Orion_B26Q Supplicant deployment means that a user downloads Orion_B26Q Supplicant through the Web page and then initiates authentication by using Orion_B26Q Supplicant. 2nd-generation Orion_B26Q Supplicant deployment facilitates fast deployment of Orion_B26Q Supplicant in an environment with massive users.

1.5.2 Restrictions and Guidelines

- If the function of kicking users offline in real time provided by Orion_B26Q SAM/SMP software needs to be used, configure Simple Network Management Protocol (SNMP) parameters correctly. For the SNMP parameter configuration, see "Configuring SNMP" in the *Network Management and Monitoring Configuration Guide*.

- When multiple types of authentication client software are used in the network, disable the non-Orion_B26Q client filtering function.

- Changing the IP authorization mode will force authenticated users offline and they need to be re-

authenticated before going online again.

- In mixed authorization mode, if an IP authorization mode with a higher priority takes effect during user authentication, the IP authorization mode with a higher priority is used. If RADIUS authorization is used originally but Supplicant provides an IP address during re-authentication, this address is used for authorization.
- 2nd-generation Orion_B26Q Supplicant deployment and Web authentication are mutually exclusive.
- Redirection parameters need to be configured for 2nd-generation Orion_B26Q Supplicant deployment. For details about redirection parameters, see "Configuring Web Authentication" in the *Security Configuration Guide*.

1.5.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the global IP authorization mode.

aaa authorization ip-auth-mode { **disable** | **supplicant** | **radius-server** | **dhcp-server** | **mixed** }

Global IP authorization is disabled by default.

(4)(Optional) Enable 2nd-generation Orion_B26Q Supplicant deployment function.

dot1x redirect

The 2nd-generation Orion_B26Q Supplicant deployment function is disabled by default.

After 2nd-generation Orion_B26Q Supplicant deployment is configured, users who are connected to controlled ports and have no IEEE 802.1X client installed can download the IEEE 802.1X client through the Web page.

(5)(Optional) Enable the non-Orion_B26Q client filtering function.

dot1x private-supplicant-only

The non-Orion_B26Q client filtering function is disabled by default.

1.6 Configuring MAB

1.6.1 Overview

In actual environments, the IEEE 802.1X client cannot be installed on some dumb terminals (such as network printers). They cannot complete IEEE 802.1X authentication but their security needs to be controlled. In this case, you can configure the MAC authentication bypass (MAB) to complete the authentication of these dumb terminals.

MAB is an authentication method that uses MAC addresses of terminals as the usernames and passwords for authentication without installing the client. MAB is mainly used to provide network access control for some dumb terminals.

1.6.2 Restrictions and Guidelines

- The IEEE 802.1X function must be enabled on a controlled port before MAB is configured.
- A MAB-enabled port sends an authentication request packet at an interval specified by **tx-period**. If the request packet is sent for a certain number of times specified by **reauth-max** but no response is received from the client, the port enters the MAB mode. Ports in MAB mode can learn MAC addresses and use them as accounts for authentication.
- When configuring MAC accounts that are used as usernames and passwords on the authentication server, be sure to use the format without separators. For example, assume that the MAC address of a terminal is 00-d0-f8-00-01-02. The account added on the authentication server should be 00d0f8000102.
- IEEE 802.1X has a higher priority than MAB. If a MAB-authenticated terminal needs to go through IEEE 802.1X authentication, the device will clear MAB authentication information of the terminal.
- MAB supports only the PAP authentication mode. Ensure that MAB parameter configurations on the device are consistent with those on the authentication server.
- MAB checks whether terminals can complete IEEE 802.1X authentication by using active authentication. Therefore, enable active authentication when deploying MAB.

1.6.3 Configuration Tasks

Configure MAB. Select any of the following configuration tasks to configure.

- Configuring Single-User MAB
- Configuring Multi-User MAB

1.6.4 Configuring Single-User MAB

1. Overview

Single-user MAB applies to the scenario, in which a port has only one dumb terminal attached to it or a port has only one dumb terminal to be authenticated. After successful authentication, other terminals connected to the port can access the network.

2. Restrictions and Guidelines

As long as the MAC address of one terminal connected to a port passes MAB authentication, all terminals connected to the port are allowed to access the network. However, in some security applications, the administrator requires that only one MAC address exist under a single-user MAB port. In this case, you can configure MAB violation on this port. After MAB violation is configured on a port and the port enters the MAB mode, if more than one MAC address is found under the port, violation occurs on the port.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Enable single-user MAB.

dot1x mac-auth-bypass

Single-user MAB is disabled by default.

(5)(Optional) Enable MAB violation.

dot1x mac-auth-bypass violation

MAB violation is disabled by default.

1.6.5 Configuring Multi-User MAB

1. Overview

Multi-user MAB applies when multiple dumb terminals are connected to one port.

2. Restrictions and Guidelines

- Multi-user MAB can be used together with IEEE 802.1X authentication in mixed access scenarios such as the PC+VoIP daisy-chain topology.
- After multi-user MAB is enabled, illegitimate users connected to an interface may attack the device. Therefore, it is necessary to prevent illegitimate users from frequently initiating authentication, in an effort to reduce the server load. Configure the quiet period after a multi-user MAB failure in global configuration mode. After configuration, if a user fails the authentication, the user can re-initiate authentication only after the quiet period elapses. Configure this quiet period based on the network environment.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Enable multi-user MAB.

dot1x mac-auth-bypass multi-user

Multi-user MAB is disabled by default.

(5)(Optional) Configure the quiet period after a multi-user MAB failure.

dot1x multi-mab quiet-period *quiet-period*

The default quiet period after a multi-user MAB failure is **30** seconds.

You can use this command to restrict the authentication frequency of dumb terminals connected to a port.

(6)(Optional) Configure the number of authentication failures required for user entry aging.

dot1x multi-mab quiet-user fail-times [*fail-times*]

The default number of authentication failures required for user entry aging is **60**.

(7)(Optional) Configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.

dot1x multi-mab quiet-user authen-num [*authen-num*]

The default rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry is **50** MAC addresses per second.

(8)(Optional) Configure the server rejection count for the device to delete a user entry.

dot1x multi-mab quiet-user reject-times [*reject-times*]

The default server rejection count for the device to delete a user entry is **1**.

1.7 Configuring MAB Parameters

1.7.1 Overview

This section describes how to configure MAB parameters to meet requirements of the authentication server for MAB.

1.7.2 Configuration Tasks

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

- Configuring the Username Format for MAB
- Configuring the Username Uppercase/Lowercase for MAB
- Configuring MAB VLAN
- Configuring the MAB Timeout Duration

1.7.3 Configuring the Username Format for MAB

1. Restrictions and Guidelines

The following four username formats are supported:

- **with-colon**: Indicates that the username format is xx:xx:xx:xx:xx:xx.
- **with-dot**: Indicates that the username format is xxxx.xxxx.xxxx.
- **with-hyphen**: Indicates that the username format is xx-xx-xx-xx-xx-xx.
- **with-3hyphen**: Indicates that the username format is xxxx-xxxx-xxxx.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the username format for MAB.

dot1x mab-username format [**with-colon** | **with-dot** | **with-hyphen** | **with-3hyphen**]

No username format for MAB is configured by default.

1.7.4 Configuring the Username Uppercase/Lowercase for MAB

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)(Optional) Configure usernames used for MAB to use uppercase letters.

dot1x mab-username upper

Usernames used for MAB use lowercase letters by default.

This command is used to meet requirements of different servers for username uppercase/lowercase in MAB.

1.7.5 Configuring MAB VLAN

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure MAB VLAN.

dot1x mac-auth-bypass vlan *vlan-id*

The MAB VLAN function is disabled by default.

If MAB is needed for users only in some VLANs of an interface, you can configure the VLANs as MAB VLANs. Users not in the MAB VLANs cannot perform MAB.

1.7.6 Configuring the MAB Timeout Duration

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure the MAB timeout duration.

dot1x mac-auth-bypass timeout-activity *timeout*

MAB does not time out by default.

You can configure this parameter to restrict the network access duration of dumb terminals.

1.8 Configuring IAB

1.8.1 Overview

Inaccessible authentication bypass (IAB) is a method provided for new to-be-authenticated users to access the network when all RADIUS servers configured on the device are all unreachable. After a RADIUS server becomes reachable, it verifies the identities of users authorized in the unavailability period of RADIUS servers.

When RADIUS servers connected to a port are inaccessible and cannot authenticate the identities of users for the time being, you can add the port to a specified VLAN so that users connected to the port can access network resources only in the specified VLAN. This VLAN is called an IAB VLAN.

1.8.2 Restrictions and Guidelines

- IAB takes effect only when the global IEEE 802.1X authentication method list contains only the RADIUS authentication method and all RADIUS servers in the method list fail. If the method list has other authentication methods (such as local and none), IAB does not take effect.
- Configure an account for testing whether a RADIUS server is reachable and the criteria for judging that a RADIUS server is unreachable. For details about the criteria for judging that a RADIUS server is unreachable, see "Configuring RADIUS" in the *Security Configuration Guide*. After global multi-domain AAA is enabled, the global method list is not used during IEEE 802.1X authentication. When IAB configured on a port detects that all RADIUS servers configured in the global 802.1X authentication method list are inaccessible, it directly returns an authentication success message to users, who can access network resources with no need to enter usernames. In this case, multi-domain AAA does not take effect on this port.
- Users authenticated in IAB mode do not initiate accounting requests to the accounting server.
- Authenticated users can properly access the network and are not affected by server inaccessibility.
- In access authentication configuration mode, when 802.1X-based IP authentication is enabled globally, if a user connected to a port is authenticated, IAB cannot be performed on other users connected to the port. In gateway authentication mode, IP authorization can be performed only when IP addresses of authenticated users can be obtained.
- Complete IEEE 802.1X authentication is required on some IEEE 802.1X authentication clients (such as Windows IEEE 802.1X authentication clients) so that ports connected to the clients are considered authenticated. When IAB is performed on such clients, users actually have been authorized via IAB but an authentication failure may be displayed on the clients.
- If an IAB VLAN does not exist, it is dynamically created when a port is added to the IAB VLAN, and automatically deleted when the port is removed from the IAB VLAN.
- An IAB VLAN cannot be a private VLAN, remote VLAN, or super VLAN (including sub VLANs).

1.8.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Enable IAB.

dot1x critical

IAB is disabled by default.

(5)(Optional) Enable IAB recovery.

dot1x critical recovery action reinitialize

IAB recovery is disabled by default.

After this function is enabled on a port, when a server becomes reachable, users who are connected to the port and normally authenticated can access the network without re-authentication. For those who are IAB-authenticated during server unavailability, the device initiates active authentication.

(6)(Optional) Configure the IAB VLAN function.

dot1x critical vlan *vlan-id*

The IAB VLAN function is disabled by default.

1.9 Configuring the Port Control Mode

1.9.1 Overview

IEEE 802.1X control is classified into MAC-based control and port-based control. The control granularity of the two control modes is different. Configure the control mode as required.

In MAC-based control mode, each client connected to a port must pass authentication before accessing network resources. In port-based control mode, all clients connected to a port can access network resources as long as one of them is authenticated. The MAC-based control mode is used by default.

1.9.2 Configuration Tasks

Configure the port control mode. Select any of the following configuration tasks to configure.

- Configuring the MAC-based Control Mode
- Configuring the Port-based Control Mode

1.9.3 Configuring the MAC-based Control Mode

1. Overview

In MAC-based control mode, the MAC address of each client is used as an authentication unit. Clients with different MAC addresses can access network resources only after they pass authentication separately.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure the MAC-based control mode.

dot1x port-control-mode mac-based

A port is controlled based on MAC addresses by default.

1.9.4 Configuring the Port-based Control Mode

1. Overview

In port-based control mode, an entire port is used as an authentication unit. As long as one client connected to a port is authenticated, the port is an authenticated port and all clients connected to the port can access network resources.

To allow only one client connected to a port to pass the authentication, you can configure the port-based single-user mode on the basis of port-based control. In this mode, if other users exist on the port, the device deletes all users connected to the port and initiates re-authentication.

2. Restrictions and Guidelines

- In port-based control mode, inter-port migration can be allowed or prohibited for dynamic users. Dynamic users are allowed to migrate between different ports by default.
- In port-based authentication mode, a controlled port supports only one authenticated user while all the users are dynamic users.
- In port-based single-user control mode, only one user on the controlled port can pass authentication and make communication. The limit on the number of users on the port does not affect the limit on the number of users in this mode.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure the port-based control mode.

dot1x port-control-mode port-based

A port is controlled based on MAC addresses by default.

(5)(Optional) Configure the port-based single-user control mode.

dot1x port-control-mode port-based single-host

The port-based single-user control mode is not configured by default.

After this command is configured, only one dynamic user can make communication.

(6)(Optional) Disable migration of dynamic users.

dot1x stationarity enable

Migration is allowed for dynamic users by default.

Dynamic users on a controlled port cannot migrate to other ports before aging.

1.10 Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports

1.10.1 Overview

Automatic dynamic VLAN redirection on IEEE 802.1X ports is used to enable a server to deliver a redirected VLAN. After this function is enabled, when a server delivers a redirected VLAN, relevant users will be added to the redirected VLAN for communication.

The redirection mechanisms implemented by different types of controlled ports are different:

- If controlled ports to be redirected to a VLAN are access ports, trunk ports, or hybrid ports (with MAC VLAN disabled), you can change the native VLANs of these ports to implement dynamic VLAN redirection.
- If controlled ports to be redirected to a VLAN are hybrid ports (with MAC VLAN enabled), you can dynamically create MAC VLAN entries to add authenticated users to the delivered VLAN.

1.10.2 Restrictions and Guidelines

- The device can deliver a VLAN by extending RADIUS attributes. When a RADIUS server delivers a VLAN to an NAS by using an extended attribute, the server encapsulates the extended attribute into RADIUS standard attribute 26. The extended vendor ID is a hexadecimal number 0x00001311. The default type number of the extended attribute is 4. You can run the **radius attribute 4 vendor-type type** command on the device to receive a delivered VLAN whose extended attribute type is **type**.
- The device allows a RADIUS server to deliver VLANs by using RADIUS standard attributes, including a combination of the following attributes:
  - Attribute 64 (**Tunnel-Type**): The value is VLAN (13).
  - Attribute 65 (**Tunnel-Medium-Type**): The value is 802 (6).
  - Attribute 81 (**Tunnel-Private-Group-ID**): The value is a VLAN ID or VLAN name.
- The device can perform IEEE 802.1X authentication on access, trunk, and hybrid ports. If automatic dynamic VLAN redirection is enabled on other ports, authentication will fail.
- The delivered VLAN attribute is used as a VLAN name. The NAS checks whether a VLAN with the same name is configured. If yes, the NAS automatically adds the user port, to which the VLAN attribute is delivered, to the VLAN. If no VLAN with the same name exists, the delivered VLAN attribute is used as a VLAN ID. If the VLAN ID is valid (within the VLAN ID range supported by the system), the device automatically adds the user port to the VLAN. If the VLAN ID is 0, the device considers no VLAN information delivered. The authentication will fail in other cases.
- Delivered redirected VLANs cannot be private VLANs, remote VLANs, or super VLANs (including sub VLANs).
- When VLAN redirection is configured on an access port and a delivered VLAN does not exist on the device, if the delivered VLAN is identified as a VLAN ID, the device creates the VLAN and adds the port, to which the VLAN attribute is delivered, to the new VLAN, and user authentication succeeds. If the delivered

VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the access port on the device, users connected to the port will fail the authentication. If the delivered VLAN is configured as a redirected VLAN supported by the access port on the device, the port is removed from its VLAN and added to the delivered VLAN and user authentication succeeds.

- When VLAN redirection is configured on a trunk port and a delivered VLAN does not exist on the device, if the delivered VLAN is identified as a VLAN ID, the device creates the VLAN and changes the native VLAN of the port to the delivered VLAN, and user authentication succeeds. If the delivered VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the trunk port (see the description below), the authentication fails. If the delivered VLAN is configured as a redirected VLAN supported by the trunk port on the device, the device changes the native VLAN of the port to the delivered VLAN and user authentication succeeds.
- If the MAC VLAN function is disabled on a hybrid port, a delivered VLAN is processed as follows: If the delivered VLAN does not exist on the device and is identified as a VLAN ID, the device automatically creates the VLAN, allows the VLAN to pass through the current hybrid port in an untagged manner, and changes the native VLAN of the port to the delivered VLAN, and user authentication succeeds. If the delivered VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the hybrid port (or the VLAN is contained in the tagged VLAN list of the hybrid port), user authentication fails. Otherwise, the delivered VLAN is allowed to pass through the hybrid port in an untagged manner, the native VLAN of the port is changed to the delivered VLAN, user authentication succeeds.
- If the MAC VLAN function is enabled on a hybrid port, a delivered VLAN is processed as follows: User authentication fails if the VLAN delivered by the authentication server does not exist on the device (the VLAN must be statically configured according to requirements of the MAC VLAN function), the delivered VLAN has been added to the tagged VLAN list of the hybrid port, or the MAC VLAN function does not support the type of the VLAN (for details, see "Configuring MAC VLAN" in the *Ethernet Switching Configuration Guide*). Otherwise, the device dynamically creates MAC VLAN entries based on the delivered VLAN and user MAC addresses, and user authentication succeeds. When a user goes offline, the MAC VLAN entry of the user will be dynamically deleted.
- If the MAC VLAN function is disabled on a port, after a VLAN is delivered, the device changes the native VLAN of the port but will not change the native VLAN command configuration of the port. The priority of a delivered VLAN is higher than that of a VLAN configured by a command. That is, after successful authentication, the delivered VLAN takes effect, and the native VLAN configured by a command functions after a user goes offline.
- If MAC VLAN is enabled on a port and user authentication is based on MAC addresses, VLANs are delivered through the dynamic creation of MAC VLAN entries, and the native VLAN of the port is not changed.
- No matter whether MAC VLAN is enabled on a hybrid port, if the VLAN delivered via authorization is added to the tagged VLAN list of the port, the VLAN delivery fails.

1.10.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Enable automatic dynamic VLAN redirection on the interface.

dot1x dynamic-vlan enable

Dynamic VLAN redirection is disabled on a port by default.

1.11 Configuring the Guest VLAN Function

1.11.1 Overview

The guest VLAN function is used to provide network access permissions for terminals, on which the IEEE 802.1X client is not installed.

After the guest VLAN function is configured, if no IEEE 802.1X client is detected on a controlled port, the port is added to the guest VLAN to allow terminals connected to the port to access network resources in the guest VLAN.

1.11.2 Restrictions and Guidelines

- If a port added to a guest VLAN receives an EAPOL packet, the port is considered to have an IEEE 802.1X-authenticated client attached to it. In this case, the port exits the guest VLAN and performs IEEE 802.1X authentication.
- If any of the following conditions is met, a controlled port is considered to have no IEEE 802.1X-authenticated client attached to it:
  - The port sends an active authentication packet three times consecutively, but receives no EAPOL response packet.
  - The port receives no EAPOL response packet within 90 seconds.
  - The MAC address authentication fails in MAB mode.
- Automatic dynamic VLAN redirection must be enabled on IEEE 802.1X ports.
- When a port switches from Linkup state to Linkdown state, it exits the guest VLAN. When it switches from Linkdown state to Linkup state, the device judges whether the port needs to be added to the guest VLAN.
- After a port fails to receive EAPOL packets within 90s and redirects to a guest VLAN, clients connected to the port need to wait for a long period of time before re-initiating DHCP requests because of the time increment mechanism in the transmission of DHCP discover packets. As a result, it takes a long time for clients to obtain IP addresses after the port redirects to the guest VLAN.
- To configure guest VLAN on a hybrid port, add the VLAN to the untagged VLAN list of the port and then configure the VLAN as a guest VLAN.

1.11.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure the guest VLAN function on the controlled port.

dot1x guest-vlan *vlan-id*

The guest VLAN function is disabled on a controlled port by default.

(Optional) After the guest VLAN function is enabled on a controlled port, the device judges whether the port has an IEEE 802.1X authentication client attached to it. If no, the device adds the port to the guest VLAN.

1.12 Configuring the Failed VLAN Function

1.12.1 Overview

The failed VLAN function is used to provide network access permissions for clients that fail the authentication.

After the failed VLAN function is configured on a port, when the authentication failure count of a client connected to the port reaches the specified number, the port is added to the failed VLAN to allow the client to access network resources in the failed VLAN.

1.12.2 Restrictions and Guidelines

- You can configure the maximum number of consecutive failed authentication attempts for clients. If the authentication failure count of a client reaches this number, the device adds the port connected to the client to a failed VLAN.
- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port is added to the failed VLAN and automatically removed when the port exits the failed VLAN.
- Automatic dynamic VLAN redirection must be enabled on IEEE 802.1X ports.
- When a port switches to Linkdown state, the port automatically exits the failed VLAN.
- The failed VLAN and guest VLAN can be set to the same VLAN.
- In port-based control mode, after a controlled port is added to a failed VLAN, only the users who fail the authentication can re-initiate authentication and other users' authentication requests will be discarded. This restriction does not apply to the MAC-based control mode.
- Private VLANs cannot be configured as 802.1X failed VLANs.

1.12.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure failed VLAN.

dot1x auth-fail vlan *vlan-id*

The failed VLAN function is disabled by default.

(5)(Optional) Configure the maximum number of consecutive failed authentication attempts.

dot1x auth-fail max-attempt *max-attemp-number*

The default maximum number of consecutive failed authentication attempts is **3**.

This command is used to configure the maximum number of times that a user is consecutively rejected by the authentication server. If the rejection count reaches this number, the port, to which the user is connected, will be added to a failed VLAN.

1.13 Configuring Extended Features

1.13.1 Overview

This section describes how to configure some extended features supported by Orion_B26Q devices.

1.13.2 Configuration Tasks

Configure extended features. All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Active Authentication
- Configuring a List of Hosts Allowed for Authentication
- Disabling the Virtual Source MAC Address Function
- Configuring Multi-Account Authentication with One MAC Address
- Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface
- Configuring the Function of Initiating Accounting After an IP Address Is Obtained
- Configuring the Priority Order of IEEE 802.1X and MAB
- Configuring the Accounting Update Period
- Configuring Compatibility with H3C Clients and Servers
- Disabling the Global IEEE 802.1X Features

1.13.3 Enabling Active Authentication

1. Overview

Active authentication refers that the NAS actively sends a Request/Identity packet, which triggers IEEE 802.1X clients to initiate IEEE 802.1X authentication.

2. Restrictions and Guidelines

- Some clients use authentication clients embedded in the OS. They may not initiate authentication immediately after connecting to the network, and users cannot use the network promptly. The configured active authentication can urge such clients to initiate authentication in a timely manner after they connect to the network.
- You can use this function to detect whether a client is using Supplicant.
- This function must be configured for MAB deployment.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable active authentication.

dot1x auto-req

The active authentication function is enabled by default.

(4)(Optional) Configure the maximum number of active authentication request packets that can be sent.

dot1x auto-req packet-num *packet-number*

The device always sends authentication request packets actively by default.

(5)(Optional) Configure the interval for sending active authentication request packets.

dot1x auto-req req-interval *req-interval*

The default interval for the device to send active authentication request packets is **30** seconds.

(6)(Optional) Enable the function of detecting whether a user is being authenticated during active authentication.

dot1x auto-req user-detect

The function of detecting whether a user is being authenticated during active authentication is enabled by default.

1.13.4 Configuring a List of Hosts Allowed for Authentication

1. Overview

You can configure only clients with specific MAC addresses connected to specified ports to perform IEEE 802.1X authentication to improve network security.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure a list of hosts allowed for authentication.

dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

1.13.5 Disabling the Virtual Source MAC Address Function

1. Overview

The virtual source MAC address function enables the device to use a virtual MAC address as the source MAC address of EAP packets in IEEE 802.1X authentication.

This function is used together with Orion_B26Q Supplicant to determine whether an NAS is a Orion_B26Q device. Then, private features can be implemented on Supplicant if the NAS is a Orion_B26Q device. The virtual source MAC address function is enabled by default. You can determine whether to disable the function as required.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3) Disable the virtual source MAC address function.

dot1x pseudo source-mac

The source MAC address of IEEE 802.1X packets sent by the device is a virtual MAC address by default.

1.13.6 Configuring Multi-Account Authentication with One MAC Address

1. Overview

The multi-account function allows a user to switch the account upon re-authentication. In some special scenarios in which an account change is needed, such as Windows domain authentication, an access domain is used and an account may be changed for authentication. This function applies to such scenarios.

2. Restrictions and Guidelines

The multi-account authentication function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable multi-account authentication with one MAC address.

dot1x multi-account enable

Multi-account authentication with one MAC address is disabled by default.

1.13.7 Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the maximum number of users who can be authenticated on an interface.

dot1x default-user-limit *limit-number*

The maximum number of users who can be authenticated on an interface is unlimited.

1.13.8 Configuring the Function of Initiating Accounting After an IP Address Is Obtained

1. Overview

Clients do not initiate accounting immediately after passing authentication, but wait until they obtain IP addresses.

Some servers request accounting request packets to carry IP addresses. This function can meet this requirement. Authenticated users go online and obtain IP addresses from Supplicant or DHCP snooping. IEEE 802.1X initiates accounting requests only after the users obtain IP addresses. The device may not initiate accounting within a long period of time due to a lack of IP addresses of authenticated clients. For this, the function provides an IP address detection timeout duration. If the device does not obtain the IP address of a client within the timeout duration, the device brings the client offline.

2. Restrictions and Guidelines

- In an IPv4 environment where Orion_B26Q Supplicant client is deployed, Supplicant is capable of uploading IPv4 addresses of clients and therefore, the function does not need to be enabled.
- This function is unavailable in static IP address environments.

3. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of initiating accounting after a user's IP address is obtained.

dot1x valid-ip-acct enable

The function of initiating accounting after a user's IP address is obtained is disabled by default.

(4)Configure the timeout duration for an authenticated user to obtain an IP address.

dot1x valid-ip-acct timeout *timeout*

The default timeout duration for an authenticated user to obtain an IP address is **5** minutes.

1.13.9 Configuring the Priority Order of IEEE 802.1X and MAB

1. Overview

IEEE 802.1X authentication has a higher priority than MAB by default. This function allows you to configure the priority order of IEEE 802.1X authentication and MAB.

If both IEEE 802.1X authentication and MAB are enabled, IEEE 802.1X authentication or MAB is carried out, whichever is triggered first, and IEEE 802.1X authentication is prior to MAB. Therefore, if the device receives an EAPOL packet from a MAB-authenticated user, the device brings the user offline and performs IEEE 802.1X

authentication on the user. Currently, the device performs IEEE 802.1X authentication on each user, and then performs MAB on users who fail the authentication. In addition, MAB takes priority over IEEE 802.1X authentication, and IEEE 802.1X authentication is ignored for MAB-authenticated users.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the priority of IEEE 802.1X authentication to be lower than that of MAB.

dot1x auth-with-order

IEEE 802.1X authentication has a higher priority than MAB by default.

1.13.10 Configuring the Accounting Update Period

1. Overview

Some servers do not deliver the accounting update period during user re-authentication, but require that accounting update packets be sent at the accounting update period delivered at the first authentication. In this case, you can use this function to configure the accounting update period delivered by the server at the first authentication as the accounting update period of re-authentication.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Set the accounting update period to that delivered by the server at the first authentication.

dot1x acct-update base-on first-time server

The accounting update period delivered by the server at the first authentication is not configured as the accounting update period for re-authentication by default.

1.13.11 Configuring Compatibility with H3C Clients and Servers

1. Overview

This function enables Orion_B26Q devices to be compatible with H3C 802.1X clients and authentication servers.

When 802.1X authentication is performed by a Orion_B26Q device on an H3C iNode, the username provided by the client for authentication uses a special format unrecognized by Orion_B26Q device, resulting in an authentication failure. Usernames required by H3C authentication servers for MAB are in the format of xx-xx-xx-xx-xx-xx, which is different from the default MAB authentication username format of Orion_B26Q devices. As a result, the authentication fails. You can configure this function to implement correct interworking with H3C devices.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the compatibility with H3C 802.1X authentication clients and authentication servers.

dot1x user-name compatible

The compatibility with H3C 802.1X authentication clients and authentication servers is disabled by default.

1.13.12 Disabling the Global IEEE 802.1X Features

1. Overview

You can disable IEEE 802.1X features on all ports at a time.

After global IEEE 802.1X features are disabled, users can access the network without authentication and online users will be brought offline. After global IEEE 802.1X features are enabled, if IEEE 802.1X authentication is configured on a port, users connected to the port need to be authenticated before accessing the network.

2. Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Disable global IEEE 802.1X features.

dot1x system disable

Global IEEE 802.1X features are enabled by default.

1.14 Monitoring

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

Run the **dot1x** commands to restore global configuration.

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 switch immediately after use.

Table 1-1IEEE 802.1X Monitoring

Command	Purpose
show radius server	Displays the configuration of a RADIUS server.
show dot1x	Displays IEEE 802.1X protocol parameters.

Command	Purpose
show dot1x auth-address-table [**address** *mac-address*] [**interface** *interface-type interface-number*]	Displays the list of hosts allowed for authentication.
show dot1x auto-req	Displays the active authentication status and parameters.
show dot1x port-control [**interface** *interface-type interface-numbe*r]	Displays information about controlled ports.
show dot1x probe-timer	Displays client detection parameters.
show dot1x summary	Displays entries of authenticated users.
show dot1x max-req	Displays the maximum retransmission count of Request/Challenge packets.
show dot1x private-supplicant-only	Displays the status of the non-Orion_B26Q client filtering function.
show dot1x re-authentication	Displays the status of the re-authentication function.
show dot1x reauth-max	Displays the maximum retransmission count of Request/Identity packets.
show dot1x timeout quiet-period	Displays the quiet period after an authentication failure.
show dot1x timeout re-authperiod	Displays the re-authentication interval.
show dot1x timeout server-timeout	Displays the server timeout duration.
show dot1x timeout supp-timeout	Displays the retransmission interval of Request/Challenge packets.
show dot1x timeout tx-period	Displays the retransmission interval of Request/Identity packets.
show dot1x user id *user-id*	Displays details about a user with a specific user ID.
show dot1x user mac *mac-addr*	Displays details about a user with a specific MAC address.
show dot1x user name *user-name*	Displays details about a user with a specific username.
clear dot1x user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *user-name* }	Deletes an IEEE 802.1X-authenticated user.
dot1x default	Restores the default IEEE 802.1X configuration.
debug aaa	Debugs AAA (for details, see "Configuring AAA").
debug radius	Debugs RADIUS (for details, see "Configuring RADIUS").
debug dot1x event	Debugs IEEE 802.1X events.

Command	Purpose
debug dot1x packet	Debugs IEEE 802.1X packet processing.
debug dot1x stm	Debugs the IEEE 802.1X authentication state machine.
debug dot1x com	Debugs IEEE 802.1X internal communication.
debug dot1x error	Debugs IEEE 802.1X errors.

1.15 Configuration Examples

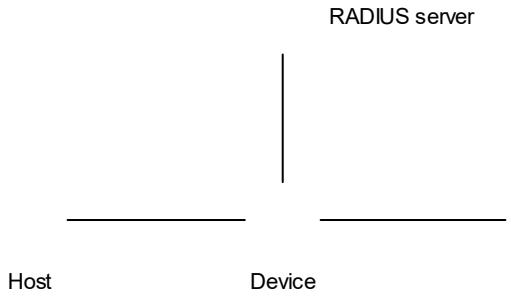
1.15.1 Configuring IEEE 802.1X Authentication

1. Requirements

IEEE 802.1X basic features need to be enabled on a device port so that clients connected to the port can access the network only after passing IEEE 802.1X authentication.

2. Topology

Figure 1-1Topology of IEEE 802.1X Authentication



3. Notes

- Configure a RADIUS server and add IEEE 802.1X users on the RADIUS server.
- Enable AAA services.
- Configure the server address and key.
- Configure the authentication and accounting method lists.
- Apply the authentication and accounting method lists.
- Enable IEEE 802.1X basic features on an interface.

4. Procedure

(1)Configure a RADIUS server and add an IEEE 802.1X user with the username **hostname1** and password **password1** on the RADIUS server. (The configuration is omitted here. For the configuration of the RADIUS server, see the RADIUS server configuration manual.)

(2)Enable AAA services.

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

(3)Configure the address and shared key of the AAA server (a RADIUS server is used as an example here, the IP address is set to 192.168.1.3, and the shared key is set to **radiuskey**).

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

(4)Configure the authentication and accounting method lists.

```
Device(config)# aaa authentication dot1x auth-method group radius
Device(config)# aaa accounting network account-method start-stop group radius
```

(5)Apply the authentication and accounting method lists.

```
Device(config)# dot1x authentication auth-method
Device(config)# dot1x accounting account-method
```

(6)Enable IEEE 802.1X basic features on an interface.

```
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x port-control auto
```

5. Verification

The user cannot access network resources before authentication, but can access network resources after authentication.

Run the **show dot1x summary** command to display information about the authenticated user.

```
Device# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  hostname1    0023.aeaa.4286  Gi0/1     1    Authenticated   Idle
Authed      static    0days 0h 0m 7s
```

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
```

```
!
```

7. Common Errors

- RADIUS parameters are incorrectly configured.
- A server uses a special access policy, for example, RADIUS packets must carry certain attributes.
- The AAA method list is different from the IEEE 802.1X method list, causing an authentication failure.

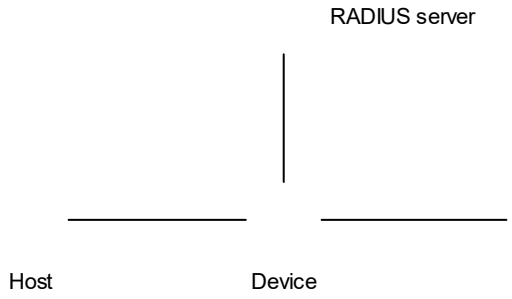
1.15.2 Configuring the IP Authorization Mode

1. Requirements

After IP authorization is configured, only clients with specified IP addresses can pass authentication.

2. Topology

Figure 1-1Topology of IP Authorization Mode



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure the IP authorization mode.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Configure the Supplicant authorization mode.

```
Device> enable
Device# configure terminal
Device(config)# aaa authorization ip-auth-mode supplicant
```

5. Verification

A client using a non-specified IP address fails the authentication.

6. Configuration Files

```
!
aaa authorization ip-auth-mode supplicant
dot1x authentication auth-method
dot1x accounting account-method
```

```
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
!
```

7. Common Errors

- There are multiple authentication clients in the network. After non-Orion_B26Q client filtering is enabled, some clients fail the authentication.
- Orion_B26Q SAM/SMP is used but SNMP parameters are not configured on the device. As a result, the function of kicking users offline fails.

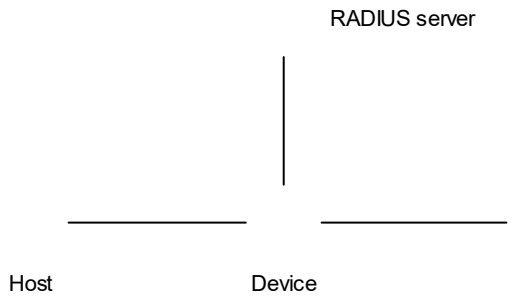
1.15.3 Configuring Multi-user MAB

1. Requirements

Multi-user MAB applies when multiple dumb terminals are connected to one port. After multi-user MAB is configured, each dumb terminal connected to a port needs to be authenticated so that they can access the network.

2. Topology

Figure 1-1Topology of Multi-user MAB



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure multi-user MAB.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Configure multi-user MAB.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass multi-user
```

5. Verification

Connect dumb terminals A and B to a port.

(1)If the MAC account of dumb terminal A is added on the RADIUS server, dumb terminal A can access the network properly but dumb terminal B cannot.

(2)Both dumb terminals A and B can access the network properly only after both their MAC accounts are added on the RADIUS server.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x mac-auth-bypass multi-user
!
```

7. Common Errors

The MAC account format is incorrect on the server.

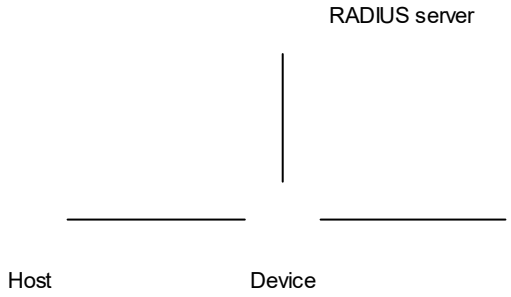
1.15.4 Configuring IAB

1. Requirements

After IAB is configured, when all RADIUS servers configured on the device are unreachable, new access users are allowed to access the network directly.

2. Topology

Figure 1-1 Topology of IAB



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure RADIUS server reachability detection.
- Configure IAB.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Configure the criteria for judging that a RADIUS server is unreachable as follows: The consecutive timeout count is 5 and the timeout duration is 60 seconds.

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 60 tries 5
```

(3)Configure IAB.

```
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x critical
```

5. Verification

When all RADIUS servers are unreachable, a client can directly access the network after initiating IEEE 802.1X authentication. Authentication will not fail due to the unavailability of RADIUS servers.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 test username testname key 7 $10$3b4$ln0s66i8XfEi$
radius-server dead-criteria time 60 tries 5
!
```

```
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x critical
!
```

7. Common Errors

- There is a RADIUS server reachable.
- The IEEE 802.1X authentication method list contains other methods besides the RADIUS method.

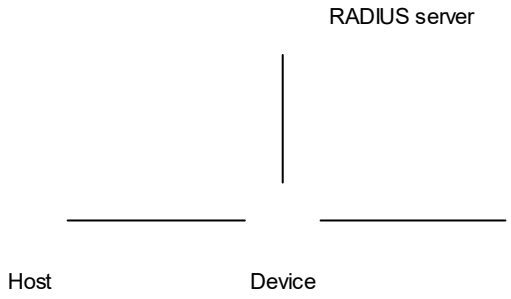
1.15.5 Configuring Automatic Dynamic VLAN Redirection

1. Requirements

After automatic dynamic VLAN redirection is enabled, when the server delivers a redirected VLAN to a port, users connected to the port will be added to the VLAN for communication.

2. Topology

Figure 1-1Topology of Automatic Dynamic VLAN Redirection



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Enable automatic dynamic VLAN redirection on a controlled port.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Enable automatic dynamic VLAN redirection on an interface.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

5. Verification

Configure the RADIUS server to deliver VLAN attributes. Run the **show dot1x summary** command to display information about the authenticated user. The port, to which the user is connected, redirects from VLAN 2 to VLAN 3.

```
Device# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  Hostname1    0023.aeaa.4286  Gi0/1     3    Authenticated   Idle
Authed      static    0days 2h17m29s
```

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x dynamic-vlan enable
!
```

7. Common Errors

- RADIUS attributes of the VLAN to be delivered are not correctly configured on the authentication server.
- The RADIUS command for supporting delivered VLAN attributes is not configured on the device.
- When the MAC VLAN configured on a hybrid port is a redirected VLAN, the delivered VLAN is a tagged VLAN.

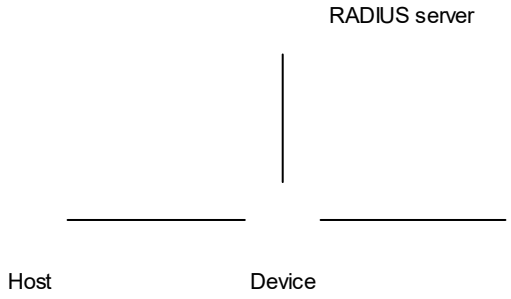
1.15.6 Configuring Guest VLAN

1. Requirements

IEEE 802.1X authentication needs to be enabled on a device port and guest VLAN needs to be configured on the port. If the IEEE 802.1X client is not installed on a terminal connected to the port, the terminal is allowed to access network resources in the guest VLAN.

2. Topology

Figure 1-1 Topology of Guest VLAN



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Enable automatic dynamic VLAN redirection on a controlled port.
- Add the port to a guest VLAN.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Enable automatic dynamic VLAN redirection on the port.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

(3)Add the port to the guest VLAN with the VLAN ID 1.

```
Device(config-if-GigabitEthernet 0/1)# dot1x guest-vlan 1
```

5. Verification

After the port is added to the guest VLAN, the device generates the following log:

```
%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface GigabitEthernet 0/1 from
default-vlan 1 to guest-vlan 1 OK.
```

When the IEEE 802.1X client is not configured on a terminal, the terminal can and can only access network resources in VLAN 1 without authentication.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
```

```
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x dynamic-vlan enable
 dot1x guest-vlan 1
!
```

7. Common Errors

A port receives an EAPOL packet, and as a result, the port cannot be added to a guest VLAN.

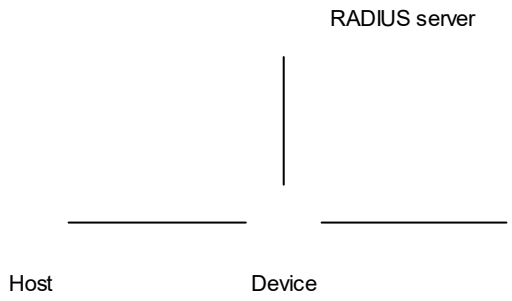
1.15.7 Configuring Failed VLAN

1. Requirements

IEEE 802.1X authentication needs to be enabled on a device port and failed VLAN needs to be configured on the port. If a terminal fails the IEEE 802.1X authentication, it is allowed to access network resources in the failed VLAN.

2. Topology

Figure 1-1 Topology of Failed VLAN



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Add the port to a failed VLAN.

4. Procedure

(1)Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2)Add the port to a failed VLAN with the VLAN ID 1.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x auth-fail vlan 1
```

5. Verification

A terminal cannot access the network before authentication. The terminal uses an incorrect account for authentication. After the authentication fails, the terminal can access network resources in the failed VLAN.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x auth-fail vlan 1
!
```

7. Common Errors

If a user fails the authentication not due to the rejection from the authentication server, for example, the authentication client cannot be installed because of underlying resource insufficiency, the user will not be added to a failed VLAN.