Chapter 31: 802.1X

Contents

Chapter 31 802.1X

31.1 802.1X Overview

IEEE 802.1X is the accessing management protocol standard based on interface accessing control passed in June, 2001. Traditional LAN does not provide accessing authentication. Usersaccess the devices and resources in LAN when connecting to the LAN, which is a security hidden trouble. For application of motional office and CPN, device provider hopes to control and configure user's connecting. There is also the need for accounting.

IEEE 802.1X is a network accessing control technology based on interface which is the accessing devices authentication and control by physical accessing level of LAN devices. Physical accessing level here means the interface of LAN GPON devices. When getting authentication, GPON is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing GPON and verifies the information through authenticationserver. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

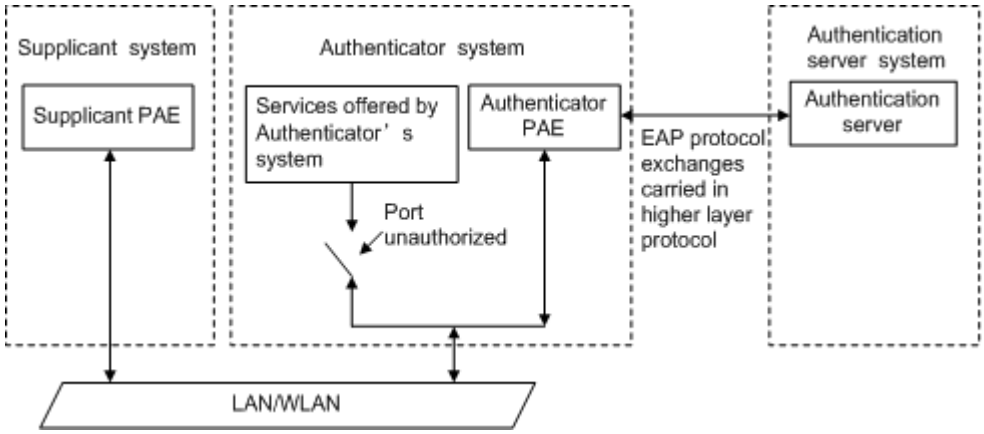
31.1.1 Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: supplicant system, authenticator system, and authentication server system.

Supplicant system: A system at one end of the LAN segment, which is authenticated by the

authenticator system at the other end. A supplicant system is usually a user-end device and initiates 802.1x authentication through 802.1x client software supporting the EAP over LANs (EAPOL) protocol.

Authenticator system: A system at the other end of the LAN segment, which authenticatesthe connected supplicant system. An authenticator system is usually an 802.1x-enablednetwork device and provides ports (physical or logical) for supplicants to access the LAN. **Authentication server system:** The system providing authentication, authorization, andaccounting services for the authenticator system. The authentication server, usually a RemoteAuthentication Dial-in User Service (RADIUS) server, maintains user information likeusername, password, VLAN that the user belongs to, committed access rate (CAR)parameters, priority, and ACLs.



The above systems involve three basic concepts: PAE, controlled port, control direction.

1) PAE

Port access entity (PAE) refers to the entity that performs the 802.1x algorithm and protocol

operations.

The authenticator PAE uses the authentication server to authenticate a supplicant trying to access the LAN and controls the status of the controlled port according to the authentication result, putting the controlled port in the authorized or unauthorized state. In authorized state, the port allows user data to pass, enabling the supplicant(s) to access the network resources; while in unauthorized state, the port denies all data of the supplicant(s).

The supplicant PAE responds to the authentication request of the authenticator PAE and provides authentication information. The supplicant PAE can also send authentication requests and logoff requests to the authenticator.

2) Controlled port and uncontrolled port

An authenticator provides ports for supplicants to access the LAN. Each of the ports can be regarded as two logical ports: a controlled port and an uncontrolled port.

The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol frames to pass, guaranteeing that the supplicant can always send and receiveauthentication frames.

The controlled port is open to allow normal traffic to pass only when it is in the authorized state.The controlled port and uncontrolled port are two parts of the same port. Any frames arriving at the port are visible to both of them.

3) Control direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the supplicant or just the traffic from the supplicant.

31.1.1 Rule of 802.1x

The 802.1x authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the supplicant PAE, authenticator PAE, and authentication server.

At present, the EAP relay mode supports four authentication methods: EAP-MD5, EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol).

1) When a user launches the 802.1x client software and enters the registered username and password, the 802.1x client software generates an EAPOL-Start frame and sends it to the authenticator to initiate an authentication process.

2) Upon receiving the EAPOL-Start frame, the authenticator responds with an EAP-Request/Identity packet for the username of the supplicant.

3) When the supplicant receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the authenticator.

4) Upon receiving the EAP-Response/Identity packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.

5) When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the authenticator.

6) After receiving the RADIUS Access-Challenge packet, the authenticator relays the contained EAP-Request/MD5 Challenge packet to the supplicant.

7) When receiving the EAP-Request/MD5 Challenge packet, the supplicant uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the authenticator.

8) After receiving the EAP-Response/MD5 Challenge packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.

9) When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the authenticator a RADIUS Access-Accept packet.

10) Upon receiving the RADIUS Access-Accept packet, the authenticator opens the port to grant the access request of the supplicant. After the supplicant gets online, the authenticator periodically sends handshake requests to the supplicant to check whether the supplicant is still online. By default, if two consecutive handshake attempts end up with failure, the authenticator concludes that the supplicant has gone offline and performs the necessary operations, guaranteeing that the authenticator always knows when a supplicant goes offline.

11) The supplicant can also send an EAPOL-Logoff frame to the authenticator to go offline unsolicitedly. In this case, the authenticator changes the status of the port from authorized to unauthorized and sends an EAP-Failure frame to the supplicant.

31.2 Configure AAA

Finish necessary configuration of domain and RDIUS project of 802.1X authentication.

31.2.1 Configure RADIUS Server

RADIUS server saves valid user's identity. When authentication, system transfers user's identity to RADIUS server and transfer the validation to user .User accessing to system can access LAN resources after authentication of RADIUS server.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Enter RAIDUS configuration	**radius host** *radius-name*	
Configure primary auth RADIUS	**primary-auth-ip** *ip-address port*	
Configure primary acct RADIUS	**primary-acct-ip** *ip-address port*	
Configure second auth RADIUS	**second-auth-ip** *ip-address port*	
Configure second acct RADIUS	**second-acct-ip** *ip-address port*	
Configure key string of RADIUS	**auth-secret-key** *keystring*	
Configure key string of RADIUS	**acct -secret-key** *keystring*	
Configure NAS-RAIDUS address	**nas-ipaddress** *ip-address*	
Setup the username format	**username-format** { with-domain | without-domain }	
Configure accounting	**realtime-account**	
Configure the times of accouting	**realtime-account interval** *account-times*	

31.2.1 Configure Local User

Client need configure local user name and password.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Configure local user	**local-user username** *name* **password** *pwd* [**vlan** *vlan-id*]	

31.2.2 Configure Domain

Client need provide username and password when authentication. Username contains user's ISP information, domain and ISP corresponded. The main information of domain is theRADIUS server authentication and accounting the user should be.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Configure default Domain	**default domain-name** { disable | enable }	
setup Domain	**domain** *domain-name*	
Configure default Domain scheme	**scheme** { local | radius [local] }	
choice RADIUS name	**radius host binding** *radius-name*	
configure access limit users	**access-limit** { enable *number* | disable }	
active the state	**state** { active | block }	

31.2.1 Configure RADIUS Features

Configure RADIUS some compatible or special features as below:

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enter AAA mode	**aaa**	
Enable user re-authentication, when it executives	**accounting-on** { enable *account-num* | disable }	
H3C Cams compatible under this feature can uprate-value / dnrate-value to configure the upstream bandwidth / downstream bandwidth of the Vendor Specific attribute name of the attribute number.	**h3c-cams** { enable | disable }	
Accounting function	**radius accounting**	
Accounting packets without response need cut off users	**radius server-disconnect drop 1x**	
Enable port priority	**radius 8021p enable**	This feature is turned on, if the user authentication passes, it will be modified by the user where the priority of the port.

Enable port PVID	**radius vlan enable**	This feature is turned on, if the user authentication passes , it will be modified by the user where port PVID is
Enable limit port of MAC address numbers	**radius mac-address-number enable**	This feature is turned on, if the user authentication passes, the user will modify the port about the limiting number of MAC address learning.
Enable limit port bandwidth	**radius bandwidth-limit enable**	By default unit is kbps, can be modified through radius config-attribute access-bandwidth unit.

31.3 Configure 802.1X

31.3.1 Configure EAP

The 802.1X authentication can be initiated by either a supplicant or the authenticator system. A supplicant can initiate authentication by launching the 802.1x client software to send an EAPOL-Start frame to the authenticator system, while an authenticator system can initiate authentication by unsolicitedly sending an EAP-Request/Identity packet to an unauthenticated supplicant.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
set the protocol type between system and RADIUS	**dot1x** { **eap-finish** | **eap-transfer** }	

31.3.2 Enable 802.1x

802.1x provides a user identity authentication scheme. However, 802.1x cannot implement the authentication scheme solely by itself. RADIUS or local authentication must be configured to work with 802.1x

Enabling 802.1S authentication, users connected to the system can access to LAN per passing the authentication.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable 802.1x	**dot1x method** { **macbased** | **portbased** }	

31.3.3 Configure 802.1x Parameters for a Port

The 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure 802.1x parameters for a port	**dot1x port-control** { **auto** | **forceauthorized** | **forceunauthorized** } [**interface ethernet** *interface-list*]	

31.3.4 Configure Re-Authentication

In EAP-FINISH way, the port supports re-authentication. After the user is authenticated, theport can be configured to immediately re-certification, or periodic re-certification.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Immediately re-certification	**dot1x re-authenticate** [**interface ethernet** *interface-list*]	
Periodic re-authentication enabled on a port	**dot1x *re-authentication*** [**interface ethernet** *interface-list*]	
Periodic re-authentication time configuration port	**dot1x timeout re-authperiod** *time* [**interface ethernet** *interface-list*]	

31.3.5 Configure Watch Feature

Opening function, the port without the user's circumstances, will watch regularly sends a 1xpacket, triggering the following 802.1x user authentication.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Open the watch function	**dot1x daemon** [**interface ethernet** *interface-list*]	
Configuration time between sending	**dot1x daemontime** [**interface ethernet**	
packets Watch	*interface-list*]	

31.2.1 Configure User Features

The operations mainly conclude of the number of users for port configuration, user and delete users, and heartbeat detection operations.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configuration allows the maximum number of users through the authentication	**dot1x max-user** *user-num* [**interface ethernet** *interface-list*]	
Deletes the specified users online	**dot1x user cut** { **username** *name* | **mac-address** *mac-address* }	
Open heartbeat detection	**dot1x detect** [**interface ethernet** *interface-list*]	
Heartbeat detection time configuration	**dot1x detect interval** *time*	