目 录

第1章 802.1x 配置

1.1 802.1x 简介

1.1.1 802.1x 标准简介

IEEE 802.1x 标准（以下简称 802.1x）的主要内容是一种基于端口的网络接入控制（Port Based Network Access Control）协议，IEEE 于 2001 年颁布该标准文本并建议业界厂商使用其中的协议作为局域网用户接入认证的标准协议。802.1x 的提出起源于 IEEE 802.11 标准——无线局域网用户接入协议标准，其最初目的主要是解决无线局域网用户的接入认证问题；但由于它的原理对于所有符合 IEEE 802 标准的局域网具有普适性，因此后来它在有线局域网中也得到了广泛的应用。

在符合 IEEE 802 标准的局域网中，只要与局域网接入控制设备如 LANSwitch 相接，用户就可以与局域网连接并访问其中的设备和资源。但是对于诸如电信接入、商务局域网（典型的例子是写字楼中的 LAN）以及移动办公等应用场合，局域网服务的提供者普遍希望能对用户的接入进行控制，为此产生了本章开始就提到的对“基于端口的网络接入控制”的需求。

顾名思义，“基于端口的网络接入控制”是指在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源——相当于连接被物理断开。

802.1x 定义了基于端口的网络接入控制协议，并且仅定义了接入设备与接入端口间点到点这一种连接方式。其中端口既可以是物理端口，也可以是逻辑端口。典型的应用环境如：LANSwitch 的每个物理端口仅连接一个用户的计算机工作站（基于物理端口），IEEE 802.11 标准定义的无线 LAN 接入环境（基于逻辑端口）等。

1.1.2 802.1x 体系结构

使用 802.1x 的系统为典型的 C/S（Client/Server）体系结构，包括三个实体，如下图所示分别为：Supplicant System（接入系统）、Authenticator System（认证系统）以及 Authentication Server System（认证服务器系统）。

局域网接入控制设备需要提供 802.1x 的认证系统（Authenticator System）部分；用户侧的设备如计算机等需要安装 802.1x 的客户端（Supplicant）软件，如华为公司提供的 802.1x 客户端（或如 Windows XP 自带的 802.1x 客户端）；802.1x 的认证服务器系统（Authentication Server System）则一般驻留在运营商的 AAA 中心。

Authenticator 与 Authentication Server 间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）帧交换信息，Supplicant 与 Authenticator 间则以 IEEE 802.1x 所定义的 EAPoL（EAP over LANs，局域网上的 EAP）帧交换信息，EAP 帧中封装了认证数据，该认证数据将被封装在其它 AAA 上层协议（如 RADIUS）的报文中以穿越复杂的网络到达 Authentication Server，这一过程被称为 EAP Relay。

Authenticator 的端口又分为两种：非受控端口（Uncontrolled Port）和受控端口（Controlled Port）。非受控端口始终处于双向连通状态，用户接入设备可以随时通过这些端口访问网络资源以获得服务；受控端口只有在用户接入设备通过认证后才处于连通状态，才允许用户通过其进一步访问网络资源。

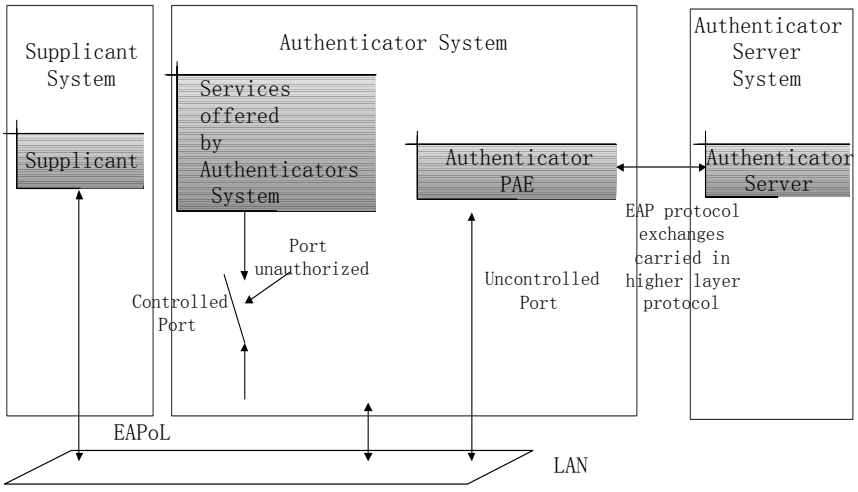

图1-1 802.1x 体系结构

1.1.3 802.1x 的认证过程

802.1x 通过 EAP 帧承载认证信息。标准中共定义了如下几种类型的 EAP 帧：

- EAP-Packet：认证信息帧，用于承载认证信息。
- EAPoL-Start：认证发起帧，Supplicant 主动发起的认证发起帧。
- EAPoL-Logoff：退出请求帧，主动终止已认证状态。
- EAPoL-Key：密钥信息帧，支持对 EAP 报文的加密。

- EAPoL-Encapsulated-ASF-Alert：用于支持 Alert Standard Forum（ASF）的 Alerting 消息。

其中 EAPoL-Start、EAPoL-Logoff 和 EAPoL-Key 仅在 Supplicant 和 Authenticator 间存在；EAP-Packet 信息由 Authenticator System 重新封装后传递到 Authentication Server System；EAPoL-Encapsulated-ASF-Alert 与网管信息相关，由 Authenticator 终结。

由上述的原理我们可以看到，802.1x 提供了一个用户身份认证的实现方案，但是仅仅依靠 802.1x 是不足以实现该方案的——接入设备的管理者还要对 AAA 方法进行配置，选择使用 RADIUS 或本地认证方法，以配合 802.1x 完成用户的身份认证。AAA 方法的具体配置细节，请参见本书的“AAA 和 RADIUS 协议配置”章节。

1.1.4 802.1x 在以太网交换机中的实现

Quidway 系列以太网交换机在 802.1x 的实现中，不仅支持协议所规定的端口接入认证方式，还对其进行了扩展、优化：

- 支持一个物理端口下挂接多个用户的应用场合；
- 接入控制方式（即对用户的认证方式）不仅可以基于端口，还可以基于 MAC 地址。

这样可极大地提高系统的安全性和可管理性。

1.2 802.1x 配置

802.1x 本身的各项配置任务都可以在以太网交换机的系统视图下完成。当全局 802.1x 没有开启时，可以对端口的 802.1x 状态进行配置，其配置项会在开启全局 802.1x 后生效。

🕮 **说明：**

(1) 请不要同时启动 802.1x 与 RSTP（或 MSTP），两者同时启动时不能保证交换机的正常工作。

(2) 如果端口启动了 802.1x，则不能配置该端口的最大 MAC 地址学习个数（通过命令 **mac-address max-mac-count** 配置），反之，如果端口配置了最大 MAC 地址学习个数，则禁止在该端口上启动 802.1x。

802.1x 的配置包括：

- 开启/关闭 802.1x 特性

- 设置端口接入控制的模式
- 设置端口接入控制方式
- 检测通过代理登录交换机的用户
- 设置端口接入用户数量的最大值
- 配置 802.1x 用户的认证方法
- 设置允许 DHCP 触发认证
- 设置认证请求帧的可重复发送次数
- 设置定时器参数
- 打开/关闭 quiet period 定时器

在以上的配置任务中，第一项任务是必配的，否则 802.1x 无法发挥作用；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

1.2.1 开启/关闭 802.1x 特性

可以通过下面的命令开启/关闭指定端口上的 802.1x 特性；当不指定任何确定的端口时，开启/关闭全局的 802.1x 特性。

请在系统视图或以太网端口视图下进行下列配置。

表1-1 开启/关闭 802.1x 特性

操作	命令
开启 802.1x 特性	**dot1x** [**interface** *interface-list*]
关闭 802.1x 特性	**undo dot1x** [**interface** *interface-list*]

各端口的 802.1x 状态在全局 802.1x 没有开启之前可以配置，但不起作用；在全局 802.1x 启动后，各端口配置会立即生效。

缺省情况下，全局及端口的 802.1x 特性均为关闭状态。

1.2.2 设置端口接入控制的模式

可以通过下面的命令来设置 802.1x 在指定端口上进行接入控制的模式。当没有指定任何确定的端口时，设置的是所有端口进行接入控制的模式。

请在系统或以太网端口视图下进行下列配置。

表1-2 设置端口接入控制的模式

操作	命令
设置端口接入控制的模式	**dot1x port-control** {**authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]
将端口接入控制的模式恢复为缺省值	**undo dot1x port-control** [**interface** *interface-list*]

缺省情况下，802.1x 在端口上进行接入控制的模式为 **auto**（自动识别模式，又称为协议控制模式），即：端口初始状态为非授权状态，仅允许 EAPoL 报文收发，不允许用户访问网络资源；如果认证流程通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

1.2.3 设置端口接入控制方式

可以通过下面的命令来设置 802.1x 在指定端口上进行接入控制方式。当没有指定任何确定的端口时，设置的是所有端口进行接入控制的方式。

请在系统或以太网端口视图下进行下列配置。

表1-3 设置端口接入控制方式

操作	命令
设置端口接入控制方式	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]
将端口接入控制方式恢复为缺省值	**undo dot1x port-method** [**interface** *interface-list*]

缺省情况下，802.1x 在端口上进行接入控制方式为 **macbased**，即基于 MAC 地址进行认证。

1.2.4 检测通过代理登录交换机的用户

可以通过下面的命令实现交换机对通过代理登录的用户的检测及相关控制。

请在系统或以太网端口视图下进行下列配置。

表1-4 设置通过代理登录交换机的用户的检测及控制

操作	命令
使能对通过代理登录交换机的用户的检测及控制	**dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]

操作	命令
取消对通过代理登录交换机的用户的检测及控制	**undo dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]

1.2.5 设置端口接入用户数量的最大值

可以通过下面的命令来设置 802.1x 在指定端口上可容纳接入用户数量的最大值。当没有指定任何确定的端口时，指示所有端口都可容纳相同数量的接入用户。

请在系统或以太网端口视图下进行下列配置。

表1-5 设置端口接入用户数量的最大值

操作	命令
设置端口接入用户数量的最大值	**dot1x max-user** *user-number* [**interface** *interface-list*]
将端口接入用户数量的最大值恢复为缺省值	**undo dot1x max-user** [**interface** *interface-list*]

缺省情况下，802.1x 在 S5516 以太网交换机所有的端口上都允许最多有 256 个接入用户。

1.2.6 设置允许 DHCP 触发认证

可以通过下面的命令来设置 802.1x 是否允许以太网交换机在用户运行 DHCP、申请动态 IP 地址时就触发对其的身份认证。

请在系统视图下进行下列配置。

表1-6 设置允许 DHCP 触发认证

操作	命令
允许 DHCP 触发认证	**dot1x dhcp-launch**
不允许 DHCP 触发认证	**undo dot1x dhcp-launch**

缺省情况下，不允许在用户运行 DHCP 申请动态 IP 地址时就触发对其的身份认证。

1.2.7 设置 802.1x 用户的认证方法

可以通过下面的命令来设置 802.1x 用户的认证方法。目前提供 3 种认证方法：PAP 认证（该功能的实现，需要 RADIUS 服务器支持 PAP 认证）、CHAP 认证（该功能的实现，需要 RADIUS 服务器支持 CHAP 认证）、EAP 中继认证（直接把认证信息以 EAP 报文的形式发送给 RADIUS 服务器，该功能的实现，需要 RADIUS 服务器支持 EAP 认证）

请在系统视图下进行下列配置。

表1-7 设置 802.1x 用户认证方法

操作	命令
设置 802.1x 用户的认证方法	**dot1x authentication-method { chap | pap | eap md5-challenge]**
恢复缺省 802.1x 用户认证方法	**undo dot1x authentication-method**

缺省情况下，交换机 802.1x 用户认证方法为 CHAP 认证。

1.2.8 设置认证请求帧的最大可重复发送次数

可以通过下面的命令来设置以太网交换机可重复向接入用户发送认证请求帧的最大次数。

请在系统视图下进行下列配置。

表1-8 设置认证请求帧的最大可重复发送次数

操作	命令
设置认证请求帧的最大可重复发送次数	**dot1x retry** *max-retry-value*
将认证请求帧的最大可重复发送次数恢复为缺省值	**undo dot1x retry**

缺省情况下，*max-retry-value* 为 3，即交换机最多可重复向接入用户发送 3 次认证请求帧。

1.2.9 配置定时器参数

可以通过下面的命令来配置 802.1x 的各项定时器参数。

请在系统视图下进行下列配置。

表1-9 配置定时器参数

操作	命令
配置定时器参数	**dot1x timer** { **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* }
将定时器参数恢复为缺省值	**undo dot1x timer** { **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout** }

其中：

quiet-period：静默定时器。当对 802.1x 用户认证失败以后，Authenticator 设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不进行 802.1x 认证的相关处理。

quiet-period-value：静默定时器设置的时长，取值范围 10～120，单位为秒。

server-timeout：Authentication Server 超时定时器。若在该定时器设置的时长内，Authentication Server 未成功响应，Supplicant 设备将重发认证请求报文。

server-timeout-value：Authentication Server 超时定时器设置的时长，取值范围为 100～300，单位为秒。

supp-timeout：Supplicant 认证超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功响应，Authenticator 设备将重发认证请求报文。

supp-timeout-value：Supplicant 认证超时定时器设置的时长，取值范围为 10～120，单位为秒。

tx-period：传送超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功发送认证应答报文，则 Authenticator 设备将重发认证请求报文。

tx-period-value：传送超时定时器设置的时长，取值范围为 10～120，单位为秒。

缺省情况下，*quiet-period-value* 为 60 秒；*tx-period-value* 为 30 秒；*supp-timeout-value* 为 30 秒；*server-timeout-value* 为 100 秒。

1.2.10 打开/关闭 quiet-period 定时器

可以通过下面的命令来打开/关闭 Authenticator 设备（如 Quidway 系列以太网交换机）的 quiet-period 定时器。当 802.1x 用户认证失败以后，Authenticator

设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不进行 802.1x 认证的相关处理。

请在系统视图下进行下列配置。

表1-10 打开/关闭 quiet-period 定时器

操作	命令
打开 quiet-period 定时器	**dot1x quiet-period**
关闭 quiet-period 定时器	**undo dot1x quiet-period**

1.3 802.1x 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 802.1x 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除 802.1x 相关配置。

在用户视图下，执行 **debugging** 命令可对 802.1x 进行调试。

表1-11 802.1x 的显示和调试

操作	命令
清除 802.1x 的统计信息	**reset dot1x statistics** [**interface** *interface-list*]
显示 802.1x 的配置、运行情况和统计信息	**display dot1x** [**interface** *interface-list*] **|** [**sessions** [**interface** *interface-list*] **|** [**statistics**[**interface** *interface-list*]]
打开 802.1x 的错误/事件/报文/全部调试开关	**debugging dot1x** { **error**	**event**	**packet**	**all** }
关闭 802.1x 的错误/事件/报文/全部调试开关	**undo debugging dot1x** { **error**	**event**	**packet**	**all** }

1.4 802.1x 典型配置举例

1. 组网需求

如下图所示，某用户的工作站与以太网交换机的端口 GigabitEthernet 1/1 相连接。

交换机的管理者希望在各端口上对用户接入进行认证，以控制其访问 Internet；接入控制模式要求是基于 MAC 地址的接入控制。

所有 AAA 接入用户都属于一个缺省的域：huawei163.net，该域最多可容纳 30 个用户；认证时，先进行 RADIUS 认证，如果 RADIUS 服务器没有响应再转而进行本地认证；计费时，如果 RADIUS 计费失败则切断用户连接使其下线；此外，接入时在用户名后不添加域名，正常连接时如果用户有超过 20 分钟流量持续小于 2000Byte/s 的情况则切断其连接。

由两台 RADIUS 服务器组成的服务器组与交换机相连，其 IP 地址分别为 10.11.1.1 和 10.11.1.2，要求使用前者作为主认证/从计费服务器，使用后者作为从认证/主计费服务器；设置系统与认证 RADIUS 服务器交互报文时的加密密码为“name”、与计费 RADIUS 服务器交互报文时的加密密码“money”，设置系统在向 RADIUS 服务器发送报文后 5 秒种内如果没有得到响应就向其重新发送报文，重复发送报文的次数总共为 5 次，设置系统每 15 分钟就向 RADIUS 服务器发送一次实时计费报文，指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

本地 802.1x 接入用户的用户名为 localuser，密码为 localpass，使用明文输入，闲置切断功能处于打开状态。

2. 组网图

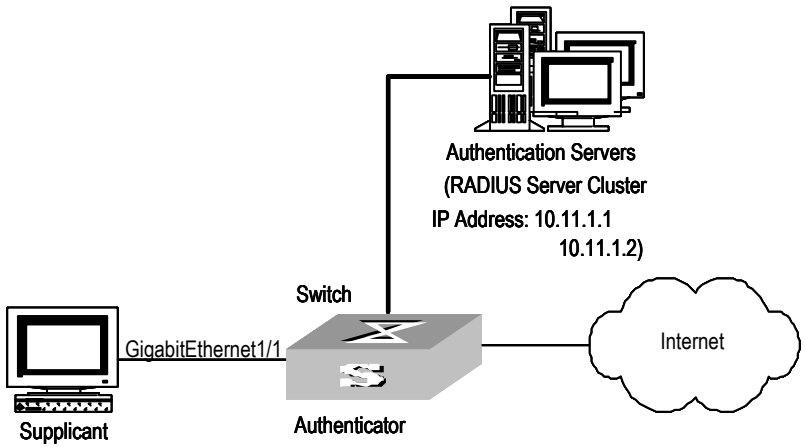

图1-2 启动 802.1x 和 RADIUS 对接入用户进行 AAA 操作

3. 配置步骤

📖 说明：

下述各配置步骤包含了大部分 AAA/RADIUS 协议配置命令，对这些命令的介绍，请参见“AAA 和 RADIUS 协议配置”一章的相关章节。

此外，接入用户工作站和 RADIUS 服务器上的配置略。

开启指定端口 GigabitEthernet 1/1 的 802.1x 特性。

[Quidway] dot1x interface GigabitEthernet 1/1

设置接入控制方式（该命令可以不配置，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

[Quidway] dot1x port-method macbased interface GigabitEthernet 1/1

创建 RADIUS 组 radius1 并进入其视图。

[Quidway] radius scheme radius1

设置主认证/计费 RADIUS 服务器的 IP 地址。

[Quidway-radius-radius1] primary authentication 10.11.1.1

[Quidway-radius-radius1] primary accounting 10.11.1.2

设置从认证/计费 RADIUS 服务器的 IP 地址。

[Quidway-radius-radius1] secondary authentication 10.11.1.2

[Quidway-radius-radius1] secondary accounting 10.11.1.1

设置系统与认证 RADIUS 服务器交互报文时的加密密码。

[Quidway -radius-radius1] key authentication name

设置系统与计费 RADIUS 服务器交互报文时的加密密码。

[Quidway-radius-radius1] key accounting money

设置系统向 RADIUS 服务器重发报文的时间间隔与次数。

[Quidway-radius-radius1] timer 5

[Quidway-radius-radius1] retry 5

设置系统向 RADIUS 服务器发送实时计费报文的时间间隔。

[Quidway-radius-radius1] timer realtime-accounting 15

指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

[Quidway-radius-radius1] user-name-format without-domain

[Quidway-radius-radius1] quit

创建用户域 huawei163.net 并进入其视图。

[Quidway] domain huawei163.net

指定 radius1 为该域用户的 RADIUS 服务器组。

[Quidway-isp-huawei163.net] radius-scheme radius1

设置该域最多可容纳 30 个用户。

[Quidway-isp-huawei163.net] access-limit enable 30

启动闲置切断功能并设置相关参数。

[Quidway-isp-huawei163.net] idle-cut enable 20 2000

添加本地接入用户。

[Quidway] local-user localuser

[Quidway-user-localuser] service-type lan-access

[Quidway-user-localuser] password simple localpass

开启全局 802.1x 特性。

[Quidway] dot1x

第2章 AAA 和 RADIUS 协议配置

2.1 AAA 和 RADIUS 协议简介

2.1.1 AAA 概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称，它提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，实际上是对网络安全的一种管理。

这里的网络安全主要是指访问控制，包括：

- 哪些用户可以访问网络服务器？
- 具有访问权的用户可以得到哪些服务？
- 如何对正在使用网络资源的用户进行计费？

针对以上问题，AAA 必须提供下列服务：

- 认证：验证用户是否可获得访问权。
- 授权：授权用户可使用哪些服务。
- 计费：记录用户使用网络资源的情况。

AAA 一般采用客户/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。

2.1.2 RADIUS 协议概述

如前所述，AAA 是一种管理框架，因此，它可以用多种协议来实现。在实践中，人们最常使用 RADIUS 协议来实现 AAA。

1. 什么是 RADIUS

RADIUS 是 Remote Authentication Dial-In User Service（远程认证拨号用户服务）的简称，它是一种分布式的、客户机/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常被应用在既要求较高安全性、又要求维持远程用户访问的各种网络环境中（例如，它常被应用来管理使用串口和调制解调器的大量分散拨号用户）。RADIUS 系统是 NAS（Network Access Server）系统的重要辅助部分。

当 RADIUS 系统启动后，如果用户想要通过与 NAS（PSTN 环境下的拨号接入服务器或以太网环境下带接入功能的以太网交换机）建立连接从而获得访问其它网络的权利或取得使用某些网络资源的权利时，NAS，也就是 RADIUS 客户端将把用户的认证、授权和计费请求传递给 RADIUS 服务器。RADIUS 服务器上有一个用户数据库，其中包含了所有的用户认证和网络服务访问信息。RADIUS 服务器将在接收到 NAS 传来的用户请求后，通过对用户数据库的查找、更新，完成相应的认证、授权和计费工作，并把用户所需的配置信息和计费统计数据返回给 NAS——在这里，NAS 起到了控制接入用户及对应连接的作用，而 RADIUS 协议则规定了 NAS 与 RADIUS 服务器之间如何传递用户配置信息和计费信息。

NAS 和 RADIUS 之间信息的交互是通过将信息承载在 UDP 报文中来完成的。在这个过程中，交互双方将使用密钥对报文进行加密，以保证用户的配置信息（如密码）被加密后才在网络上传递，从而避免它们被侦听、窃取。

2. RADIUS 操作

RADIUS 服务器对用户的认证过程通常需要利用接入服务器等设备的代理认证功能，通常整个操作步骤如下：首先，客户端向 RADIUS 服务器发送请求报文（该报文中包含用户名和加密口令）；然后，客户端会收到 RADIUS 服务器的响应报文，如 ACCEPT 报文、REJECT 报文等（其中，ACCEPT 报文表明用户通过认证；REJECT 报文表明用户没有通过认证，需要用户重新输入用户名和口令，否则访问被拒绝）。

2.1.3 AAA/RADIUS 在以太网交换机中的实现

由前面的概述，我们可以明白，在这样一个 AAA/RADIUS 框架中，Quidway 系列以太网交换机是作为用户接入设备即 NAS，相对于 RAIDUS 服务器来说，Quidway 系列以太网交换机是 RADIUS 系统的客户端；换句话说，AAA/RADIUS 在 Quidway 系列以太网交换机中实现的是其客户端部分。Quidway 系列以太网交换机参与的、使用 RADIUS 认证的组网示意图如下所示。

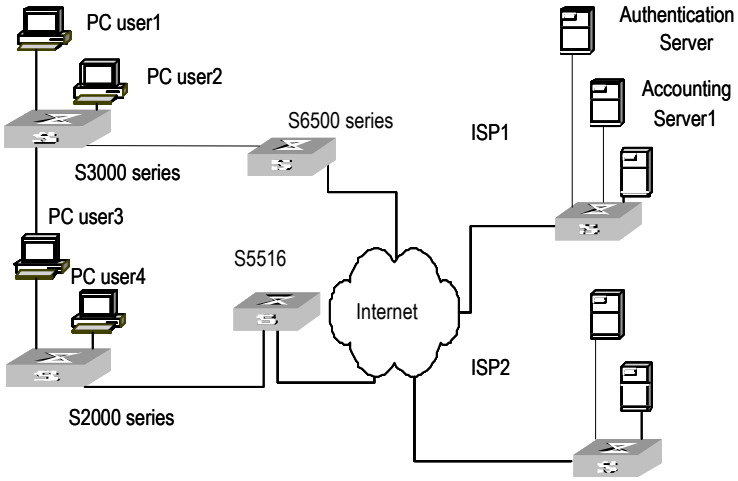

图2-1 使用 RADIUS 认证的典型组网图

2.2 AAA 配置

AAA 的配置包括：

- 创建/删除 ISP 域
- 配置 ISP 域的相关属性
- 创建本地用户
- 设置本地用户的属性
- 强制切断用户连接

在以上的配置任务中，创建 ISP 域是必需的，否则无法区分接入用户的属性；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.2.1 创建/删除 ISP 域

什么是 ISP（Internet Service Provider）域？简单点说，ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 gw20010608@huawei163.net）的用户名中，“@”后的“isp-name”（如例中的“huawei163.net”）即为 ISP 域的域名。在 Quidway 系列以太网交换机对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统就将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 Quidway 系列以太网交换机的 ISP 域视图

下，可以为每个 ISP 域配置包括 AAA 策略（使用的 RADIUS 服务器组等）在内的一整套单独的 ISP 域属性。

对于 Quidway 系列以太网交换机来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。如果某个用户在登录时没有上报 ISP 域名，则系统将把它归于缺省的 ISP 域。

请在系统视图下进行下列配置。

表2-1 创建/删除 ISP 域

操作	命令
创建 ISP 域或进入指定 ISP 域视图	**domain** [*isp-name* | **default** { **disable** | **enable** *isp-name* }]
删除指定的 ISP 域	**undo domain** *isp-name*

缺省情况下，系统中没有任何 ISP 域。

2.2.2 配置 ISP 域的相关属性

ISP 域的相关属性包括引用的 RADIUS 服务器组、ISP 域的状态、可容纳接入用户数的最大数值和用户闲置切断开关设置。其中：

- 引用的 RADIUS 服务器组指定的是该 ISP 域下所有用户所使用的 RADIUS 服务器组的组名。该 RADIUS 服务器组可被用于进行 RADIUS 认证和 RADIUS 计费。缺省情况下，使用缺省的 RADIUS 服务器组。此命令需与 RADIUS 服务器和服务器组的设置命令联合使用，具体请参见本章后面的 RADIUS 配置一节。
- 每个 ISP 域有两种状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；当指示某个 ISP 域处于 block 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。一个 ISP 域在刚被创建时是处于 active 状态的，即：在这个时候，允许任何属于该域的用户请求网络服务。
- 可容纳接入用户数的最大值用来指定该 ISP 域最多可容纳多少个接入用户。缺省情况下，对任何一个 ISP 域，没有任何可容纳接入用户数的限制。
- 用户闲置切断功能是当用户在设定的时间内流量小于设定的流量时，切断该用户的连接。

请在 ISP 域视图下进行下列配置。

表2-2 配置 ISP 域的相关属性

操作	命令
指定引用的 RADIUS 服务器组	**radius-scheme** *radius-scheme-name*
恢复域为默认的 RADIUS 组	**undo radius-scheme**
设置 ISP 域的状态	**state** { **active** | **block** }
指定可容纳接入用户数的最大值	**access-limit** { **disable** | **enable** *max-user-number* }
恢复可容纳接入用户数到缺省设置	**undo access-limit**
设置用户闲置切断	**idle-cut** { **disable | enable** *minute* flow}

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**；其可容纳的接入用户没有数量限制；不设置闲置切断。

2.2.3 创建本地用户

所谓本地用户，是指在 NAS 上设置的一组用户的集合。该集合以用户名为用户的唯一标识。为使某个请求网络服务的用户可以进行本地认证，需要在 NAS 上添加相应的本地用户。

请在系统视图下进行下列配置。

表2-3 创建/删除本地用户

操作	命令
添加本地用户	**local-user** *user-name*
删除所有本地户	**undo local-user all**
删除指定类型的本地用户	**undo local-user** { *user-name* | **all** [**service-type** { **lan-access** | **ftp** | **telnet** }] }

缺省情况下，系统中没有任何本地用户。

2.2.4 设置本地用户的属性

本地用户的属性包括：用户密码、用户状态、用户业务类型等的设置。

请在系统视图下进行下列设置。

表2-4 设置本地用户密码设置方式

操作	命令
设置本地用户密码设定方式	**local-user password-display-mode { cipher-force | auto }**
取消设置的本地用户密码设置方式	**undo local-user password-display-mode**

其中，**auto** 表示按照用户配置的密码显示方式（参考下面表格中 **password** 命令）显示，**cipher-force** 表示所有接入用户的密码显示必须采用密文方式。

请在本地用户视图下进行下列配置。

表2-5 设置/取消指定用户的相关属性

操作	命令
设置指定用户的密码	**password { simple | cipher }** *password*
取消指定用户的密码设置	**undo password**
设置指定用户的状态	**state { active | block }**
取消指定用户的状态	**undo state { active | block }**
设置指定用户的服务类型	**service-type { telnet [level** *level* **] | ftp [ftp-directory** *directory* **] | lan-access }**
取消指定用户的服务类型	**undo service-type { telnet [level] | ftp [ftp-directory] | lan-access }**
服务类型为 lan-access 用户的属性设置	**attribute { ip** *ip-address* **| mac** *mac-address* **| idle-cut** *minute* **| access-limit** *max-user-number* **| vlan** *vlanid* **| location [nas-ip** *ip-address* **] port** *portnum* **}**
取消服务类型为 lan-access 用户的属性设置	**undo attribute { ip | mac | idle-cut | access-limit | vlan | location }**

2.2.5 强制切断用户连接

在某些时候，可能有必要强制切断某个或某类用户的连接。系统提供了下面的命令以实现这个目的。

请在系统视图下进行下列配置。

表2-6 强制切断用户连接

操作	命令
强制切断用户连接	**cut connection** { **all** | **access-type** { **dot1x** | **gcm** } | **domain** *domain-name* | **interface** *portnum* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name* }

2.3 RADIUS 协议配置

Quidway 系列以太网交换机的 RADIUS 协议配置，是以 RADIUS 服务器组为单位进行的。一个 RADIUS 服务器组在实际组网环境中既可以是一台独立的 RADIUS 服务器，也可以是两台配置相同、但 IP 地址不同的主、备 RADIUS 服务器。由于存在上述情况，因此每个 RADIUS 服务器组的属性包括：主服务器的 IP 地址、备份服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

实际上，RADIUS 协议配置仅仅定义了 NAS 和 RADIUS Server 之间进行信息交互所必须的一些参数。为了使这些参数能够生效，还必须在某个 ISP 域视图下指定该域引用配置有上述参数的 RADIUS 服务器组。具体配置命令的细节，请参见前述的“AAA 配置”一节。

RADIUS 协议的配置包括：

- 创建/删除 RADIUS 服务器组
- 设置 RADIUS 服务器的 IP 地址和端口号
- 设置 RADIUS 报文的加密密钥
- 设置 RADIUS 服务器响应超时定时器
- 设置 RADIUS 请求报文的最大传送次数
- 设置实时计费间隔
- 设置允许实时计费请求无响应的最大次数
- 使能停止计费报文缓存功能
- 设置停止计费请求报文的最大发送次数
- 设置支持何种类型的 RADIUS 服务器
- 设置 RADIUS 服务器的状态
- 设置发送给 RADIUS 服务器的用户名格式
- 设置发送给 RADIUS 服务器的数据流的单位
- 配置本机 RADIUS 服务器组

在以上的配置任务中，创建 RADIUS 服务器组、设置 RADIUS 服务器的 IP 地址是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.3.1 创建/删除 RADIUS 服务器组

如前所述，RADIUS 协议的配置是以 RADIUS 服务器组为单位进行的。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 服务器组并进入其视图。

可以使用下面命令创建/删除 RADIUS 服务器组。

请在系统视图下进行下列配置。

表2-7 创建/删除 RADIUS 服务器组

操作	命令
创建 RADIUS 服务器组并进入其视图	**radius scheme** *radius-server-name*
删除 RADIUS 服务器组	**undo radius scheme** *radius-server-name*

一个 RADIUS 服务器组可以同时被多个 ISP 域引用。

缺省情况下，系统中已创建了一个名为“default”的 RADIUS 服务器组，其各项属性均为缺省值。

2.3.2 设置 RADIUS 服务器的 IP 地址和端口号

当创建一个新的 RADIUS 服务器组之后，需要对属于此服务器组的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备份服务器的区别，因此最多可以设置 4 组 IP 地址和 UDP 端口号。不过，至少必须配置一个认证/授权服务器和一个计费服务器，以保证认证/授权和计费工作能够进行。

可以使用下面命令设置 RADIUS 服务器的 IP 地址和端口号。

请在 RADIUS 服务器组视图下进行下列配置。

表2-8 设置 RADIUS 服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 认证/授权或计费服务器的 IP 地址和端口号	**primary** { **accountig | authenticaiton** } *ip-address* [*port-number*]
将主 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值	**undo primary** { **accounting | authentication** }
设置备份 RADIUS 认证/授权或计费服务器的 IP 地址和端口号	**secondary** { **accounting | authentication** } *ip-address* [*port-number*]
将备份 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值	**undo secondary** { **accounting | authentication** }

在实际组网环境中，上述参数的设置需要根据具体需求来决定。例如：可以指定 4 组不同的数据以映射 4 台不同的 RADIUS 服务器；也可以指定两台服务器互为认证/授权和计费服务的主、备（即 A 作为主认证/授权服务器和备份计费服务器、B 作为备份认证/授权服务器和主计费服务器）；当然，也可以把这 4 组数据设置得完全一样，使其对应的服务器既作为认证/授权服务器，又作为计费服务器；同时，既作为主服务器，又作为备份服务器。

为了保证 NAS 与 RADIUS 服务器能够正常交互，在设置 RADIUS 服务器的 IP 地址和 UDP 端口之前，必须确保 RADIUS 服务器与 NAS 的路由连接正常。此外，由于 RADIUS 协议采用不同的 UDP 端口来收发认证/授权和计费报文，因此必须将认证/授权端口号和计费端口号设置得不同。RFC2138/2139 中建议的认证/授权端口号为 1812、计费端口号为 1813，但是也可以不选用 RFC 建议值（尤其是比较早期的 RADIUS Server，普遍采用 1645 作为认证/授权端口号、1646 作为计费端口号）。

在使用中，请保证 Quidway 系列以太网交换机上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。一般情况下 RADIUS 服务器的计费端口号为 1813，认证/授权端口号为 1812。

缺省情况下，主、备认证/授权和计费服务器的 IP 地址均为 0.0.0.0；其认证/授权服务的 UDP 端口号为 1812，计费服务的 UDP 端口号为 1813。

2.3.3 设置 RADIUS 报文的加密密钥

RADIUS 客户端（即交换机系统）与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，双方通过设置加密密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。

可以使用下面命令设置 RADIUS 报文的加密密钥。

请在 RADIUS 服务器组视图下进行下列配置。

表2-9 设置 RADIUS 报文的加密密钥

操作	命令
设置 RADIUS 认证/授权报文的加密密钥	**key authentication** *string*
恢复 RADIUS 认证/授权报文加密密钥为缺省	**undo key authentication**
设置 RADIUS 计费报文的加密密钥	**key accounting** *string*
恢复 RADIUS 计费报文加密密钥为缺省	**undo key accounting**

缺省情况下，RADIUS 认证/授权报文和 RADIUS 计费报文的加密密钥均为“huawei”。

2.3.4 设置 RADIUS 服务器响应超时定时器

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务。

可以使用下面命令设置 RADIUS 服务器响应超时定时器。

请在 RADIUS 服务器组视图下进行下列配置。

表2-10 设置 RADIUS 服务器响应超时定时器

操作	命令
设置 RADIUS 服务器响应超时定时器	**timer** *second*
将 RADIUS 服务器响应超时定时器恢复为缺省值	**undo timer**

缺省情况下，RADIUS 服务器响应超时定时器为 3 秒。

2.3.5 设置 RADIUS 请求报文的最大传送次数

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数超过最大传送次数而 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

可以使用下面命令设置 RADIUS 请求报文的最大传送次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-11 设置 RADIUS 请求报文的最大传送次数

操作	命令
设置 RADIUS 请求报文的最大传送次数	**retry** *retry-time*
将 RADIUS 请求报文的最大传送次数恢复为缺省值	**undo retry**

缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

2.3.6 设置实时计费间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 RADIUS 服务器组视图下进行下列配置。

表2-12 设置实时计费间隔

操作	命令
设置实时计费间隔	**timer realtime-accounting** *minute*
将实时计费间隔恢复为缺省值	**undo timer realtime-accounting**

其中，*minute* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-13 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥1000	≥15

缺省情况下，实时计费间隔为 12 分钟。

2.3.7 设置允许实时计费请求无响应的最大次数

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户计费。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。Quidway 系列以太网交换机提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

可以使用下面的命令设置允许实时计费请求无响应的最大次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-14 设置允许实时计费请求无响应的最大次数

操作	命令
设置允许实时计费请求无响应的最大次数	**retry realtime-accounting** *retry-times*

考虑一下该值如何计算：假设 RADIUS 服务器的连接超时时长为 T，NAS 的实时计费间隔为 t，则 NAS 的 *count* 应取为 T 除以 t 后取整的数值。因此，在实际应用中，应尽量将 T 设置为一个能被 t 整除的数。

缺省情况下，最多允许 5 次实时计费请求无响应。

2.3.8 使能停止计费报文缓存功能

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 Quidway 系列以太网交换机发出的停止计费请求报文没有响应，以太网交换机应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置交换机允许停止计费报文缓存功能。

请在 RADIUS 服务器组视图下进行下列配置。

表2-15 设置使能停止计费报文缓存功能

操作	命令
使能停止计费报文缓存功能	**stop-accounting-buffer enable**
关闭停止计费报文缓存功能	**undo stop-accounting-buffer enable**

缺省情况下，使能停止计费报文缓存功能。

2.3.9 停止计费报文最大重发次数设置

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 Quidway 系列以太网交换机发出的停止计费请求报文没有响应，以太网交换机应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置缓存后的报文的最大重发次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-16 停止计费报文最大重发次数

操作	命令
停止计费报文最大重发次数	**retry stop-accounting** *retry-time*
关闭停止计费报文最大重发次数	**undo retry stop-accounting**

缺省情况下，最多可以将缓存的停止计费请求报文重发 500 次。

2.3.10 设置支持何种类型的 RADIUS 服务器

Quidway 系列以太网交换机同时支持标准的 RADIUS 协议和华为公司自行开发的 IP Hotel、201+、Portal 等扩展 RADIUS 业务平台。

可以使用下面的命令来选择支持何种 RADIUS 服务器类型。

请在 RADIUS 服务器组视图下进行下列配置。

表2-17 设置支持何种类型的 RADIUS 服务器

操作	命令
设置支持何种类型的 RADIUS 服务器	**server-type** { **huawei** | **iphotel** | **portal** | **standard** }

缺省情况下，RADIUS 服务器的类型为 **standard**。

2.3.11 设置 RADIUS 服务器的状态

对于某个 RADIUS 服务器组中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障与 NAS 的通信中断时，NAS 会主动地转而与备份服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备份服务器通信；直到备份服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过下面的命令手工将主服务器的状态设为 **active**。

当主服务器与备份服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

请在 RADIUS 服务器组视图下进行下列配置。

表2-18 设置 RADIUS 服务器的状态

操作	命令
设置主 RADIUS 认证/授权服务器的状态	**state primary authentication { block | active }**
设置主 RADIUS 计费服务器的状态	**state primary accounting { block | active }**
设置备份 RADIUS 认证/授权服务器的状态	**state secondary authentication { block | active }**
设置备份 RADIUS 计费服务器的状态	**state secondary accounting { block | active }**

缺省情况下，RADIUS 服务器组中各 RADIUS 服务器的状态均为 **active**。

2.3.12 设置发送给 RADIUS 服务器的用户名格式

如前所述，接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，Quidway 系列以太网交换机就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，Quidway 系列以太网交换机提供下面的命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

表2-19 设置发送给 RADIUS 服务器的用户名格式

操作	命令
设置发送给 RADIUS 服务器的用户名格式	**user-name-format { with-domain | without-domain }**

📖 说明：

如果指定某个 RADIUS 服务器组不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 服务器组，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

缺省情况下，RADIUS 服务器组默认：发送给 RADIUS 服务器的用户名携带有 ISP 域名。

2.3.13 设置发送给 RADIUS 服务器的数据流的单位

Quidway 系列以太网交换机提供下面的命令以指定发送给 RADIUS 服务器的数据流的单位。

表2-20 设置发送给 RADIUS 服务器的数据流的单位

操作	命令
设置发送给 RADIUS 服务器的数据流的单位	**data-flow-format data [byte | giga-byte | kilo-byte | mega-byte] packet [giga-packet | kilo-packet | mega- packet | one-packet]**
恢复发送到 RADIUS 服务器的数据流的单位为缺省设置	**undo data-flow-format**

缺省情况下，RADIUS 服务器组默认的发送数据单位为 byte，数据包的单位为 one packet。

2.3.14 配置本机 RADIUS 服务器组

华为 Quidway 系列交换机除了支持如前所述的传统的作为 RADIUS 客户端的服务——即分别采用认证/授权服务器、计费服务器的方式进行用户的认证管理外，还提供了本机的简单 RADIUS 服务器端功能（包括认证和授权），称之为本机 RADIUS 服务器功能，Quidway 系列交换机最多可以支持 16 个本机 RADIUS 服务器组。

可以使用下面命令来配置本机 RADIUS 服务器。

请在系统视图下进行下列配置。

表2-21 配置本机 RADIUS 服务器

操作	命令
创建本机 RADIUS 服务器	**local-sever nas-ip** *ip-address* **key** *password*
删除本机 RADIUS 服务器	**undo local-server nas-ip** *ip-address.*

缺省情况下，本机 RADIUS 服务器组默认的 IP 地址为 127.0.0.1，默认的密码为 huawei。

需要注意的，采用华为公司的本机 RADIUS 服务器功能时，认证服务的 UDP 端口号为 1645，授权服务的 UDP 端口号为 1646。

2.4 AAA 和 RADIUS 协议的显示和调试

完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 AAA、RADIUS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除 AAA、RADIUS 相关配置。

在用户视图下，执行 **debugging** 命令可对 AAA、RADIUS 进行调试。

表2-22 AAA 和 RADIUS 协议的显示和调试

操作	命令
显示所有或指定 ISP 域的配置信息	**display domain** [*isp-name*]
显示用户连接的相关信息	**display connection** [**access-type** { **dot1x** | **gcm** } | **domain** *isp-name* | **interface** *portnum* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name*]
显示本地用户的相关信息	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **service-type** { **telnet** | **ftp** | **lan-access** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlanid*]
显示本机 RADIUS 服务器组的相关信息	**display local-server statistics**
显示所有或指定 RADIUS 服务器组的配置信息	**display radius** [*radius-server-name*]

操作	命令
显示 RADIUS 报文的统计信息	**display radius statistics**
显示缓存的没有得到响应的停止计费请求报文	**display stop-accounting-buffer** { **radius-scheme** *radius-server-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
打开 RADIUS 报文调试开关	**debugging radius packet**
关闭 RADIUS 报文调试开关	**undo debugging radius packet**
打开本机 RADIUS 服务器组调试开关	**debugging local-server** { **all** | **error** | **event packet** }
关闭本机 RADIUS 服务器组调试开关	**undo debugging local-server** { **all** | **error** | **event packet** }

2.5 AAA 和 RADIUS 协议典型配置举例

AAA/RADIUS 协议与 802.1x 协议配合使用的例子，请参见“802.1x 配置”一章的“典型配置举例”部分，此处不再赘述。

2.5.1 FTP/Telnet 用户远端 RADIUS 服务器认证配置

📖 说明：

Telnet 用户与 FTP 用户的远端服务器认证配置方法类似，下面描述以 Telnet 用户的远端认证为例。

1. 组网需求

如下图所示的环境中，通过对交换机的配置实现 RADIUS 服务器对登录交换机的 Telnet 用户的远端认证。

其中：由一台 RADIUS 服务器（其担当认证 RADIUS 服务器的职责）与交换机相连，服务器 IP 地址为 10.110.91.146，设置交换机与认证 RADIUS 服务器交互报文时的加密密码为“expert”，设置交换机从用户名中去除用户域名后再将之传给 RADIUS 服务器。

2. 组网图

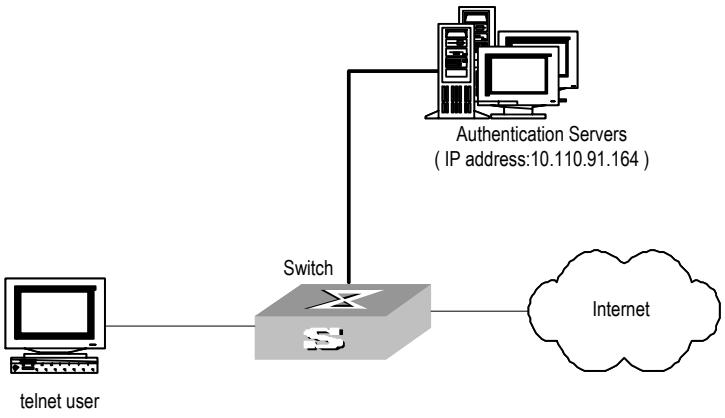

图2-2 配置 Telnet 用户的远端 RADIUS 认证

3. 配置步骤

添加 Telnet 用户。

此处略。

📖 说明：

FTP、Telnet 用户的一些配置请参考《Quidway S5516 以太网交换机 操作手册》的“入门操作”部分“用户界面配置”相关内容。

配置 Telnet 用户采用远端认证方式，即 scheme 方式。

[Quidway-ui-vty0-4] authentication-mode scheme

配置 domain。

[Quidway] domain cams

[Quidway-isp-cams] quit

配置 RADIUS 方案。

[Quidway] radius scheme cams

[Quidway-radius-cams] primary authentication 10.110.91.146 1812

[Quidway-radius-cams] key authentication expert

[Quidway-radius-cams] server-type Huawei

[Quidway-radius-cams] user-name-format without-domain

配置 domain 和 RADIUS 的关联。

[Quidway-radius-cams] quit

[Quidway] domain cams

[Quidway-isp-cams] radius-scheme cams

2.5.2 FTP/Telnet 用户本地 RADIUS 服务器认证配置

Telnet/FTP 用户的本地 RADIUS 认证方法与 2.5.1 小节中的远端 RADIUS 认证方法类似，只需要将 2.5.1 小节中“配置 RADIUS 方案”中的服务器 IP 地址修改为 127.0.0.1，认证密码修改为 huawei，认证服务的 UDP 端口号修改为 1645 即可。

📖 **说明：**

Telnet/FTP 用户的本地 RADIUS 认证的一些知识，可参考“2.3.14 配置本机 RADIUS 服务器组”的相关内容。

2.6 AAA 和 RADIUS 协议故障的诊断与排除

RADIUS 协议在 TCP/IP 协议族中处于应用层，它主要规定 NAS 与 ISP 的 RADIUS 服务器间如何交互用户信息，因此它失效的可能性比较大。

- 故障之一：用户认证/授权总是失败

故障排除：

(1) 用户名不是“userid@isp-name”的形式，或 NAS 没有指定缺省的 ISP 域——请使用正确形式的用户名或在 NAS 中设定缺省的 ISP 域。

(2) RADIUS 服务器的数据库中没有配置该用户——检查 RADIUS 服务器的数据库以保证该用户的配置信息确实存在。

(3) 用户侧输入的密码不正确——请保证接入用户输入正确的密码。

(4) RADIUS 服务器和 NAS 的报文加密密码不同——请仔细比较两端的加密密钥，确保它们相同。

(5) NAS 与 RADIUS 服务器之间存在通信故障（可以通过在 NAS 上 ping RADIUS 服务器来检查）——请保证 NAS 与 RADIUS 服务器之间能够正常通信。

- 故障之二：RADIUS 报文无法传送到 RADIUS 服务器

故障排除：

(1) NAS 与 RADIUS 服务器之间的通信线路不通（物理层/链路层）——请保证线路通畅。

(2) NAS 上没有设置相应的 RADIUS 服务器 IP 地址——请保证正确设置 RADIUS 服务器的 IP 地址。

(3) 认证/授权和计费服务的 UDP 端口设置得不正确——请保证与 RADIUS 服务器提供的端口号一致。

- 故障之三：用户认证通过并获得授权，但是不能向 RADIUS 服务器传送计费话单。

故障排除：

(1) 计费端口号设置得不正确——请正确设置 RADIUS 计费端口号。

(2) 计费服务器和认证/授权服务器不是同一台机器，NAS 却要求认证/授权和计费在同一个服务器（IP 地址相同）——请保证 NAS 的认证/授权和计费服务器的设置与实际情况相同。