802.1x Configuration

XXXX Communication Technology Co., Ltd

Tel: (86)

Fax: (86)

URL:

Email:

XXXX values and appreciates comments you may have concerning our products or this document. Please address comments to:

XXXX Communication Technology Co., Ltd

Tel: (86)

Fax: (86)

URL:

Email:

XXXX Feedback Form

Your opinion helps us improve the quality of our product documentation and offer better services.

Document Title			
Product Version		Document Revision Number	1.0
Evaluate this document	**Presentation:** (Introductions, procedures, illustrations, completeness, arrangement, appearance) ☐ Good ☐ Fair ☐ Average ☐ Poor		
	Accessibility: (Contents, index, headings, numbering) ☐ Good ☐ Fair ☐ Average ☐ Poor		
	Editorial: (Language, vocabulary, readability, clarity, technical accuracy, content) ☐ Good ☐ Fair ☐ Average ☐ Poor		
Your suggestions to improve the document	**Please check suggestions to improve this document:** ☐ Improve introduction ☐ Make more concise ☐ Improve Contents ☐ Add more step-by-step procedures/tutorials ☐ Improve arrangement ☐ Add more technical information ☐ Include images ☐ Make it less technical ☐ Add more detail ☐ Improve index		
If you wish to be contacted, complete the following:			
Name		**Company**	
Postcode		**Address**	
Telephone		**E-mail**	

Contents

Chapter1 Configuring 802.1X

1.1 Brief Introduction to 802.1X Configuration

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. Users access 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 Switch devices. When getting authentication, switch is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing switch and verifies the information through authentication server. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

1.1.1 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, as shown in figure 1-1.

- 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 authenticates the connected supplicant system. An authenticator system is usually an 802.1x-enabled network device and provides ports (physical or logical) for supplicants to access the LAN.
- Authentication server system: The system providing authentication, authorization, and accounting services for the authenticator system. The authentication server, usually a Remote Authentication Dial-in User Service (RADIUS) server, maintains user information like username, password, VLAN that the user belongs to, committed access rate (CAR) parameters, priority, and ACLs.

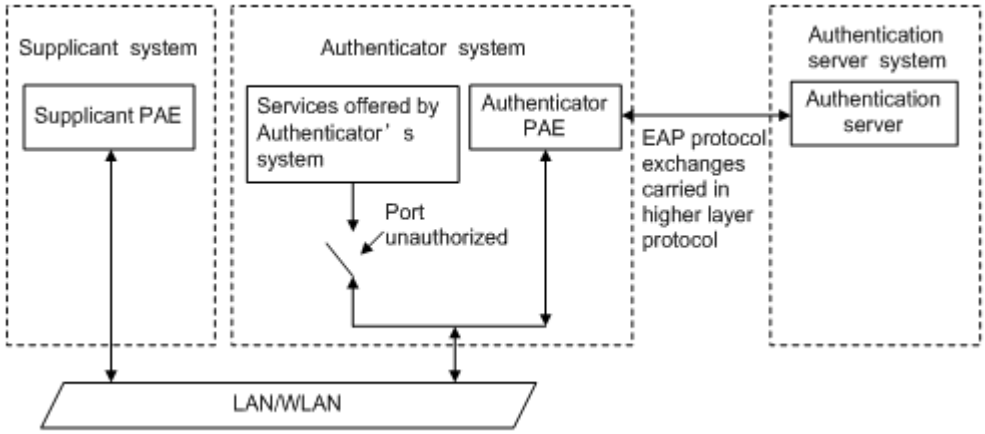

Figure 1-1 Architecture of 802.1x

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 receive authentication 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.

1.1.2 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.

1.1.3 Configuring AAA

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

1.1.4 Configuring 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.

Table1-1 Configure RADIUS server

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

1.1.5 Configuring Local User

Client need configure local user name and password.

Table 1-2 Configure local user

Operation	Command	Remark
Enter global configuration mode	**configure terminal**	-
Enter AAA mode	**aaa**	required
Configure local user	**local-user username** *name* **password** *pwd*	required

	[vlan *vid* **]**	

1.1.6 Configuring 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 the RADIUS server authentication and accounting the user should be.

Table 1-3 Configure Domain

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

1.1.7 Configuring RADIUS Features

Configuring RADIUS some compatible or special features as below:

Table 1-4 Configure RADIUS features

Operation	Command	Remark
Enter global configuration mode	**configure terminal**	-
Enter AAA mode	**aaa**	required
Enable user re-authentication, when it executives, the device restarts after a user authentication to the RADIUS server sends Accounting-On message, notify the RADIUS server to force the device goes offline.	**accounting-on** { **enable** *send-num* | **disable** }	optional
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 }**	optional
This feature can be under the RADIUS attribute client-version to the version of configuration information to send the client to the RADIUS server.		
accounting function	**radius accounting**	optional
Accounting packets without response need cut off users	**radius server-disconnect drop 1x**	optional

port priority This feature is turned on, if the user authentication passes, it will be modified by the user where the priority of the port. This feature is by default the property name in the Vendor Specific attribute number to 77, with radius config-attribute you can modify the properties of numbers.	**radius 8021p enable**	optional
Port PVID This feature is turned on, if the user authentication passes , it will be modified by the user where port PVID is This function is fixed by the Tunnel-Pvt-Group-ID attribute names, which requires a string of the property value, this string for the VLAN by name descriptor matches the VLAN value.	**radius vlan enable**	optional
Limit port of MAC address numbers This feature is turned on, if the user authentication passes, the user will modify the port about the limiting number of MAC address learning. This feature is by default the property name in the Vendor Specific attribute number to 50, with radius config-attribute you can modify the properties of numbers.	**radius mac-address-number enable**	optional
Limit port bandwidth This feature is turned on, if the user authentication passes, the user will modify the port bandwidth limitation. Upstream bandwidth control carries out per attribute number 75 in Vendor specific attribution and be modified attribution by using radius config-attribute. Downstream bandwidth control carries out per attribute number 76 in Vendor specific attribution and be modified attribution by using radius config-attribute.	**radius bandwidth-limit enable**	optional

By default unit is kbps, can be modified through radius config-attribute access-bandwidth unit.		

1.1 Configuring 802.1X

1.1.8 Configuring 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.

Table 1-4 Configure EAP

Operation	Command	Remark
Enter global configuration mode	**configure terminal**	-
set the protocol type between system and RADIUS	**dot1x eap-finish | eap-transfer**	optional

1.1.9 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.

Table 1-5 Enable 802.1x

Operation	Command	Remark
Enter global configuration mode	**configure terminal**	-
Enable 802.1x	**dot1x method { macbased | portbased }** [*interface-list*]	required

1.1.10 Configuring 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.

Table 1-6 Configure 802.1x parameters for a port

Operation	Command	Remark
Enter global configuration mode	**configure terminal**	-

Configure 802.1x parameters for a port	**dot1x port-control { auto | forceauthorized | forceunauthorized }** [*interface-list*]	required

1.1.11 Configuring Re-Authentication

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

Table 1-7 Configure re-authentication

operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Immediately re-certification	**dot1x re-authenticate** *[interface-list]*	Optional
Periodic re-authentication enabled on a port	**dot1x re-authentication** *[interface-list]*	Optional
Periodic re-authentication time configuration port	**dot1x timeout re-authperiod** *time [interface-list]*	Optional

1.1.12 Configuring Watch Feature

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

Table 1-8 Configure watch feature

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Open the watch function	**dot1x daemon** *[interface-list]*	Optional
Configuration time between sending packets Watch	**dot1x daemon time** time *[interface-list]*	Optional

1.1.13 Configuring User Features

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

Table 1-9 Configure user feature

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-

Configuration allows the maximum number of users through the authentication	**dot1x max-user** *user-num [interface-list]*	Optional
Deletes the specified users online	**dot1x user cut {username name | mac-address** mac [vlan *vid]}*	Optional
Open heartbeat detection	**dot1x detect** *[interface-list]*	Optional
Heartbeat detection time configuration	**dot1x detect interval** *time*	Optional