JXNET 甲信

甲信三层以太网交换机 802.1X 技术配置手册

配置指南(CLI)

(Rel_01)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

目录

1.1 802.1x

1.1.1 简介

802.1x 是基于 IEEE 802.1x 协议即基于接口的网络接入控制技术。802.1x 功能的主要目的是解决局域网用户的接入认证和安全问题。

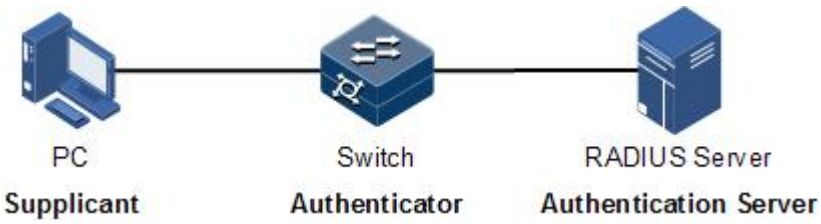
在网络设备的物理接入层对接入设备进行认证和控制，仅定义了设备接口和用户设备之间的点到点连接方式。连接在接口上的用户设备如果能够通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法通过交换机访问网络中的资源。

802.1x 体系结构

802.1x 认证采用客户端/服务器模式，如下图所示，包括以下 3 个部分：

- 申请者（Supplicant）：需要安装 802.1x 客户端软件（例如 Windows XP 自带的 802.1x 客户端）的用户侧设备，如计算机等。
- 认证者（Authenticator）：提供 802.1x 认证功能的接入控制设备，如交换机等。
- 认证服务器（Authentication Server）：用于对用户进行认证、授权和计费，通常使用 RADIUS 服务器作为 802.1x 认证服务器。

图 1-1 802.1x 认证体系结构



接口接入控制模式

认证者利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果对接入接口授权或者非授权状态进行控制。用户可以通过配置接口的接入控制模式来控制接口的接入状态。802.1x 认证支持三种接口接入控制模式：

- 协议授权模式（auto）：由协议状态机决定认证授权结果，在认证成功之前，仅允许收发 EAPoL 报文，不允许用户访问网络资源和交换机提供的服务。如果认证通过，则接口切换到授权状态，允许用户访问网络资源和交换机提供的服务。
- 强制接口授权模式（authorized-force）：接口始终处于授权状态，允许用户不经认证授权即可访问网络资源和交换机提供的服务。
- 强制接口非授权模式（unauthorized-force）：接口始终处于非授权状态，不允许用户访问网络资源和交换机提供的服务，即不允许用户进行认证。

802.1x 认证过程

802.1x 系统支持 EAP 中继和 EAP 终结两种方式完成与 RADIUS 服务器之间的认证过程。

- EAP 中继方式

申请者与认证服务器之间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）报文交换信息。申请者与认证者之间则以 IEEE802.1x 协议所定义的 EAPoL（EAP over LAN，基于局域网的 EAP）报文交换信息。EAP 报文中封装了认证数据，该认证数据将被封装在 RADIUS 协议的报文中，以穿越复杂的网络到达认证服务器，这一过程称为 EAP 中继。

认证者或申请者均能发起 802.1x 认证过程。以申请者发起认证过程为例，EAP 中继认证过程如下：

1. 用户输入用户名和密码，申请者向认证者发送一个 EAPoL-Start 报文，开始一次 802.1x 认证；
2. 认证者向申请者发送 EAP-Request/Identity 报文，询问请求者的用户名；
3. 申请者响应一个 EAP-Response/Identity 给认证者，其中包括用户名信息；
4. 认证者将 EAP-Response/Identity 报文封装到 RADIUS 协议报文中，发送给认证服务器；
5. 认证服务器将接收到的用户名信息与数据库中的用户名表进行比对，找到该用户的口令信息，利用随机生成的加密字对口令信息进行加密处理。同时，认证服务器将此加密字发送给认证者，认证者再将此加密字发送给申请者；
6. 申请者利用接收到的加密字对口令进行加密，并通过认证者发送给认证服务器；
7. 认证服务器对比收到的加密口令与自身生成的加密口令否一致。如果认证成功，认证者将接口改为授权状态，允许用户通过接口访问网络，并发送 EAP-Success 报文给申请者；如果认证失败，则接口为非授权状态，并发送 EAP-Failure 报文给通知申请者。

- EAP 终结方式

将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费过程。设备端支持与 RADIUS 服务器之间采用 PAP 或者 CHAP 认证方法。

在 EAP 终结方式中，用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息共同发送给 RADIUS 服务器，进行相关的认证处理。

802.1x 定时器

802.1x 认证过程中，认证设备上涉及到 5 个定时器：

- Reauth-period：重认证定时器。在该定时器超时后，会重新发起 802.1x 认证。

- Quiet-period：静默定时器。用户认证失败以后，认证设备需要静默一段时间，静默定时器超时后再重新发起认证。在静默期间，交换机不处理认证报文。
- Tx-period：请求报文发送超时定时器。当交换机向用户请求端发送 Request/Identity 请求报文后，会启动该定时器，在该定时器超时后，用户端软件未成功发送认证应答报文，则设备重发认证请求报文，此报文共重发 3 次。
- Supp-timeout：申请者认证超时定时器。当交换机向用户请求端发送了用于请求用户端 MD5 加密密文的 Request/Challenge 请求报文后，交换机启动该定时器。若在该定时器设置的时长内用户请求端未成功响应，交换机将重发该报文，此报文共重发两次。
- Server-timeout：认证服务器超时定时器。该定时器定义认证者和认证服务器会话超时的总时长，此定时器超时后认证者结束同认证服务器会话，重新开始一次新的认证过程。

802.1x guest-vlan

在网络中，用户在未经过 802.1x 认证时只能访问有限资源，当配置 guest-vlan 功能后，设备对 untag 报文添加 guest-vlan，并允许该报文通过端口。

- 基于端口认证：认证时认证通过会删除端口的 guest-vlan。
- 基于用户认证：认证通过会保留端口的 guest-vlan。
- guset-vlan 不能是 supervlan，也不能是 voice-vlan。

1.1.2 配置准备

场景

为了实现对局域网用户的接入认证，并解决接入用户的安全问题，需要在设备上配置 802.1x 认证。

对于认证通过的用户，允许其访问网络中的资源；如果认证未通过，则该用户无法访问网络资源。通过对用户接入接口的认证控制，达到对用户管理的目的。

前提

配置 802.1x 认证之前，如果使用 RADIUS 认证服务器，需要完成以下任务：

- 配置 RADIUS 服务器 IP 地址和 RADIUS 公有密钥。
- 交换机能够与 RADIUS 服务器 Ping 通。

1.1.3 802.1x 功能的缺省配置

设备上 802.1x 功能的缺省配置如下。

功能	缺省值
全局 802.1x 功能状态	禁止
接口 802.1x 功能状态	禁止
全局认证方式	**chap**
接口接入控制模式	**auto**
接口认证方式	**macbased**
RADIUS 服务器超时定时器时间	10s
802.1x 重认证功能状态	允许
802.1x 重认证定时器时间	5600s
802.1x 静默定时器时间	60s
请求报文重传定时器时间	30s
最大用户数	128

1.1.4 配置 802.1x 基本功能

注意

- 一个接口同一时刻只能处理一个用户认证请求。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#dot1x { start | stop }`	使能或去使能全局 802.1x 功能。
3	`JX(config)#dot1x aaa authentication method` *`method-name`*	绑定全局 802.1x 认证时的 AAA 方法。
4	`JX(config)#dot1x max-user` *`user-number`*	配置全局 802.1x 认证最大用户数。
5	`JX(config)#interface` *`interface-type interface-number`*	进入二层物理接口配置模式。
6	`JX(config-ge-1/0/*)#dot1x enable`	使能接口 802.1x 功能。
7	`JX(config-ge-1/0/*)#dot1x port-control { auto | force-auth | force-unauth }`	配置接口接入控制模式。
8	`JX(config-ge-1/0/*)#dot1x port-method { mac | port }`	配置接口认证方式。

步骤	配置	说明
9	JX(config-ge-1/0/*)#**dot1x max-user** *user-number*	配置 802.1x 端口允许认证的最大用户数。
10	JX(config-ge-1/0/*)#**nac guest-vlan** *vlan-id*	配置指定端口的 Guest VLAN，对 802.1x 协议和 mac 认证都生效。
11	JX(config-ge-1/0/*)#**dot1x critical-vlan** *vlan-id*	配置指定端口的 802.1x Critical VLAN。
12	JX(config-ge-1/0/*)#**dot1x restrict-vlan** *vlan-id*	配置指定端口的 802.1x Restrict VLAN。
13	JX(config-ge-1/0/*)#**dot1x reauthenticate all user**	手动触发指定端口下 802.1x 用户进行重认证。
14	JX(config-ge-1/0/*)#**dot1x delete all user**	强制将端口下 802.1x 用户下线。
15	JX(config-ge-1/0/*)#**dot1x quiet { disable | enable }**	使能或去使能端口 802.1x 用户静默功能。
16	JX(config-ge-1/0/*)#**dot1x quiet-times** *times*	配置端口 802.1x 用户触发静默功能的认证失败次数，默认 3 次。

说明

如果全局或接口模式下未使能 802.1x 功能，则接口下不能使能 802.1x 功能。

1.1.5 配置 802.1x 重认证

注意

重认证功能是针对已授权的用户发起的，所以在使能重认证功能之前，应该保证使能全局和接口 802.1x 功能。处于授权状态的接口在重认证过程中仍保持授权状态，如果重认证失败，才进入非授权状态。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate { enable | disable }**	使能 802.1x 重认证功能。

1.1.6 配置 802.1x 定时器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate period** *time*	配置重认证定时器时间。
4	JX(config-ge-1/0/*)#**dot1x timer quiet-period** *time*	配置静默定时器时间。
5	JX(config-ge-1/0/*)#**dot1x supp period** *time*	配置 Request/MD5 Challenge 请求报文超时定时器。
6	JX(config-ge-1/0/*)#**dot1x server-timeout period** *time*	配置认证服务器超时定时器时间。
7	JX(config-ge-1/0/*)#**dot1x tx period** *time*	配置 Request/Identity 请求报文超时定时器。

1.1.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show dot1x config**	查看所有 802.1x 相关配置信息。
2	JX#**show dot1x information**	查看 802.1x 协议统计信息。
3	JX#**show dot1x user**	查看 802.1x 协议认证的用户信息。
4	JX#**show dot1x** *interface-type interface-number*	查看接口下 802.1x 相关统计及配置信息。

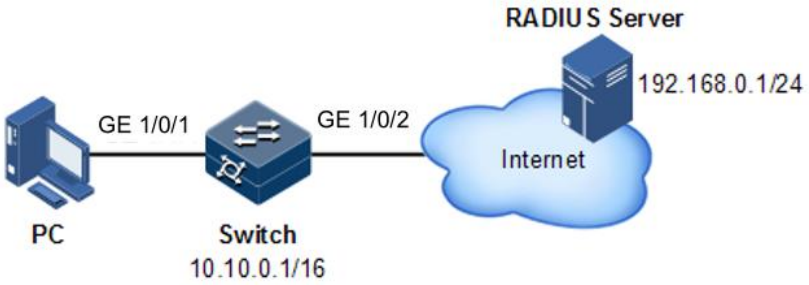
1.1.8 配置 802.1x 示例

组网需求

为了使用户访问外部网络，如下图所示，在交换机上配置 802.1x 认证，具体要求如下：

- 交换机的 IP 地址是 10.10.0.1，掩码是 255.255.0.0，缺省网关地址为 10.10.0.2。
- 通过 RADIUS 服务器进行认证和授权，RADIUS 服务器的 IP 地址是 192.168.0.1，密码是 JX。
- 在认证通过后，可以在 600s 后自动发起重认证过程。

图 1-2 802.1x 应用组网示意图



配置步骤

步骤 1 配置交换机 IP 地址及 RADIUS 服务器地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlan1)#ip address 10.10.0.1/16
JX(config-vlan1)#exit
JX(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
JX(config)#exit
JX(config)#aaa
JX(config-aaa)#radius-server host server1 ip-address
192.168.0.1 key 12345
JX(config-aaa)#server-group grp1 radius-server server1
JX(config-aaa)#aaa authentication dot1x method d1 first grp1
```

步骤 2 使能全局及接口 802.1x 认证功能。

```
JX#config
JX(config)#dot1x start
JX(config)#dot1x aaa authentication method d1
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x reauthenticate period 600
```

检查结果

通过 **show dot1x** 命令查看设备上 802.1x 功能的配置结果。

```
JX#show dot1x interface ge 1/0/1
Interface                  : ge 1/0/1
 Authentication Guest Vlan    : n/a
 Max User Num               : 1
 Default Max User Num        : 1
 Current User Num           : 1
 Authen Success User Num     : 0
 Authen Fail User Num        : 1
 Authen Timeout User Num     : 1
 Authenting User Num         : 0
 Authentication Method       : n/a
 Accounting Method           : n/a
 Quiet                     : Disable
 Reauthentication            : Enable
```

```
Reauthentication Period     : 5600
Mac Bypass                 : Disable
Offline Detect              : Disable
Restrict Vlan              : n/a
Critical Vlan              : n/a
TX Period                  : 30
Supp Timeout Period         : 5
Server time Period          : 120
Port Control               : Auto
Port Method                : Mac Based
Port Auth State             : Unauthenticated
Auth Method                : Chap
Not Eapol Trigger           : Disable
Trigger Authen Type         : None
Trigger Auth Pkt Type       : ARP NDP DHCP DHCP6
Rx Eapol Start Pkt Num      : 61
Rx Eapol Logoff Pkt Num     : 0
Rx Eap Idenitity Pkt Num    : 12
Rx Eap MD5 Pkt Num          : 5
Tx Eap Success Pkt Num      : 0
Tx Eap Fail Pkt Num         : 11
Tx Eap Idenitity Pkt Num    : 6
Tx Eap MD5 Pkt Num          : 5
```