JXNET 甲信

甲信三层以太网交换机 AAA 认证技术配置手册

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 AAA

1.1.1 简介

AAA

AAA（Authentication、Authorization、Accounting，认证、授权、计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

- 认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。
- 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA 采用客户端/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。

AAA 可以通过多种协议来实现，这些协议规定了 NAS 与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议和 TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）。

RADIUS

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是一种用于对远程访问用户进行集中鉴别的标准化通信协议。RADIUS 使用 UDP 作为传输协议（端口 1812、1813），具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

- 认证功能

RADIUS 使用客户端/服务器模式，网络访问设备作为 RADIUS 服务器的客户端。RADIUS 服务器负责接收用户的连接请求、对用户进行鉴别，然后将所有客户端所需的配置信息传回，以便为用户提供服务。通过这种方式可以控制用户对设备和网络的访问，提高网络的安全性。

客户端与 RADIUS 服务器之间的通信是通过共享密钥的使用来鉴别的，这个共享密钥不会通过网络传送。此外，任何用户口令在客户机和 RADIUS 服务器间发送时都需要进行加密过程，以避免有人通过嗅探非安全网络得到用户密码。

- RADIUS 计费功能

RADIUS 计费功能主要针对通过 RADIUS 认证的用户进行。在用户登录时给 RADIUS 计费服务器发送一个开始计费的报文，在登录期间根据计

费策略给 RADIUS 计费服务器发送计费更新报文，退出登录时，给 RADIUS 计费服务器发送停止计费报文，报文里面包含用户的登录时间。通过这些报文，RADIUS 计费服务器可以记录每个用户的访问时间和操作。

TACACS+

TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）是一种与 RADIUS 类似的网络接入认证协议。其区别如下：

- TACACS+使用 TCP 端口 49，相对于 RADIUS 使用的 UDP 端口，具有更高的传输可靠性。
- TACACS+加密数据包除标准的 TACACS+头部外的整体，而包头中有一个区域会指示数据包是否加密。相对于 RADIUS 的只加密用户密码，安全性更高。
- TACACS+的认证功能与授权、计费功能相分离，部署更灵活。

综上所述，TACACS+较 RADIUS 更加安全、可靠，但是 RADIUS 作为一种开放性的协议，在网络中的应用更加广泛。

1.1.2 配置准备

场景

为了控制用户对设备和网络的访问，可以在网络中部署 RADIUS/TACACS+服务器对用户进行认证和计费。本设备可以作为 RADIUS/TACACS+服务器的代理设备，根据 RADIUS/TACACS+服务器反馈的结果对用户访问进行授权。TACACS+较 RADIUS 更加安全、可靠。

前提

无

1.1.3 缺省配置

设备上 AAA 的缺省配置如下。

功能	缺省值
RADIUS 认证服务器未响应之后的失效时间	60 秒
RADIUS 报文重传次数	3
RADIUS 报文重传时间间隔	2 秒
RADIUS 认证服务器未响应之后的失效时间	60 秒
TACACS 认证服务器 TCP 连接超时和收包超时时间	2 秒

1.1.4 配置 RADIUS 服务器

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)# **aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**radius-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，单位为秒，缺省值为 60 秒。
4	JX(config-aaa)#**radius-server max-retransmit** { *count* | **default** }	全局配置发送请求失败后的重传次数，缺省值为 3 次。
5	JX(config-aaa)#**radius-server retransmit-interval** { *interval* | **default** }	全局配置重传时间间隔，缺省值为 2 秒。
6	JX(config-aaa)#**radius-server host** *server-name* **ip-address** *ip-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip** *ip-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv4 RADIUS 服务器。
7	JX(config-aaa)#**radius-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip6** *ipv6-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv6 RADIUS 服务器。

1.1.5 配置 TACACS+服务器

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)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**tacacs-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，单位为秒，缺省值为 300 秒。
4	JX(config-aaa)#**tacacs-server timeout** { *second* | **default** }	全局配置与服务器的 TCP 连接超时和收包超时时间，缺省值为 2 秒。

步骤	配置	说明
5	JX(config-aaa)#**tacacs-server host** *server-name* **ip-address** *ip-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip** *ip-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv4 TACACS 服务器。
6	JX(config-aaa)#**tacacs-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip6** *ipv6-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv6 TACACS 服务器。

1.1.6 配置 AAA 服务器组

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)#**aaa**	进入 AAA 配置模式。
3	JX (config-aaa)#**server-group** *group-name* { **radius-server** | **tacacs-server** } *server-name*	创建 AAA 服务器组或向 AAA 服务器组添加服务器

1.1.7 配置 AAA 方法

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)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**aaa authentication** { **dot1x** | **login** | **mac-authen** | **enable** } **method** *method-name* **first** { *group-name* | **local** } **second** { *group-name* | **local** | **none** } **third** { *group-name* | **local** | **none** }	配置 AAA 认证方法。 注意事项：服务器组最多配置两个。
4	JX(config-aaa)#**aaa authorization** { **login** | **cmd** } **method** *method-name* **first** { *group-name* | **local** } **second** { *group-name* | **local** | **none** } **third** { *group-name* | **local** | **none** }	配置 AAA 授权方法。 注意事项：服务器组最多配置两个。

步骤	配置	说明
5	JX (config-aaa)#**aaa accounting { dot1x | login | mac-authen } method** *method-name* **first {** *group-name* **| local } second { group-name | local | none } third {** *group-name* **| local | none }**	配置 AAA 计费方法。 注意事项：服务器组最多配置两个。

1.1.8 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 aaa config**	查看 AAA 配置信息。
2	JX#**show aaa information**	查看 AAA 全局信息。
3	JX#**show aaa server**	查看 AAA 服务器信息。
4	JX#**show aaa server-group**	查看 AAA 服务器组信息。
5	JX#**show aaa method**	查看 AAA 方法信息。

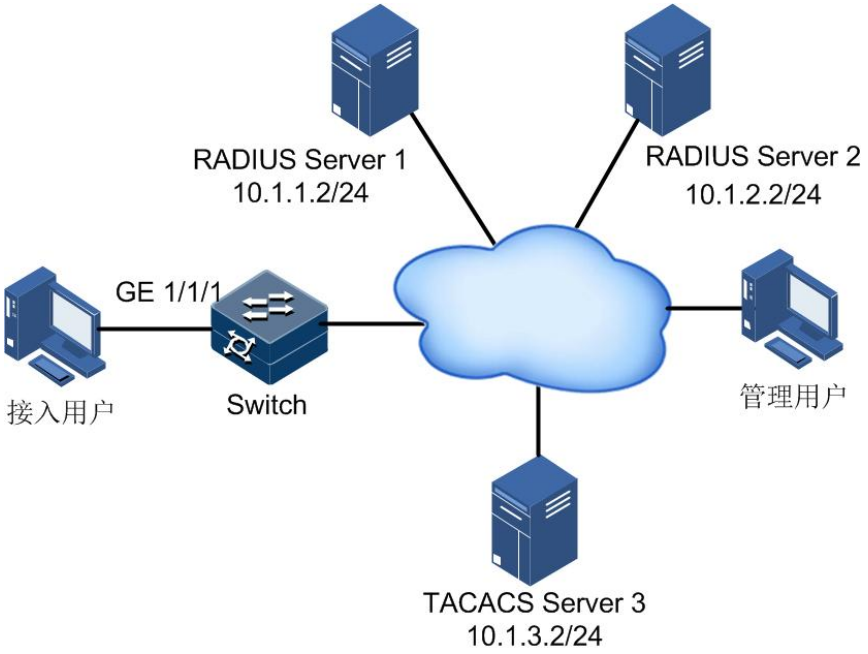
1.1.9 配置 AAA 示例

组网需求

如下图所示，实现接入用户和管理用户接入不同的服务器，要求配置如下：

- 在 Switch 上配置 IP 地址、Vlan 和路由，用于用户连接及认证。
- 创建本地用户，配置管理用户所用的 AAA 模板和方案，采用 TACACS Server 3 进行认证和授权，RADIUS Server 2 进行计费。
- 开启 Dot1x 功能，配置接入用户所使用的 AAA 模板和方案，采用 RADIUS Server 1 进行认证、计费和授权。

图 1-1 分域认证应用组网示意图



配置步骤

步骤 1 配置 IP 地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlanif-1)#ip address 10.1.0.254/24
JX(config-vlanif-1)#exit
JX(config)ip route-static 0.0.0.0 0.0.0.0 10.1.0.1
```

步骤 2 配置 AAA 服务器。

```
JX(config)#aaa
JX(config-aaa)#radius-server host Server1 ip-address 10.1.1.2
JX(config-aaa)#radius-server host Server2 ip-address 10.1.2.2
JX(config-aaa)#tacacs-server host Server3 ip-address 10.1.3.2
```

步骤 3 配置 AAA 服务器组。

```
JX(config-aaa)#server-group Group1 radius-server Server1
JX(config-aaa)#server-group Group2 radius-server Server2
JX(config-aaa)#server-group Group3 tacacs-server Server3
```

步骤 4 配置 AAA 方法。

```
JX(config-aaa)#aaa authentication login method Method1 first
Group3
JX(config-aaa)#aaa authorization login method Method2 first
Group3
JX(config-aaa)#aaa accounting login method Method3 first Group2
JX(config-aaa)#aaa authentication dot1x method Method4 first
Group1
JX(config-aaa)#aaa accounting dot1x method Method5 first Group1
switch(config-aaa)#exit
```

步骤 5 配置管理用户认证、授权、计费方法。

```
JX(config)#line vty * *
JX(config-line)#login authentication aaa method Method1
JX(config-line)#login authorization aaa method Method2
JX(config-line)#login accounting aaa method Method3
JX(config-line)#exit
```

步骤 6 配置接入用户认证、授权、计费方法。

```
JX(config)#dot1x start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x aaa-authentication Method4
JX(config-ge-1/0/1)#dot1x aaa-accounting Method5
JX(config-ge-1/0/1)#exit
```

1.1.10 检查结果

步骤 1 通过 **show aaa config** 查看 AAA 配置是否正确。

```
JX#show aaa config
Version  : AAA_V7.00.00.00
!
aaa
 radius-server host Server1 ip-address 10.1.1.2
 radius-server host Server2 ip-address 10.1.2.2
 tacacs-server host Server3 ip-address 10.1.3.2
 server-group Group1 radius-server Server1
 server-group Group2 radius-server Server2
 server-group Group3 tacacs-server Server3
 aaa authentication login method Method1 first Group3
 aaa authorization login method Method2 first Group3
 aaa accounting login method Method3 first Group2
 aaa authentication dot1x method Method4 first Group1
 aaa accounting dot1x method Method5 first Group1
```