

NAS 接入服务用户手册

北京港湾网络有限公司
北京市海淀区西三环北路 21 号久凌大厦
邮编：100089
电话：010-88512088 010-88512099
传真：010-68405011 010-68473171
E-mail: customer@harbournetworks.com
<http://www.harbournetworks.com>
版权所有，不得翻录

声明

本手册总体上较为全面地包含港湾网络有限公司 NAS 接入服务的功能特性和配置内容，如遇到某些临时变化，或针对用户的某些特殊需求而采取的一些特殊变动，港湾公司保留继续使用该手册，并以其他方式通知用户的权利。

本手册及相关文档的信息受到版权保护，手册的任何部分未经港湾网络公司书面许可不得复制或传播，违者必究。

P-20030325-100

前言

随着宽带以太网建设规模的迅速扩大，网络上原有的认证系统已经不能很好的适应用户数量急剧增加和宽带业务多样性的要求。而 IEEE 802.1x 协议是目前业界最新的标准认证协议，一经推出就引起了广大网络设备制造商的重视，各大厂商纷纷组织研发力量进行基于 802.1x 协议相关产品的开发。北京港湾网络有限公司在业内率先实现了 802.1x 协议的商用化，使其在宽带以太网中被成功应用。同时，港湾公司又对 802.1x 协议的认证方式和认证体系结构进行了优化，并在 BigHammer、FlexHammer、IP-DSLAM 等系列设备中内置了 802.1x 认证系统。


为了使用户更好地了解接入服务在港湾网络公司以太网设备上的应用和配置，我们编写了此手册，它将协助您完成对网络接入、认证、计费等方面的配置和管理，同时也可作为您了解接入服务的参考资料。

组织方式

本手册主要由以下几个部分组成：

章	题目	内容描述
第 1 章	接入服务——NAS	介绍接入服务概念和原理、802.1x 协议以及 Radius 认证技术
第 2 章	接入服务配置命令详解	详细介绍港湾网络公司接入服务配置命令的功能和使用方法
第 3 章	接入服务应用配置实例	列举几种典型的配置实例作为用户在实际配置过程中的参考
附录	接入服务命令集	提供接入服务配置命令列表

图标说明

图标	作用
	提示用户需要注意的地方

读者范围

本手册适用于具有一定网络接入服务知识、且需要通过港湾网络公司以太网设备实现 Radius 认证计费功能的用户或系统管理员。如果您已经熟悉以下知识，将对理解并使用本手册提供很大帮助：

- 局域网（Local Area Networks）（LANs）
- 以太网概念（Ethernet Concepts）
- 以太网交换和桥概念（Ethernet Switching and Bridging Concepts）
- 网络协议概念（Internet Protocol Concepts）

- IP 多播概念 (IP Multicast Concepts)
- 802.1x协议
- Radius认证技术

目 录

第 1 章 接入服务	1
1.1 NAS 概述	1
1.2 802.1x 协议	4
1.2.1 802.1x 体系结构	4
1.2.2 802.1x 认证机制	6
1.2.3 协议实现内容	8
1.3 Radius 认证技术	10
第 2 章 接入服务配置命令详解	11
2.1 802.1x 配置命令	11
2.1.1 使能/关闭 802.1x 认证服务	11
2.1.2 配置协议参数	11
2.1.3 配置对端口的 802.1x 控制	12
2.1.4 设置用户绑定功能	13
2.1.5 设置重新认证机制	14
2.1.6 设置异常下线检测机制 (keepalive)	15
2.1.7 强制用户退出认证状态	16
2.1.8 清除 802.1x 统计信息	18
2.1.9 配置基于 802.1x 的动态限速功能	18
2.2 802.1x 显示命令	20
2.3 Radius 配置命令	21
2.3.1 配置 Radius 认证服务	21
2.3.2 配置 Radius 计费服务	24
2.3.3 设置 Radius CUT 功能	26
2.3.4 配置 Session Timeout 处理机制	28
2.3.5 配置 Radius Server 主备切换功能	28
2.3.6 配置 Radius 属性	29
2.3.7 配置实例	35
2.4 Radius 显示命令	36
2.5 配置域	36
2.5.1 域的基本配置	37
2.5.2 域的认证配置	38
2.5.3 域的计费配置	39
2.5.4 配置实例	41
第 3 章 接入服务应用配置实例	42
3.1 单域认证	42
3.2 多域认证	43
3.3 服务器的主备切换	44
3.4 基于 802.1x 的动态限速	46
附录 接入服务命令集	48

第1章 接入服务

1.1 NAS 概述

随着宽带以太网建设规模的迅速扩大,为了适应用户数量急剧增加和宽带业务多样性的要求,港湾网络公司通过在 Hammer 系列交换机上嵌入接入服务来完备用户的认证和管理功能,以便更好地支持宽带网络的计费、安全、运营和管理的要求。嵌入了接入服务的 Hammer 交换机称为网络访问服务器 (Network Access Server, NAS)。

接入服务在运用 802.1x 协议和 Radius 协议的基础上,实现对用户接入的认证和管理功能。使用接入服务主要有以下优点:

- **简洁高效:** 纯以太网技术内核,保持IP网络无连接特性,去除冗余昂贵的多业务网关设备,消除网络认证计费瓶颈和单点故障,易于支持多业务;
- **容易实现:** 可在普通L3、L2、IP DSLAM上实现,网络综合造价成本低;
- **安全可靠:** 在二层网络上实现用户认证,并可以通过设备实现MAC、端口、账户和密码等绑定技术,具有很高的安全性;
- **易于运营:** 控制流和业务流完全分离,易于实现多业务运营。

接入服务在运用 802.1x 基于端口的访问控制协议的基础上扩展了该协议,实现了基于用户 MAC 地址的访问控制,可以对设备一个端口上的多个接入用户分别进行认证和管理,提供对用户接入的灵活控制。同时能够与动态主机配置协议中继代理(DHCP Relay)相结合,为计费服务器提供用户的 IP 地址。

接入服务提供 3 种身份验证方式: PAP, CHAP 和 EAP-MD5 方式,根据业务运营的不同需求,可以使用其中任何一种身份验证方式实现接入服务:

1. 使用 PAP 方式进行身份验证

如图 1-1 所示,首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务,交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端,要求用户提供身份标识,用户终端返回 EAP-RESPONSE/IDENTITY 响应报文表示连接建立。然后交换机发送 EAP-REQUEST/PAP 报文通知用户使用 PAP 方式验证身份,用户终端发送 EAP-RESPONSE/PAP 报文到交换机,该报文中含有用户名和用户密码。交换机根据来自用户终端的 EAP-RESPONSE/PAP 报文组装并发送 ACCESS REQUEST 报文到 Radius 服务器。Radius 服务器对用户进行认证,如果认证通过,返回 ACCESS ACCEPT 报文给交换机,由交换机完成相应操作以允许用户接入,同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

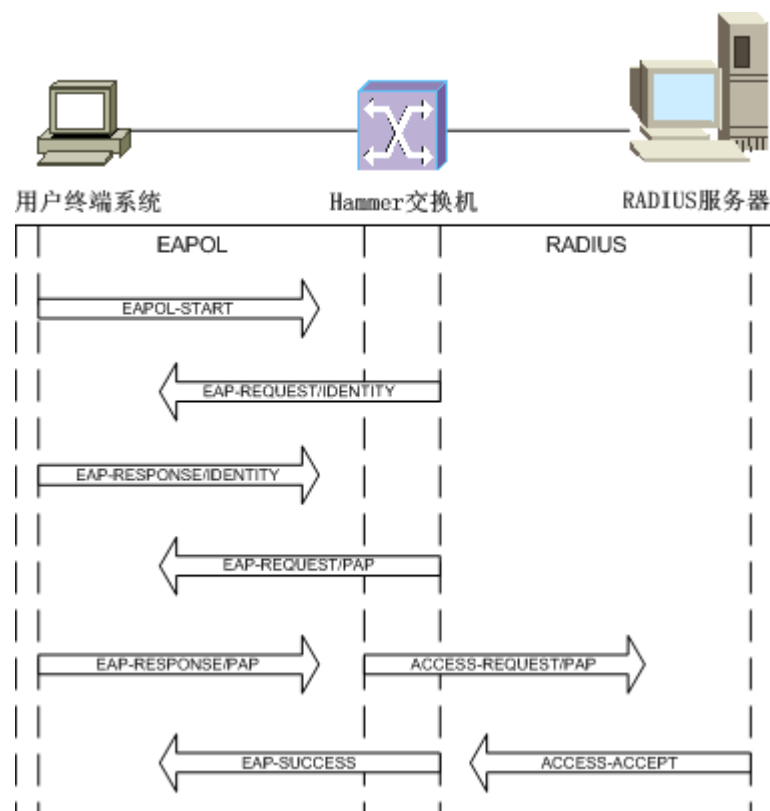


图 1-1 使用 PAP 方式进行身份验证的过程

2. 使用 CHAP 方式进行身份验证

如图 1-2 所示, 首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务, 交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端, 要求用户提供身份标识, 用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后交换机生成 challenge 信息, 并发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 CHAP 方式验证身份, 用户终端返回 EAP-RESPONSE/MD5-CHALLENGE 响应报文给交换机。交换机根据来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文组装并发送 ACCESS REQUEST 报文送到 Radius 服务器。Radius 服务器对用户进行认证, 如果认证通过, 返回 ACCESS ACCEPT 报文给交换机, 由交换机完成相应操作以允许用户接入, 同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

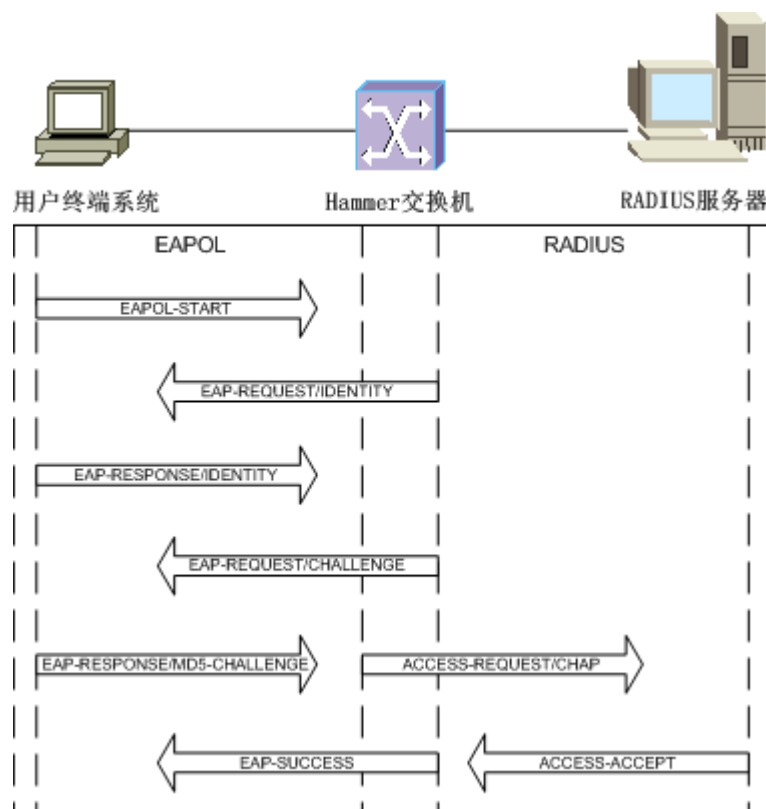


图 1-2 使用 CHAP 方式进行身份验证的过程

3. 使用 EAP-MD5 方式进行身份验证

如图 1-3 所示, 首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务, 交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端, 要求用户提供身份标识, 用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后由交换机发送 ACCESS-REQUEST 到 Radius 服务器, Radius 服务器生成 challenge 信息, 并将 ACCESS-CHALLENGE 报文发送给交换机。接下来, 交换机向用户终端发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 EAP-MD5 方式验证身份, 终端返回 EAP-RESPONSE/MD5-CHALLENGE 报文作为响应。交换机将来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文封装到 ACCESS REQUEST 报文中, 并发送到 Radius 服务器。Radius 服务器对用户进行认证, 如果认证通过, 则返回 ACCESS ACCEPT 报文给交换机, 由交换机完成相应操作以允许用户接入, 同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

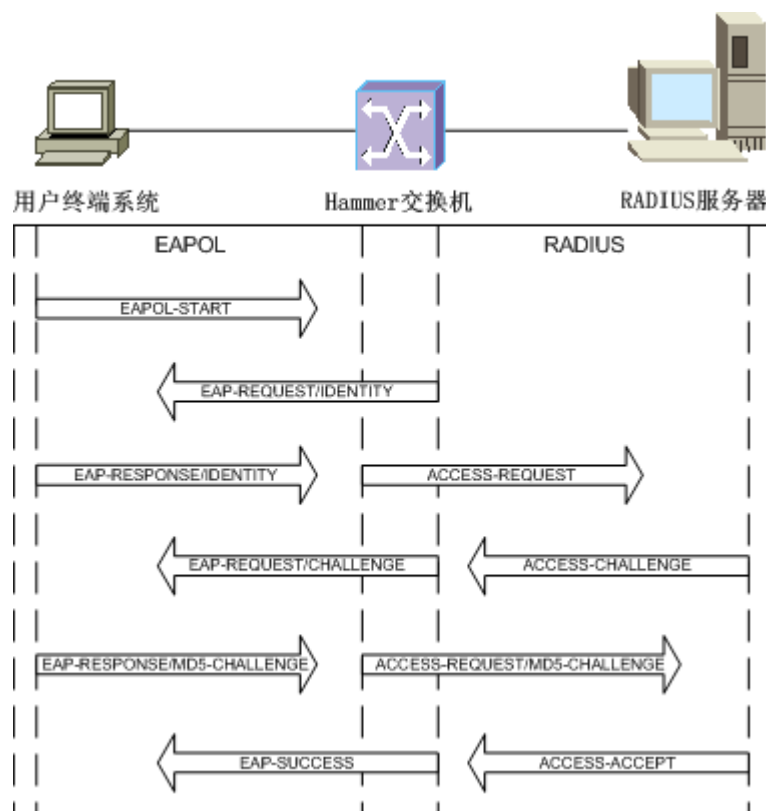


图 1-3 使用 EAP-MD5 方式进行身份验证的过程

1.2 802.1x 协议

在 IEEE 802 所定义的局域网环境中，只要存在物理的接口，未经授权的网络设备就可以直接或通过连接到局域网的设备进入局域网。随着局域网技术的广泛应用，在很多网络环境中，往往不希望有未经授权的设备或用户连接到网络，使用网络提供的资源和服务。特别是在运营网络中的应用，对其安全认证的要求已经提到了议事日程上。如何既能够利用局域网技术简单、廉价的组网特点，同时又能够对用户或设备访问网络的合法性提供认证，是目前业界讨论的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE 802.1x 称为基于端口的访问控制协议 (Port based network access control protocol)，该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。这里的端口是指连接到 LAN 的一个单点结构，可以是认证系统的 MAC 地址，也可以是服务器或网络设备上连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。

1.2.1 802.1x 体系结构

IEEE 802.1x 协议的体系结构包括三个重要的组成部分：Supplicant 客户端、Authenticator System 认证系统、Authentication Server 认证服务器。下图描述了三者之间的关系以及相互之间的通信。

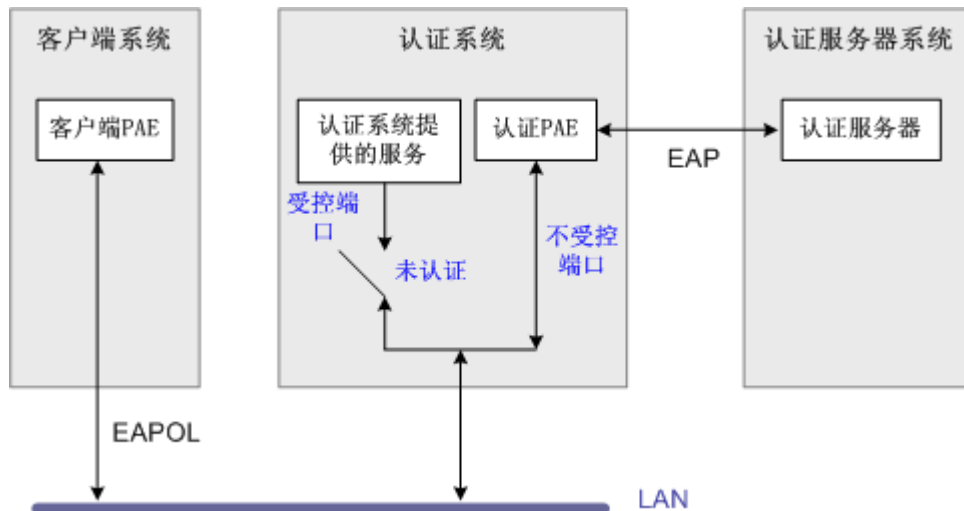


图 1-4 IEEE 802.1x 认证体系结构

客户端系统一般指用户终端系统，该终端系统通常需要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

认证系统通常指那些支持 802.1x 协议的网络设备，如港湾网络公司的 Hammer 系列交换机和无线访问点设备。支持 802.1x 协议的网络设备对应不同的用户端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控（Controlled Port）端口和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终能够发出或接受认证。受控端口只有在认证通过的状态下才可打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，用户无法访问认证系统提供的服务。图 1-4 中认证系统的受控端口处于未认证状态，因此客户端无法访问认证系统提供的服务。

PAE 是端口访问实体 (Port Access Entity), 分为客户端 PAE 和认证系统 PAE:

- 客户端PAE：位于客户端，主要负责响应来自认证系统建立信任关系的请求。
- 认证系统PAE：位于认证系统，负责与客户端的通信，把从客户端收到的信息传送给认证服务器以完成认证。

认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信,二者之间运行 EAPOL 协议。
认证系统的 PAE 与认证服务器之间运行 EAP (Extensible Authentication Protocol) 协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时，两个实体之间的通信就可以不采用 EAP 协议。

认证服务器通常为 Radius 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。

图 1-4 描述了终端用户的认证机制，对于网络设备之间的认证也是一样。例如：当一个

网络设备 A 要求访问网络设备 B 所提供的服务时，系统 A 的 PAE 就成为客户端（Suppliant），系统 B 的 PAE 为认证系统（Authenticator）；如果 B 要求访问 A 所提供的服务时，B 的 PAE 就成为客户端，A 的 PAE 就成为认证系统。

1.2.2 802.1x 认证机制

802.1x 作为一种认证协议，在实现的过程中有很多重要的工作机制，这里我们主要介绍其中四种机制：

- 认证发起机制
- 退出认证机制
- 重新认证机制
- 认证报文丢失重传机制

1. 认证发起机制

认证的发起可以由用户主动发起，也可以由认证系统发起。当认证系统探测到有未经过认证的用户使用网络时，就会主动发起认证。用户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

◎ 由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制为未认证状态。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request 报文后，将发送 EAP-Response 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

◎ 由客户端发起认证

如果用户要上网，则可以通过客户端软件向认证系统发送 EAPOL-Start 报文主动发起认证。认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

2. 退出认证机制

有以下几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态：

- a) 客户端未通过认证服务器的认证
- b) 管理性的控制端口始终处于未认证状态
- c) 与端口对应的 MAC 地址出现故障（管理性禁止或硬件故障）

- d) 客户端与认证系统之间的连接失败，造成认证超时
- e) 重新认证超时
- f) 客户端未响应认证系统发起的认证请求
- g) 客户端发送 EAPOL-Logoff 报文，主动下线

退出已认证状态的直接结果就是导致用户下线，如果用户要继续上网则要再发起一个认证过程。为什么要专门提供一个 EAPOL-Logoff 机制呢？主要是出于如下安全的考虑：当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的登录请求，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

3. 重新认证机制

为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名和密码。

重新认证由认证系统发起，时间是从最近一次成功认证后算起。交换机上的重新认证功能可以激活或关闭，默认情况下是关闭的。重新认证的时间默认值为 3600 秒（一个小时）。

注意：

重新认证的时间设定需要认真的规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

4. 认证报文丢失重传机制

对于认证系统和客户端之间通信的 EAP 报文，如果发生丢失，由认证系统负责进行报文的重传，通过一个超时计数器来完成对重传时间的设定。考虑到网络的实际环境，一般认为认证系统和客户端之间报文丢失的几率比较低，且传送延迟低，因此设定默认的重传时间为 30 秒钟。

由于对用户身份合法性的认证最终由认证服务器执行，因此认证系统和认证服务器之间的报文丢失重传也很重要，我们通过建立另一个超时计数器来实现对认证系统和认证服务器之间重传报文时间的设定。

另外需要注意的是，如果客户端需要通过 DHCP Server 动态获取 IP 地址，那么在执行 802.1x 认证过程中，只有客户端认证通过后，才会有 DHCP 发起和 IP 地址分配的过程。对于未通过认证的客户端，其所连接的认证系统的端口将丢弃任何 DHCP 请求报文。

1.2.3 协议实现内容

802.1x 协议在实现整个安全认证的过程中，其三个关键部分（客户端、认证系统、认证服务器）之间是通过通信协议进行交互的，因此有必要对其相关的通信协议做一介绍。

EAP 协议

802.1x 协议采用 EAP 协议在客户端、认证系统和认证服务器之间进行通信。EAP（Extensible Authentication Protocol 扩展的认证协议，RFC 2284）是 PPP 认证的一个通用协议，支持多种认证机制。EAP 在链路控制（LCP）阶段并不选择好一种认证机制，而是把这一步推迟到认证阶段，这就允许认证系统在确定某种特定认证机制之前请求更多的信息。

通过支持 EAP 协议，认证系统只需控制其受控端口的状态，而并不干涉通过非受控端口在客户端和认证服务器之间传递的认证信息，这样可实现认证流和业务流的完全分离。可以使用认证服务器来实现各种认证机制，认证系统仅仅需要传送认证信息，并根据认证返回的结果控制受控端口的状态。

EAP 帧结构如图 1-5 所示：

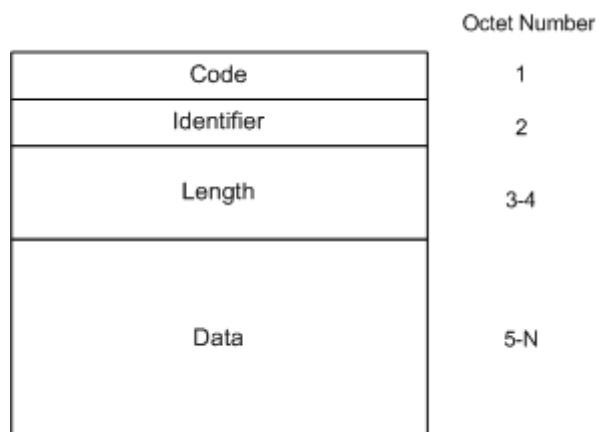


图 1-5 EAP 帧结构

EAP 帧格式中各字段含义如下：

字段	占用字节数	描述
Code	1 个字节	表示 EAP 帧的四种类型： 1. Request 2. Response 3. Success 4. Failure
Identifier	1 个字节	用于匹配 Request 和 Response。 Identifier 的值和系统端口一起单独标识一个认证过程
Length	2 个字节	表示 EAP 帧的总长度
Data	0 或更多字节	表示 EAP 数据

EAPOL 协议

EAPOL 是 EAP 协议在 802.3/以太网上的一种封装技术，称为 EAP over LANs（局域网上的扩展认证协议），主要用于在客户端和认证系统之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。

EAPOL 帧结构如图 1-6 所示：

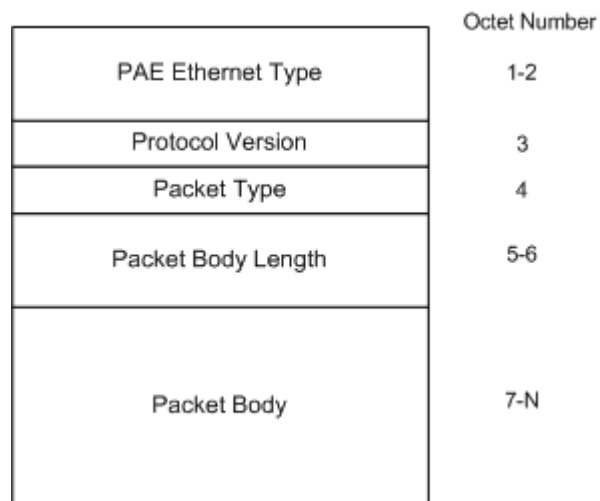


图 1-6 EAPOL 帧结构

EAPOL 帧格式中各字段含义如下：

字段	占用字节数	描述
PAE Ethernet Type	2 个字节	表示协议类型，802.1x 分配的协议类型为 888E
Protocol Version	1 个字节	表示 EAPOL 帧的发送方所支持的协议版本号。本规范使用值为 0000 0001
Packet Type	1 个字节	表示传送的帧类型，如下几种帧类型： <ul style="list-style-type: none"> a) EAP-Packet. 值为 0000 0000，表示为 EAP 帧 b) EAPOL-Start. 值为 0000 0001，表示为 EAPOL-Start 帧 c) EAPOL-Logoff. 值为 0000 0010，表示为 EAPOL-Logoff 请求帧 d) EAPOL-Key. 值为 0000 0011，表示为 EAPOL-Key 帧。 e) EAPOL-Encapsulated-ASF-Alert. 值为 0000 0100
Packet Body Length	2 个字节	表示 Packet Body 的长度
Packet Body	0 或更多字节	如果 Packet Type 为 EAP-Packet、EAPOL-Key

或 EAPOL-Encapsulated-ASF-Alert 的值，则 Packet Body 取相应的值；对于其他帧类型，该值为空。

EAPOL 帧在传送过程中不携带 802.1q 的 VLAN 标记，但是可以携带 802.1p 优先级标记。所有的 PAE 都能够接收带或不带优先级标记的 EAPOL 帧。

EAPOL 帧在二层传送时，必须要有目标 MAC 地址，当客户端和认证系统彼此之间不知道发送的目标时，其目标 MAC 地址使用由 802.1x 协议分配的组播地址 01-80-c2-00-00-03。

1.3 Radius 认证技术

Radius 的全称为（Remote Access Dial-In User Service），它是对远程拨号用户访问进行认证的一种协议，是在 Radius Server 和 Radius Client 之间进行认证、授权、计费的协议标准。认证即辨别用户是谁的过程，通常该过程通过输入有效的用户名和密码实现；授权是指对完成认证过程的用户授予相应权限，解决他能做什么的问题，在一些身份认证的实现中，认证和授权是统一在一起的；计费（Accounting）则是统计用户做过什么的过程，包括用户使用的时间和费用，可通过用户占用系统的时间、接收和发送的信息量来衡量。

Radius 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责将用户信息传送到指定的 Radius 服务器上，并根据服务器返回的结果进行相应的处理。Radius 服务器包括两种类型：授权认证服务器和计费服务器。授权认证服务器（Radius Authentication Server）负责接受用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器也可以作为 Radius 客户的代理，将其连接到另一个授权认证服务器。计费服务器（Radius Accounting Server）负责接受用户计费开始请求和计费结束请求，并实现计费功能。

Radius 具有以下属性：

- Radius 以 Client/Server 模式工作，实现了对远程用户的身份认证、授权和计费功能。
- Radius Client 主要用来将用户信息传递给 Radius Server；Server 则对用户进行认证，并返回用户的配置信息。
- 为保证传输的安全性，在 Client 和 Server 之间传送的数据均以 MD5 方式加密。
- 认证具有灵活性。采取多种认证机制，包括 PAP 和 CHAP。

第2章 接入服务配置命令详解

2.1 802.1x 配置命令

2.1.1 使能/关闭 802.1x 认证服务

使能/关闭 802.1x 认证服务，使用以下配置命令：

```
config dot1x [enable|disable]
```

选择 enable 表示使能 802.1x 认证服务，选择 disable 表示关闭 802.1x 认证服务。

例如：使能 802.1x 认证服务

```
Harbour(config)# config dot1x enable
```

2.1.2 配置协议参数

802.1x 端口访问控制协议通过在客户端系统和认证系统之间传递 EAPOL 数据包、在认证系统和认证服务器之间传递 Radius 数据包实现访问控制，在传递数据包的过程中有如下的计时属性：

quietPeriod：是指在一次认证失败后多长时间内认证系统不接收来自客户端系统的认证请求，这项功能可以防止一些不良用户试图不停的进行认证。

TxPeriod：认证系统在某个指定的时间内如果没有收到客户端系统的回复，便会重发 EAP-Request/Identity 数据帧到客户端，TxPeriod 便是这个指定的重传 EAP-Request/Identity 数据帧的时间间隔。

max-req：该参数用于设置当认证系统在某个指定的时间内没有收到客户端系统的回复时，向客户端重发 EAP-Request/Identity 数据帧的最大次数。

suppTimeout 和 serverTimeout：表示在认证过程中认证系统接收来自客户端数据包的超时时间和来自认证服务器数据包的超时时间。

1. 配置 quietPeriod

配置 quiet 时间后，当用户终端收到从 Authentication Server 传来的拒绝该用户的接入请求报文后，在此时间间隔内，不论用户采取任何手段与服务器联系，系统将保持沉默不予理睬，默认值为 60 秒，使用以下配置命令：

```
config dot1x quiet-period <0-65535>
```

2. 配置 txPeriod

配置认证系统向客户端系统重传 EAP-Request/Identity 数据帧的时间间隔，默认值为 30

秒，使用以下配置命令：

```
config dot1x tx-period <1-65535>
```

3. 配置 max-req

配置认证系统向客户端重传数据帧的最大次数，默认值是 2，用以下配置命令：

```
config dot1x max-req <1-10>
```

4. 配置 suppTimeout

配置认证系统接收来自客户端系统的数据包的超时时间，默认值是 30 秒，使用以下配置命令：

```
config dot1x supp-timeout <1-65535>
```

5. 配置 serverTimeout

配置认证系统接收来自认证服务器的数据包的超时时间，默认值是 30 秒，使用以下配置命令：

```
config dot1x server-timeout <1-65535>
```

2.1.3 配置对端口的 802.1x 控制

1. 配置端口的认证状态

端口有三种认证状态，分别是 auto、forceauth 和 forceunauth：

auto：此时端口处于接受认证状态，用户能否访问网络完全取决于用户能否认证成功。
缺省配置下，端口的认证状态为 auto。

forceauth：此时端口无条件的处于已授权状态，用户可以不受限制的访问网络。

forceunauth：此时端口无条件的处于未经授权状态，用户不能访问网络。

配置命令如下：

```
config port [<portlist>|all] dot1x authcontrolledportcontrol [auto|  
forceauth|forceunauth]
```

例如：将交换机的端口 1、2、3 分别设置为 auto，forceauth，forceunauth 状态

```
Harbour(config)# config port 1 dot1x authcontrolledportcontrol auto
```

```
Harbour(config)# config port 2 dot1x authcontrolledportcontrol forceauth
```

```
Harbour(config)# config port 3 dot1x authcontrolledportcontrol forceunauth
```


2. 配置端口的控制模式

端口的控制模式有两种：一种是基于端口的控制，另一种是基于 MAC 的控制。在基于端口控制模式下，一个端口上只要有一个合法用户认证通过，则接在该端口下的其他用户不需认证即可获得访问权限；而在基于 MAC 控制模式下，一个端口上的每个用户都要进行独立的认证和计费，只有认证通过的合法用户才能获得访问权限，未通过认证的用户则无法访问网络。在同一认证系统的不同端口上可同时配置两种不同的控制模式。

配置端口控制模式的命令如下：

```
config port [<portlist>|all] dot1x port-control-mode [MAC-based| port-based]
```

参数<portlist>表示端口号的列表。一次可以对多个端口进行相同的配置，参数 all 表示对所有的端口进行配置；参数 MAC-based 表示端口的控制模式是基于 MAC 的控制；参数 port-based 表示端口的控制模式是基于端口的控制。缺省配置下，端口的控制模式为 MAC-based。

例如：配置交换机的端口 1-4 采用基于端口的控制模式，端口 5-10 采用基于 MAC 的控制模式。

```
Harbour(config)# config port 1-4 dot1x port-control-mode port-based
```

```
Harbour(config)# config port 5-10 dot1x port-control-mode MAC-based
```

3. 设置一个端口最多允许接入客户端的数目

港湾公司 Hammer 系列交换机的一个端口在基于 MAC 的控制模式下可支持多个认证用户，使用以下命令设置允许端口接入的最大用户数：

```
config dot1x multiple-host-one-port max-host-count <2-512>
```

<2-512>表示一个端口允许接入的最大用户数的范围，缺省配置为 255。其中，512 既是一个端口允许接入的最大用户数，也是 Hammer 交换机整个认证系统允许接入的最大用户数（uHammer24 交换机除外，uHammer24 允许接入的最大用户数是 256，单端口允许接入的最大用户数范围是<2-256>）。该命令只对基于 MAC 控制模式的端口有效。

例如：设置每个端口允许接入的最大用户数是 10

```
Harbour(config)# config dot1x multiple-host-one-port max-host-count 10
```

2.1.4 设置用户绑定功能

默认情况下，端口的用户绑定功能是禁用的，任何用户通过认证系统（Hammer 交换机）的任何端口都可以请求认证，并在认证通过后访问网络资源。如果希望认证系统只对特定的用户进行认证，可以设置用户绑定功能。启用该功能后，只有端口上绑定的用户才可以请求认证，并在通过认证后访问网络资源，未绑定的用户则不能请求认证。一个端口可以绑定一个或多个用户，如果希望将一个用户绑定到多个端口，可以打开单用户多端口功能。有关用户绑定的配置命令具体如下：

◎ 使能或禁止用户绑定功能

```
config dot1x binduser [enable|disable]
```

◎ 使能或关闭一个用户绑定到多个端口的功能

```
config dot1x binduser multi-port-per-user [enable|disable]
```

◎ 在端口处添加或删除绑定的用户

```
config dot1x binduser [add|delete] port [<portlist>|all] user <username>
```

◎ 清除所有用户绑定信息

```
config dot1x binduser clear-all
```

2.1.5 设置重新认证机制

为了保证用户和认证系统（Hammer 系列交换机）之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程。

1. 使能/关闭重新认证机制

使用如下配置命令：

```
config dot1x re-authentication [enable|disable]
```

选择 enable 表示使能重新认证机制，选择 disable 表示关闭重新认证机制。系统缺省设置为关闭重新认证机制。

例如：使能重新认证机制

```
Harbour(config)# config dot1x re-authentication enable
```

2. 设置重新认证的时间间隔


使用如下配置命令：

```
config dot1x re-authentication period <1-65535>
```

该命令用于配置重新认证的时间间隔。重新认证由认证系统发起，时间是从最近一次成功认证后算起，范围是 1~65535 秒，默认值为 3600 秒，即 1 小时。

例如：设置交换机重新认证的时间间隔为 4000 秒

```
Harbour(config)# config dot1x re-authentication period 4000
```

 重新认证的时间设定需要认真规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

2.1.6 设置异常下线检测机制（keepalive）

除了重新认证机制，为判断接入用户是否保持连接状态，接入模块还提供了另一种检测机制——异常下线检测机制。重新认证机制需要为每个在线用户启动一次完整的认证过程，在用户量较大的情况下，启动重新认证功能将导致频繁产生认证报文，对交换机造成一定的负担，而异常下线检测机制只需要少量的报文交互便可以确定用户是否在线。有关异常下线检测的命令如下：

1. 使能/禁止异常下线检测功能

使用如下配置命令：

```
config dot1x keepalive[enable|disable]
```

选择 enable 表示启用异常下线检测功能，选择 disable 表示关闭异常下线检测功能。系统缺省为关闭该功能。

例如：使能异常下线检测功能

```
Harbour(config)# config dot1x keepalive enable
```

2. 设置异常下线检测的方法

异常下线检测机制提供两种检测方式：一种方式是由交换机主动向客户端定期发送检测请求（state-machine），请求报文利用了 802.1x 协议定义的 EAPOL/EAP ReqId 报文，如果收到客户端的 EAPOL/EAP RespId 响应，说明该用户在线，反之，如果未收到响应则说明用户已经下线。

另一种方式是由客户端主动向交换机定期发送检测请求报文（ping-pong），发送的时间间隔 SendKeepaliveRequestPeriod 和允许的最多无响应次数 MaxNoKeepaliveResponseCount 均由交换机决定，并通知给客户端。检测报文没有利用协议中规定的报文格式，而是定义了专门的格式。交换机收到来自客户端的检测报文后确认客户端在线并响应客户端的检测请求。如果在规定的时间内（该时间由命令行配置换算得出，它的值=客户端允许最多不响应次数 MaxNoKeepaliveResponseCount×客户端定期发送 keepalive 请求的时间间隔 SendKeepaliveRequestPeriod + 30）。没有收到客户端的检测请求，说明客户端已经异常下线。缺省时，系统使用 ping-pong 机制。

配置命令如下：

```
config dot1x keepalive mechanism [ping-pong|state-machine]
```

3. 设置 statemachine 方式下发送检测报文的时间间隔

使用如下配置命令：

```
config dot1x keepalive state-machine-period <10-3600>
```

该命令用于设置交换机每隔多长时间检测一次 802.1x 客户端是否仍为 active 状态。时间范围是 10~3600 秒，默认间隔为 300 秒。

例如：设置交换机每隔 180 秒钟检测一次 802.1x 客户端的在线情况

```
Harbour(config)# config dot1x keepalive state-machine-period 180
```

4. 设置 ping-pong 方式下发送检测报文的时间间隔

使用如下配置命令：

```
config dot1x keepalive ping-pong-period <60-600>
```

该命令用于设置客户端向交换机定期发送检测报文的时间间隔。时间范围是 60~600 秒，默认时间间隔是 120 秒。

例如：设置 ping-pong 方式下发送检测报文的时间间隔为 180 秒

```
Harbour(config)# config dot1x keepalive ping-pong-period 180
```

5. 设置允许客户端未响应的最大次数

使用如下配置命令：

```
config dot1x keepalive max-no-response-count <2-30>
```

设置了这条命令参数后，当交换机在规定的响应时间内未收到客户端的响应报文时，它将再次发送检测报文继续检测。只有客户端未响应的次数超过这个设定的值后，才确定客户端异常下线，并断开连接。该参数的范围是 2~30 次，缺省值是 5。

例如：设置允许客户端未响应的最大次数为 3

```
Harbour(config)# config dot1x keepalive max-no-response-count 3
```

2.1.7 强制用户退出认证状态

出于对管理和安全的考虑，交换机允许管理者强令某个或某些用户退出认证状态，可根据以下条件强制用户退出：

1. 根据客户端的 IP 地址强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff IP <A.B.C.D>
```

设置了这条命令后，对符合该 IP 地址的客户端，交换机将强制其退出认证状态。

例如：令 IP 地址为 10.10.2.6 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff IP 10.10.2.6
```

2. 根据端口访问实体（PAE）的 ID 号强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff id <paeid>
```

该命令表示对 PAE 的 ID 号为<paeid>的客户端，交换机将强制其退出认证状态。

例如：令 paeid 为 10 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff id 10
```

3. 根据 ISP 域名强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff isp-domain <domain>
```

此命令强制那些属于名为<domain>的 ISP 域的客户端退出认证状态。

例如：令属于名为 usergroup1 的 ISP 域的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff isp-domain usergroup1
```

4. 根据客户端的 MAC 地址强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff mac <usermac>{port<portno>}*1
```

此命令强制 MAC 地址为<usermac>的客户端退出认证状态。当使用{port<portno>}参数时，表示该命令只对交换机某个指定端口（<portno>）上的 MAC 地址为<usermac>的客户端有效，如果不使用这个参数，则对任何端口上连接的 MAC 地址为<usermac>的客户端有效。

例如：令交换机端口 3 上所连接的 MAC 地址为 12-00-1c-36-02-11 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff mac 12001c360211 port 3
```

5. 根据端口号强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff port<portno>
```

该命令强制交换机某个端口下的所有用户都退出认证状态。

例如：令交换机端口 10 上的所有客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff port 10
```

6. 根据用户名强制用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff username <username>
```

该命令强制用户名为<username>的用户退出认证状态。

例如：令用户名为 client 的用户退出认证状态

```
Harbour(config)# config dot1x pae force-logoff username client
```

7. 强制所有用户退出认证状态

使用如下配置命令：

```
config dot1x pae force-logoff all
```

该命令强制交换机上的所有 802.1x 用户退出认证状态。

例如：令所有用户退出认证状态

```
Harbour(config)# config dot1x pae force-logoff all
```

2.1.8 清除 802.1x 统计信息

使用以下命令可以清除所有 802.1x 的统计信息：

```
config dot1x clear-statistic
```

2.1.9 配置基于 802.1x 的动态限速功能

 此功能只应用于安装有三层模块的 FlexHammer16i 和 FlexHammer24 交换机。

交换机通过与路由引擎相结合而具备多种限速功能。它可以按 64Kbps 为单位进行速率限制，最高速率可达到 64Mbps。使用限速功能提高了网络带宽的利用率，使网络资源得到有效的控制，增强了网络性能。如果交换机上配有三层路由模块，那么在启动 802.1x 认证服务后，对认证通过的用户可通过打开限速功能来控制其上行和下行的数据流量，并统计出实际的流量。在认证过程中，限速参数通过 Radius 服务器的 Access Accept 报文属性带到交换机。具体使用哪些属性，不同的厂商可能有不同的要求，可能会使用标准属性，也可能使用 26 号属性——厂商自定义的属性，我们可以根据厂商

的要求用命令行来灵活配置,关于如何从属性中接收限速参数的问题将在后面的 Radius 属性配置中介绍。

需要注意的是,用户也可不使用基于 802.1x 的动态限速配置方式,而直接通过命令行以手动配置的方式使用限速功能。这两种限速配置方式是互斥的,也就是说如果启动了基于 802.1x 的动态限速配置,就不能再使用手动方式进行限速配置。

基于 802.1x 的动态限速功能的整体流程如下:

- 启动基于802.1x的动态限速功能的先决条件是802.1x服务和DHCP Relay服务均已启动。之所以要启动DHCP Relay服务,是因为下行流需要绑定用户的IP地址,L3模块的限速功能只针对那些自动获取IP地址的用户。当启动了基于802.1x的动态限速功能时,系统会默认绑定两种流类型:SMAC和DIP。用户认证通过后,RADIUS服务器将分配给用户的上下行带宽等值使用Access Accept 报文的属性带回并保存在交换机中。
- 认证通过后,用户自动申请IP地址。802.1x模块通过DHCP Relay模块获取用户的IP地址后对用户进行限速配置,限速配置将用到RADIUS服务器带回的限速参数,配置方法与命令行手动配置相同。
- 完成限速配置后,便可实现对用户带宽的限制了。用户下线后,需要清除对该用户进行的限速配置。

基于 802.1x 的动态限速功能有以下几点需要说明:

- 对用户上行流进行限速配置时,系统会自动根据源MAC地址进行限速,对用户下行流进行限速配置时,是根据目的IP地址进行限速。
- 在启动基于802.1x的动态限速功能时,如果用户已经用命令行进行了限速配置,那么将不能启动此限速功能,系统提示用户清空所有命令行限速配置。基于802.1x的动态限速配置与手动限速配置是互斥的,基于802.1x的动态限速功能生效后,禁止任何命令行的限速配置。
- 如果有用户在线,并且系统已经存在对这些用户的限速配置,那么在disable限速功能时应清除用户限速配置,在disable 802.1x服务时,也应清除用户的限速配置。

有关三层路由引擎的限速配置命令如下:

1. 设置三层路由引擎的限速控制

三层路由限速控制的配置命令如下:

```
config dot1x access-limit route-engine [rate|acl|disable]
```

根据参数[rate|acl|disable]的不同选项,具体说明如下:

- ◎ 启动基于三层模块的限速功能,输入命令:


```
config dot1x access-limit route-engine rate
```

三层路由的限速功能缺省配置时是禁止的, 执行上述命令后可以启动三层路由的限速功能。

◎ 启动或停止基于三层模块的访问控制列表功能, 输入命令:

```
config dot1x access-limit route-engine acl
```

此命令表示启动三层模块的访问控制列表功能, 选择这个参数时, 需要在交换机上预先配置好访问控制规则列表, 否则执行的 config dot1x access-limit route-engine acl 命令将不起作用。

基于三层模块的访问控制列表功能与限速功能类似, 如果交换机上配有三层路由模块, 那么在启动 802.1x 认证服务后, 对认证通过的用户可以打开访问控制功能, 对其访问权限进行控制。在认证过程中, 访问控制列表的索引通过 RADIUS Server 的 ACCESS ACCEPT 报文属性带到交换机。如何从属性中接收访问控制列表的索引, 将在后面的 Radius 属性配置中介绍。

◎ 禁止三层模块的限速控制功能

使用以下配置命令禁止三层模块的限速控制功能:

```
config dot1x access-limit route-engine disable
```

◎ 配置上行端口号

用户的下行流需要绑定用户的上行端口号, 此上行端口号是交换机连接上一级网络设备的端口, 该端口号需要手动进行配置, 输入命令:

```
config dot1x uplink-port <portno>
```

使用以下命令可以取消对上行端口的绑定:

```
delete dot1x uplink-port <portno>
```

注意

由于限速功能是通过路由引擎提供, 因此只能对经过三层转发的数据流提供限速, 故要求把用户接入端口与上行端口分别配置在不同的 VLAN 中。

2.2 802.1x 显示命令

有关 802.1x 的显示命令如表 2-1 所示:

表 2-1 802.1x 显示命令列表

显示命令	描述
------	----

show dot1x	显示 802.1x 功能开启或关闭的状态以及相关的参数配置信息
show dot1x access-limit route-engine	显示基于三层模块的限速及访问控制列表功能的配置信息
show dot1x pae id <id>	根据 PAE id 索引值显示与之对应的 PAE 信息
show dot1x pae port <portno>	根据端口号显示与之相关联的所有创建的 PAE 信息，以及 PAE 总数
show dot1x pae username <username>	根据用户名显示与之对应的端口访问实体 PAE 相关信息
show dot1x pae mac <address> {port<portno>}*1	根据 MAC 地址显示对应的端口访问实体 PAE 绑定的用户 MAC 地址、Authenticator 状态、后台认证状态、重认证状态等信息
show port [<portlist> all] dot1x	显示一组端口对应的 802.1x 相关信息，包括端口号、当前创建的 PAE 实体的个数以及在某一时刻曾经创建过最多的 PAE 实体的个数
show dot1x binduser multi-port-per-user status	显示绑定多个端口的用户信息
show dot1x binduser port [<portlist> all]	显示某一端口上的用户绑定信息
show dot1x binduser status	显示全部端口绑定信息
show dot1x binduser user <username>	根据用户名显示端口绑定信息
show dot1x pae all	显示所有 PAE
show dot1x pae isp-domain <domain>	根据所在的域显示 PAE
show dot1x statistic	显示 802.1x 统计信息
show dot1x vlan <vlanname> pae	根据 VLAN 显示 PAE
show dot1x vlan <vlanname> user-count	显示 VLAN 中的认证用户数
show dot1x uplink-port	查看上行端口
show nas accounting-statistic	显示计费统计信息
show nas version	显示 NAS 版本信息

2.3 Radius 配置命令

当交换机从用户连接请求报文中提取出与用户相关的属性之后，重新组装成 Radius 格式报文，并与 Radius Server 通信以完成后续的认证、计费功能。

2.3.1 配置 Radius 认证服务

认证服务器（Authentication Server）具有如下属性：

- 认证服务器通过 ID 号进行标识。NAS 包含一个认证服务器列表，当 NAS 发送认证请求时，它从列表中选择最先添加的且处于可用状态的认证服务器，或者选择由用

户指定的认证服务器。因此在配置某个认证服务器时，必须将该服务器加入到列表中，如果不再使用某个认证服务器了，可以将它从列表中删除。

- 添加新的认证服务器时，如果指定的ID号在服务器列表中已经存在，若仍要在新的认证服务器上使用这个ID，需要先删除使用该ID的认证服务器，然后再加入新的认证服务器。
- server-ip是认证服务器的IP地址。
- client-ip是Radius Client的IP地址，即交换机上连接认证服务器的端口所对应的IP地址。
- udp-port端口号，Radius Server 和Radius Client通过UDP发送数据包，对于认证服务器而言，这个端口号默认为1812。

1. 启动/关闭 Radius 认证功能

启动 Radius 认证功能，使用以下配置命令：

```
radius authentication enable
```

关闭 Radius 认证功能，使用以下配置命令：

```
radius authentication disable
```

2. 增加 Radius 认证服务器

增加 Radius 认证服务器的配置命令如下：

```
radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip  
<A.B.C.D> {udp-port <1-6500>} *1
```

增加一个 Radius 认证服务器，设置其 ID 号为 0~4 之一，也就是说系统最多可以设置五个认证服务器，并且要指明认证服务器的 IP 地址和 UDP 端口（默认值为 1812）。另外还要说明使用该认证服务器的客户端（client）的 IP 地址。

例如，增加一个 Radius 认证服务器，设其 ID 号为 1，IP 地址为 110.12.21.1，Radius Client 的 IP 地址为 110.12.21.2

```
Harbour(config)# radius authentication add-server id 1 server-ip 110.12.21.1  
client-ip 110.12.21.2
```

3. 删除 Radius 认证服务器

删除某个认证服务器时只要说明其索引号即可，配置命令如下：

```
radius authentication delete-server id <0-4>
```

4. 设置共享密钥

考虑到网络传输的安全性，传递的报文都是经过加密算法封装过的，配置某个认证服务器 Radius Server 和其 Radius Client 之间的共享密钥<secret>，将该字符串放到 md5 算法中和其它数据一同参与计算，可以使用以下配置命令：

```
radius authentication config-server id <0-4> shared-secret <secret>
```

其中，<0-4>为 Radius Server 的索引值，<secret>为共享密钥，缺省密钥值是 harbour。

5. 设置重传时间间隔

当设备 Radius Client 向 Radius Server 发出请求的一段时间之后没有得到 Radius Server 的应答，Radius Client 可以向 Radius Server 重传数据包，重传数据包的时间间隔默认值为 10 秒，可以使用以下配置命令设置这个间隔：

```
radius authentication config-server id <0-4> retransmit-interval <5-300>
```

其中，<0-4>为 Radius Server 的索引值，<5-300>为重传时间间隔的取值范围，单位为秒。

6. 设置重传的最大次数

当 Radius Client 需要向 Radius Server 重传数据包时，应配置 Radius Client 重传该数据包的最大次数，默认值为 3 次，可以使用以下配置命令：

```
radius authentication config-server id <0-4> max-retransmit-count <2-10>
```

其中，<0-4>为 Radius Server 的索引值，<2-10>为最大重传次数。

7. 设置最大重传丢弃数

该参数用于判断 Radius Server 是否断掉。当 Radius Client 按上述规定的重传次数完成重传后，若仍未收到 Radius Server 的回复，则丢弃数据包，系统记录一次重传丢弃。当丢弃数超过所设置的最大重传丢弃数时，则认为 Radius Server 连接已断。利用以下命令设置最大重传丢弃数：

```
radius authentication config-server id <0-4> max-retransmit-drop-count <2-30>
```

其中，<0-4>为 Radius Server 的索引值，<2-30>为最大重传丢弃数。

8. 设置最大发送失败数

该参数用于判断 Radius Server 是否断掉。如果 Radius Client 有超过最大发送失败数的包没有发送成功，则表明该 Radius Server 的连接已断。利用以下命令设置最大发送失败数：

```
radius authentication config-server id <0-4> max-send-fail-count <2-30>
```

其中，<0-4>为 Radius Server 的索引值，<2-30>为最大发送失败数。

9. 设置认证服务器的当前状态

Radius 认证服务器具有三种状态：active、inactive、dead，这三种状态各自表示的意义说明如下：

状态	描述
active	处于此状态的认证服务器能够与交换机一起完成正常的授权认证功能。
inactive	处于此状态的认证服务器不执行认证功能，但交换机仍会定期向该服务器发送检测报文，以便等待随时在需要的时候将服务器的状态改成 active。
dead	处于此状态的认证服务器不执行认证功能，交换机也不向该服务器发送检测报文。dead 状态出现在具有多台备份服务器的情况下。

认证服务器状态的改变由系统根据实际情况和需要自动完成，可以使用 show radius 命令查看服务器的当前状态。用户也可以通过手动配置的方式将当前状态为 inactive 或 dead 的认证服务器设置成 active 状态，配置命令如下：

```
radius authentication config-server id <0-4> status active
```

2.3.2 配置 Radius 计费服务

1. 启动/关闭 Radius 计费功能

启动 Radius 计费功能，使用以下配置命令：

```
radius accounting enabled
```

关闭 Radius 计费功能，使用以下配置命令：

```
radius accounting disable
```

2. 增加 Radius 计费服务器

增加一个 Radius 计费服务器，设置其 ID 索引号为 0~4 之一，也就是说系统最多可设置五个计费服务器，其中以最先添加的计费服务器作为主计费服务器，或者由用户指定主计费服务器。此外，还要指明增加的计费服务器的 IP 地址和 UDP 端口（默认值为 1813），以及使用该计费服务器的 Radius Client 的 IP 地址。使用以下配置命令：

```
radius accounting add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>} *1
```

例如，增加一个 Radius 计费服务器，设其 ID 号为 1，IP 地址为 110.12.21.1，Radius Client 的 IP 地址为 110.12.21.2

```
Harbour(config)# radius accounting add-server id 1 server-ip 110.12.21.1
```

```
client-ip 110.12.21.2
```

3. 删除 Radius 计费服务器

删除某个计费服务器时只要说明其索引号即可，配置命令如下：

```
radius accounting delete-server id <0-4>
```

4. 设置共享密钥

考虑到网络传输的安全性，传递的报文都是经过加密算法封装过的，配置某个计费服务器 Radius Server 和其 Radius Client 之间的共享密钥<secret>，将该字符串放到 md5 算法中和其它数据一同参与计算，可以使用以下配置命令：

```
radius accounting config-server id <0-4> shared-secret <secret>
```

其中，<0-4>为 Radius Server 的索引值，<secret>为共享密钥，缺省密钥值是 harbour。

5. 设置重传时间间隔

当 Radius Client 向 Radius Server 发出请求的一段时间之后没有得到 Radius Server 的应答，Radius Client 可以向 Radius Server 重传数据包，重传数据包的时间间隔默认值为 10 秒，可以使用以下配置命令设置这个间隔：

```
radius accounting config-server id <0-4> retransmit-interval <5-300>
```

其中，<0-4>为 Radius Server 的索引值，<5-300>为重传时间间隔的取值范围，单位为秒。

6. 设置重传的最大次数

当 Radius Client 需要向 Radius Server 重传数据包时，应配置 Radius Client 重传该数据包的最大次数，默认值为 3 次，可以使用以下配置命令：

```
radius accounting config-server id <0-4> max-retransmit-count <2-10>
```

其中，<0-4>为 Radius Server 的索引值，<2-10>为最大重传次数。

7. 设置最大重传丢弃数

该参数用于判断 Radius Server 是否断掉。当 Radius Client 按上述规定的重传次数完成重传后，若仍未收到 Radius Server 的回复，则丢弃数据包，系统记录一次重传丢弃。当该丢弃数超过所设置的最大重传丢弃数时，则认为 Radius Server 连接已断。利用以下命令设置最大重传丢弃数：

```
radius accounting config-server id <0-4> max-retransmit-drop-count <2-30>
```

其中，<0-4>为 Radius Server 的索引值，<2-30>为最大重传丢弃数。

8. 设置最大发送失败数

该参数用于判断 Radius Server 是否断掉。如果 Radius Client 有超过最大发送失败数的包没有发送成功，则表明该 Radius Server 的连接已断。利用以下命令设置最大发送失败数：

```
radius accounting config-server id <0-4> max-send-fail-count <2-30>
```

其中，<0-4>为 Radius Server 的索引值，<2-30>为最大发送失败数。

9. 设置计费服务器的当前状态

Radius 计费服务器具有三种状态：active、inactive、dead，这三种状态各自表示的意义说明如下：

状态	描述
active	处于此状态的计费服务器能够与交换机一起完成正常的计费功能。
inactive	处于此状态的计费服务器不执行计费功能，但交换机仍会定期向该服务器发送检测报文，以便等待随时在需要的时候将服务器的状态改成 active。
dead	处于此状态的计费服务器不执行计费功能，交换机也不向该服务器发送检测报文。dead 状态出现在具有多台备份服务器的情况下。

计费服务器状态的改变由系统根据实际情况和需要自动完成，可以使用 show radius 命令查看服务器的当前状态。用户也可以通过手动配置的方式将当前状态为 inactive 或 dead 的计费服务器设置成 active 状态，配置命令如下：

```
radius accounting config-server id <0-4> status active
```

2.3.3 设置 Radius CUT 功能

Radius CUT 是指由 Radius Server 主动发起断开与用户连接的信息。当 Radius Server 由于某种原因要求用户下线时，向认证系统（交换机）发送一种 Radius 格式的请求报文（CUT）。交换机在指定的 UDP 端口处监听该请求，一旦收到 CUT 请求，便按照以下步骤执行处理过程：


第一步：根据配置命令进行合法性检查。

通过命令行的配置，选择使用 CUT 报文中的 AUTHENTICATOR 字段进行报文的合法性检查，或者使用 MESSAGE AUTHENTICATOR 属性字段进行报文的合法性检查。Hammer 交换机采用和 Radius Server 相同的标准协议算法重新计算 AUTHENTICATOR 字段或 MESSAGE AUTHENTICATOR 属性字段，当计算结果与 CUT 报文相一致时，认为其合法，否则丢弃该 CUT 报文。使用这种机制时，不必重新认证便可由交换机直接切断与用户的连接。当然这要求配置人员必须首先了解 Radius Server 发出的 CUT 报文格式才能进行相应的配置。

第二步：按照相关属性定位用户。

如果没有找到对应用户，则说明该用户不在线，将不予处理；如果找到对应的用户，则根据配置命令使用以下其中一种方法切断 Radius Server 与 Radius Client 的连接：

- 启动重认证机制，由Radius Server发送RADIUS_ACCESS_REJECT报文拒绝用户的认证请求。
- 由交换机自动设置直接切断该用户。

 默认配置下，为了保证网络的安全，交换机不检测报文的合法性便直接断开与用户的连接，从而避免受到非法 CUT 报文的攻击。

网络中可能存在多个 Radius Server，包括认证服务器和计费服务器，可以设置交换机只处理某些服务器发出的 CUT 请求。因此在交换机中设置一个 CUT Server 列表，在此列表中存放着这些 Server 的信息。

有关 Radius CUT 功能的配置命令具体如下：

1. 启动/关闭接收 CUT 报文功能

启动接收 CUT 报文功能，使用以下命令：

```
radius cut enable
```

关闭接收 CUT 报文功能，使用以下命令：

```
radius cut disable
```

2. 向列表中增加/删除认证服务器

向列表中增加一个认证服务器，使用以下命令：

```
radius cut add-server authentication id <0-4>{udp-port <1-6500>}*1
```

从列表中删除一个认证服务器，使用以下命令：

```
radius cut delete-server authentication id <0-4>
```

Hammer 系列交换机可为每个域最多设置 5 个认证服务器，id <0-4>代表认证服务器的索引号。

3. 向列表中增加/删除计费服务器

向列表中增加一个计费服务器，使用以下命令：

```
radius cut add-server accounting id <0-4> {udp-port <1-6500>}*1
```

从列表中删除一个计费服务器，使用以下命令：


```
radius cut delete-server accounting id <0-4>
```

Hammer 系列交换机可为每个域最多设置 5 个计费服务器，id <0-4>代表计费服务器的索引号。

4. 设置校验 CUT 报文的方式

CUT 报文的合法性校验默认是关闭的，可以通过以下命令行配置以何种方式校验 CUT 报文的合法性：

```
radius cut verify-by [authenticator|message-authenticator|none]
```

- 参数authenticator表示校验CUT报文的authenticator字段
- 参数message-authenticator表示校验CUT报文的message-authenticator属性
- 参数none表示不校验CUT报文

5. 设置处理 CUT 请求机制

Hammer 交换机具有两种处理 CUT 报文的机制：启动重认证机制和直接切断与用户连接机制：

```
radius cut process-by [reauthentication|logoff]
```

参数 reauthentication 表示启动重认证机制处理 CUT 请求；参数 logoff 表示直接断开与用户的连接。默认为直接断开连接。

2.3.4 配置 Session Timeout 处理机制

Session Timeout 是 Radius Server 通过 Access Accept 报文传递的一个属性，在 RFC2866 中它的含义是授权用户本次接入服务的时间，如果该时间到达，就停止用户的接入服务，强制用户下线。港湾网络公司 Hammer 系列交换机的接入模块对这一属性进行了扩展，使得该属性既可以按照 RFC2866 中的标准使用，也可以将该属性解释为服务器希望对用户进行重认证，Session Timeout 的值为重认证的时间间隔。

配置命令如下：

```
radius accounting session-timeout-type [logoff|reauthenticate]
```

选择 logoff 表示按照 RFC2866 标准对 Session Timeout 进行处理；选择 reauthenticate 表示按照设置的重认证时间间隔由服务器对用户进行重认证。默认选项为 logoff。

2.3.5 配置 Radius Server 主备切换功能

Hammer 系列交换机可为每个域最多设置 5 个 Radius 服务器（在主备服务器环境下一般

为两个可用的服务器，一个为主用，一个为备用），如果正在使用的 Radius 主用服务器断掉，可以切换到备用的 Radius 服务器。其中的切换功能包括以下内容：

- 提供对正在认证的用户处理。认证服务器发生切换时，可以让正在认证的用户不等待原来的认证请求，立即重新在备用服务器进行重认证；计费服务器发生切换时，可以让正在发送的计费请求不等待回复而重新发送计费请求到备用的计费服务器。
- 提供对已经认证通过的用户处理。可以让已经认证通过的用户在认证服务器发生主备切换时在备用的服务器上重认证；也可以使主备切换对已经认证的用户透明，即不用重认证便可让用户继续使用接入服务。
- 提供对切换的 Radius 服务器的可用状态的检测功能。可以定期检测断掉的原服务器的可用状态，如果原服务器恢复为可用状态，可以自动将原服务器设为备用服务器，或通过命令切换到主服务器。
- 提供通过命令行切换主备 Radius 服务器的功能，使得在主用和备用服务器之间通过人为命令实现切换。

◎ 使能/禁止 Radius Server 主备切换功能，配置命令如下

```
radius [accounting|authentication] server-switch [enable|disable]
```

选择 accounting 参数表示可以使能/禁止计费服务器的主备切换功能，选择 authentication 参数表示可以使能/禁止认证服务器的主备切换功能。缺省配置为 disable。

◎ 设置是否将主备切换信息通知给 dot1x 模块

在发生 Radius 服务器主备切换时，可以设置是否将此信息通知给 dot1x 模块。如果通知 dot1x 模块，就会让已经认证的用户通过备用服务器进行重认证；如果不通知 dot1x 模块，Radius 服务器主备切换对已经认证的用户是透明的，不会进行重认证。使用以下命令来配置发生 Radius 服务器主备切换时是否通知 dot1x：

```
config radius serverswitch-notify [enable|disable]
```

2.3.6 配置 Radius 属性

1. 配置 Radius 属性的类型

用作网络访问设备（NAS）的交换机通过 Radius 报文同 Radius 服务器通信，Radius 报文中的属性用来传递认证、授权和计费的详细信息。我们现在的 NAS 版本中使用的属性主要指在 RFC2865、RFC2866、RFC2869 中规定的标准属性，另外还包括一些用户可以配置的自定义属性以传递一些我们需要的用户参数，包括用户的带宽、优先级以及 vlanid，这里我们介绍的配置 Radius 属性主要涉及配置自定义属性。

用户认证过程中，认证系统将用户的一些特征信息，通过认证请求报文传递给 Radius 服务器；用户认证通过后，Radius 服务器将一些用户配置参数通过 access-accept 报文传

递给 Radius Client。其中包括用户的上下行带宽、优先级，以及用户进出的 vlanid。Radius Client 从属性中提取出配置参数，并对用户作相应的处理。具体使用哪些属性来携带这些参数，不同的厂商可能有不同的要求，考虑到这种情况，我们能够做到根据厂商的要求利用命令行进行灵活配置。由于这些参数的取值为数值形式，因此我们要求 Radius 服务器相关属性值的类型应为 INTEGER，而不要使用 STRING 或 TEXT 类型。

属性的配置有两种方式：

- 配置使用标准属性。所谓标准属性是指RFC2865中规定的属性，属性类型占一个字节，因此可以有1~255 种属性。Radius RFC规定了大部分属性的含义，用于传递认证和计费信息。但实际应用中有许多属性是不使用的，因此可用来携带自定义的用户参数，实际上也就改变了该属性的原有含义。比如（在后面的配置实例中）我们可以使用标准属性Framed-MTU 携带用户的上行带宽，而Framed-MTU在RFC2865中定义为用户的最大传输单元值。
- 配置使用26号属性——厂商自定义属性。26号属性的定义参见RFC2865，厂商自定义属性 Vendor Specific attribute 用于不同的厂商接收自己定义的参数，因此系统默认从26号vendor-specific属性中接收配置参数。

使用标准属性携带用户参数

◎ 使用标准属性携带 Radius 服务器返回的上下行带宽信息，配置命令如下：

```
radius config-attribute access-bindwidth [uplink|downlink] standard <1-255>
```

其中，standard<1-255>是设置从标准属性类型<1-255>中的哪个属性返回上下行带宽信息。

◎ 使用标准属性携带 Radius 服务器返回的用户 ACL ID 信息，配置命令如下：

```
radius config-attribute filter-id standard <1-255>
```

其中，standard<1-255>是设置从标准属性类型<1-255>中的哪个属性返回用户的 ACL ID 信息。

◎ 使用标准属性向 Radius 服务器传递用户的 VLAN IP 信息，配置命令如下：

```
radius config-attribute vlan-ip standard <1-255>
```

其中，standard<1-255>是设置从标准属性类型<1-255>中的哪个属性返回用户的 VLAN IP 信息。

◎ 使用标准属性向 Radius 服务器传递用户的端口反查信息，配置命令如下：

```
radius config-attribute path-track standard <1-255>
```

其中, standard<1-255>是设置从标准属性类型<1-255>中的哪个属性返回端口反查信息。端口反查信息用于记录用户从哪台设备的哪个端口接入网络, 便于对用户进行跟踪管理。

◎ 使用标准属性向 Radius 服务器传递用户的 VLAN ID 信息, 配置命令如下:

```
radius config-attribute vlan-id standard <1-255>
```

其中, standard<1-255>是设置从标准属性类型<1-255>中的哪个属性携带 VLAN ID 信息。

◎ 使用标准属性向 Radius 服务器传递用户的 MAC 信息, 配置命令如下:

```
radius config-attribute source-mac standard <100-255>
```

缺省值为 100, 不携带该属性。

使用 26 号厂商自定义属性携带用户参数

◎ 使用 26 号厂商自定义属性携带 Radius 服务器返回的上下行带宽信息, 配置命令如下:

```
radius config-attribute access-bandwidth [uplink|downlink] Vendor-Specific  
<VendorType> {<VendorId>}*1
```

- Vendor-Specific表示通过标准的厂商属性返回用户的上下行带宽信息, 标准的厂商属性为26
- <VendorType>表示厂商自定义类型, 缺省配置下, 上行带宽的VendorType为1, 下行带宽的VendorType为2
- VendorId是SMI分配的厂商代码, 默认值为8212(港湾网络有限公司)

◎ 使用 26 号厂商自定义属性携带 Radius 服务器返回的用户 ACL ID 信息, 配置命令如下:

```
radius config-attribute filter-id Vendor-Specific <VendorType>  
{<VendorId>}*1
```

- Vendor-Specific表示通过标准的厂商属性返回用户的ACL ID信息, 标准的厂商属性为26
- <VendorType>表示厂商自定义类型, 缺省配置下, 用户ACL ID的VendorType为7
- VendorId是SMI分配的厂商代码, 默认值为8212(港湾网络有限公司)

◎ 使用 26 号厂商自定义属性向 Radius 服务器传递用户 VLAN IP 信息,配置命令如下:

```
radius config-attribute vlan-ip Vendor-Specific <VendorType> {<VendorId>}*1
```

- Vendor-Specific表示通过标准的厂商属性返回用户的VLAN IP信息,标准的厂商属性为26
- <VendorType>表示厂商自定义类型,缺省配置下,用户VLAN IP的VendorType为31
- VendorId是SMI分配的厂商代码,默认值为8212(港湾网络有限公司)

◎ 使用 26 号厂商自定义属性向 Radius 服务器传递端口反查信息,配置命令如下:

```
radius config-attribute path-track Vendor-Specific <VendorType> {<VendorId>}*1
```

- Vendor-Specific表示通过标准的厂商属性返回端口反查信息,标准的厂商属性为26
- <VendorType>表示厂商自定义类型,缺省配置下,端口反查的VendorType为33
- VendorId是SMI分配的厂商代码,默认值为8212(港湾网络有限公司)

◎ 使用 26 号厂商自定义属性向 Radius 服务器传递用户的 VLAN ID 信息,配置命令如下:

```
radius config-attribute vlan-id Vendor-Specific <VendorType> {<VendorId>}*1
```

- Vendor-Specific表示通过标准的厂商属性返回用户的VLAN ID信息,标准的厂商属性为26
- <VendorType>表示厂商自定义类型,缺省配置下,用户VLAN ID的VendorType为32
- VendorId是SMI分配的厂商代码,默认值为8212(港湾网络有限公司)

恢复 Radius 属性类型的默认值

当用户不希望设置 Radius 属性类型的值,而想要使用属性的默认值时,可按照以下命令进行配置:

◎ 设置上下行带宽属性类型的默认值

```
radius config-attribute access-bandwidth [uplink|downlink] default-value
```

上行带宽属性类型的默认值为使用标准厂商属性 26, 厂商自定义类型 1; 下行带宽属性类型的默认值为标准厂商属性 26, 厂商自定义类型 2。

◎ 设置访问控制列表属性类型的默认值

```
radius config-attribute filter-id default-value
```

访问控制列表属性类型的默认值为标准厂商属性 26，厂商自定义类型 7

◎ 设置端口反查属性类型的默认值

```
radius config-attribute path-track default-value
```

端口反查属性类型的默认值为标准厂商属性 26，厂商自定义类型 33

◎ 设置 VLAN ID 属性的默认值

```
radius config-attribute vlan-id default-value
```

VLAN Id 属性类型的默认值为标准厂商属性 26，厂商自定义类型 32

◎ 设置 VLAN IP 属性的默认值

```
radius config-attribute vlan-ip default-value
```

VLAN IP 属性类型的默认值为标准厂商属性 26，厂商自定义类型 31

◎ 设置 frame-protocol 属性的默认值

```
radius config-attribute frame-protocol default
```

◎ 设置 frame-protocol 属性的默认值

```
radius config-attribute nas-port-type default
```

◎ 恢复所有可配置的 Radius 属性类型的默认值

```
radius config-attribute all default-value
```

2. 配置 Radius 属性的值

由于在不同的网络环境下，不同的 Radius 服务器对某些 Radius 属性的具体值要求不同，如一些窄带的 Radius 服务器要求 frame-protocol 的值必须为 PPP，这使我们和它对接时，必须把该属性值设为 PPP。为了适应不同 Radius 服务器的要求，港湾网络公司的 Hammer 系列交换机提供了对这类属性值的配置功能。

◎ 配置 Radius 属性的值：

配置 frame-protocol 的值，配置命令如下：

```
radius config-attribute frame-protocol <0-255>
```

<0-255>为 frame-Protocol 的值，该值与协议的对应关系如下：

属性值<0-255>	对应协议
1	PPP
2	SLIP
3	AppleTalk Remote Access Protocol (ARAP)
4	Gandalf proprietary SingleLink/MultiLink protocol
5	Xylogics proprietary IPX/SLIP
6	X.75 Synchronous

当 frame-protocol 的属性值设置为 0 时，表示报文中不携带 frame-protocol 属性。

配置 nas-port-type 属性的值（nas-port-type 也是 Radius 属性之一），配置命令如下：

```
radius config-attribute nas-port-type <0-255>
```

<0-255>为 nas-port-type 的值，该值与 NAS 端口类型的对应关系如下：

属性值<0-255>	NAS 端口类型
0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual
6	PIAFS
7	HDLC Clear Channel
8	X.25
9	X.75
10	G.3 Fax
11	SDSL - Symmetric DSL
12	ADSL-CAP - Asymmetric DSL, Carrierless Amplitude Phase Modulation
13	ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone
14	IDSL - ISDN Digital Subscriber Line
15	Ethernet
16	xDSL - Digital Subscriber Line of unknown type
17	Cable
18	Wireless - Other
19	Wireless - IEEE 802.11

© 显示 Radius 属性值的配置:

```
show radius config-attribute frame-protocol
show radius config-attribute nas-port-type
```

2. 配置 Radius 服务器返回带宽值的单位

Radius 服务器返回的带宽值可以选择两种单位表示方法: bps 和 kbps, 具体配置命令如下:

```
radius config-attribute access-bandwidth unit [bps|kbps]
```

选择 bps 表示 Radius 服务器返回带宽值的单位为 bps, 选择 kbps 表示 Radius 服务器返回带宽值的单位为 kbps。系统默认为 bps。

例如: 配置 Radius 服务器返回带宽值的单位为 kbps

```
Harbour(config)# radius config-attribute access-bandwidth unit kbps
```

2.3.7 配置实例

实例 1:

打开 Radius 的认证功能, 同时增加一个 Radius 认证服务器, 该服务器的 IP 地址为 10.7.1.9, 客户端的 IP 地址是 10.7.1.253, 端口号 1812。设服务器与客户端的共享密钥为"xyzy5461"。设置允许客户端向认证服务器重传报文的时间间隔为 5 秒, 最大重传次数为 2 次, 最大发送失败次数为 2 次, 最大重传丢弃次数为 2 次。具体配置步骤如下:

```
Harbour(config)# radius authentication enable

Harbour(config)# radius authentication add-server id 0 server-ip 10.7.1.9
client-ip 10.7.1.253 udp-port 1812

Harbour(config)# radius authentication config-server id 0 shared-secret
xyzy5461

Harbour(config)# radius authentication config-server id 0 retransmit-
interval 5

Harbour(config)# radius authentication config-server id 0 max-retransmit-
count 2

Harbour(config)# radius authentication config-server id 0 max-send-fail-
count 2

Harbour(config)# radius authentication config-server id 0 max-retransmit-
drop-count 2
```

实例 2:

删除 ID 为 0 的 Radius 认证服务器, 并关闭 Radius 的认证功能。配置步骤如下:

```
Harbour(config)# radius authentication delete-server id 0
```

```
harbour(config)# radius authentication disable
```

实例 3:

将上行带宽使用标准属性带回，将下行优先级使用 26 号属性带回，VendorType = 1, VendorId = 8212

```
harbour(config)# radius config-attribute access-bandwidth uplink standard 12
```

```
harbour(config)# radius config-attribute access-bandwidth downlink vendor-specific 1
```

由于 VendorId=8212 是默认配置，所以在命令设置中可以省略。

2.4 Radius 显示命令

有关 Radius 信息的显示命令见表 2-2:

表 2-2 Radius 显示命令列表:

显示命令	功能描述
show radius [accounting authentication] server-switch	显示 Radius 认证或计费服务器的主备切换功能是否启用
show radius accounting session-timeout-type	显示计费服务器的 Session Timeout 类型
show radius cut process-way	显示 CUT 请求处理机制
show radius cut verify-way	显示 CUT 报文校验方式
show radius idpool	显示 Radius 服务器 ID 号的使用情况，用于调试
show radius {configuration}*1	显示 Radius 配置信息
show radius config-attribute frame-protocol	显示 Frame-Protocol 属性的值
show radius config-attribute nas-port-type	显示 Nas-Port-Type 属性的值
show radius config-attribute bandwidth-unit	显示 Radius 服务器返回带宽值的单位
show radius custom-attributes	显示 Radius 属性类型

2.5 配置域

在 Hammer 系列交换机的接入模块中，我们引入了域（isp-domain）的概念。不同的域可能由不同的 ISP 经营。接入设备根据用户输入的用户名中的域名部分（用户名@域名）来区分用户所属的域，并将其认证和计费请求发送到相应域的认证服务器和计费服务器。

建立了域的概念以后，当我们在系统中增加 Radius 服务器时，必须将其分配给相应的

域才能使用。系统中缺省包含一个名为 default 的域，如果不创建新的域，所有的认证计费服务器均属于这个 default 域，系统将所有的用户认证请求都发送到 default 域中的 Radius 认证服务器。

如果要删除一个域，应首先将属于该域的 Radius 服务器从域中删除。

注意

默认域 default 不能删除。

2.5.1 域的基本配置

有关域的基本配置命令具体如下：

◎ 创建域

```
create isp-domain <domain>
```

其中<domain>为所创建的域的域名

◎ 删除域

```
delete isp-domain <domain>
```

其中<domain>为所要删除的域的域名

◎ 配置是否将完整的用户名发送给 Radius 服务器

完整的用户名表现为“用户名@域名”，当选择发送不完整的用户名时表示去掉用户名后面的域名部分。配置命令如下：

```
config isp-domain <domain> username [complete|incomplete]
```

选择 complete 表示将完整的用户名发送给 Radius 服务器；选择 incomplete 表示发送不带域名的用户名。缺省配置为 complete。

例如用户输入的用户名和域名为 abc@domain，若配置为发送完整的用户名和域名，则将 abc@domain 作为用户名发送给 Radius 服务器；若使用不完整的用户名，则只将 abc 作为用户名发送给 Radius 服务器。

◎ 配置客户端软件升级的 URL

在设置通过 URL 升级客户端软件之前，应使用以下命令使能该功能：

```
config      isp-domain      <domain>      supplicant-upgrade      force-upgrade  
[enable|disable]
```

然后配置客户端软件升级的 URL，配置命令如下：

```
config isp-domain <domain> supplicant-upgrade url <supp_upgrade_
url|NULL>
```

当通过以上命令在交换机上配置了客户端软件升级的 URL 后，当用户认证通过时，交换机将客户端软件升级的 URL 返回给客户端，用户可以用该 URL 升级自己的客户端软件。

注意：参数<url> 必须是完整的路径加完整的文件名，默认为 NULL。

2.5.2 域认证配置

◎ 向域中添加/删除认证服务器

```
config isp-domain <domain> authentication [add-server|delete-
server] id <id>
```

add-server 表示向名为<domain>的域添加认证服务器，delete-server 表示从名为<domain>的域删除认证服务器。

由于一个域可以包含多个认证服务器，因此需要指定每个认证服务器的 ID 标识<id>。

◎ 启动/禁止域内的 Radius 认证功能

```
config isp-domain <domain> authentication [enable|disable]
```

启动或停止某个域的认证功能并不影响其他域的认证或计费功能。缺省配置为 enable。

◎ 配置域的认证模式

每个域有两种认证模式：独立认证模式(independent)和主备认证模式(primary-backup)。如果使用独立认证模式，当域中的主认证服务器发生故障时，不把认证转移到域内的备用认证服务器上。如果使用主备认证模式，当域中的主认证服务器发生故障时，设备自动将认证切换到备用认证服务器上。

配置域的认证模式使用以下配置命令：

```
config isp-domain <domain> authentication mode [independent|primary-backup]
```

在<domain>处输入要配置的域的域名。选择 independent 表示使用独立认证模式，选择 primary-backup 表示使用主备认证模式。缺省的认证模式为 independent。

应当注意的是，若要配置域的认证模式为 primary-backup，需要首先使能 Radius 认证服务器的主备切换功能，也就是先做如下配置：

```
Harbour(config)# radius authentication server-switch enable
```

◎ 指定主认证服务器

```
config isp-domain <domain> authentication config-server id <id> type primary
```

使用上述命令可以指定其中一个认证服务器作为主认证服务器。默认情况下，以首次添加的认证服务器作为主认证服务器。

◎ 配置域的认证方式

包括三种认证方式：PAP 认证、CHAP 认证、EAP-MD5 认证。系统默认为 EAP-MD5 认证。配置命令如下：

```
config isp-domain <domain> authentication type [pap|chap|eap-md5]
```

2.5.3 域的计费配置

◎ 向域中添加/删除计费服务器

```
config isp-domain <domain> accounting [add-server|delete-server] id <id>
```

add-server 表示向名为<domain>的域添加计费服务器，delete-server 表示从名为<domain>的域中删除计费服务器。由于一个域可以包含多个计费服务器，因此需要指定每个计费服务器的 ID 标识<id>。

◎ 启动/禁止域内的 Radius 计费功能

```
config isp-domain <domain> accounting [enable|disable]
```

默认为 enable。

◎ 配置计费服务器在域中的类型

```
config isp-domain <domain> accounting config-server id <id> type  
[primary|multi|backup]
```

primary 表示把某个 Radius 计费服务器置为主计费服务器；multi 表示把某个 Radius 服务器设置成其中一个计费服务器，若该计费服务器是主计费服务器，则保持不变，因为主计费服务器也属于多个计费服务器中的一个计费服务器；backup 表示把域中的某个 Radius 计费服务器设置成备份计费服务器，若该计费服务器是主计费服务器，则选择第一个备份计费服务器作为主计费服务器。

在缺省情况下，系统将第一个添加的计费服务器作为主计费服务器，其他计费服务器都为备份服务器。

◎ 配置域中 Radius 计费服务器的计费模式

```
config isp-domain <domain> accounting mode [independent|primary-backup  
|multi]
```

默认为 independent。

独立计费模式(independent)是指当 Radius 主计费服务器出现故障的时候,交换机不主动把计费信息发送到备用 Radius 计费服务器上;主备计费模式(primary-backup)是指当 Radius 主计费服务器出现故障的时候,交换机自动把计费切换到备用 Radius 计费服务器上;多服务器计费模式(multi)是指在交换机计费的时候,把一份计费信息同时向多个 Radius 计费服务器发送。

应当注意的是,若要配置域的计费模式为 primary-backup,需要首先使能 Radius 计费服务器的主备切换功能,也就是先做如下配置:

```
Harbour(config)# radius accounting server-switch enable
```

◎ 配置即时计费时间间隔

即时计费功能(Interim Update Accounting)是指在发送计费开始请求和计费结束请求之间定期发送即时计费请求,以便将在线用户的计费信息定期发送到 Radius 计费服务器。

配置即时计费请求的时间间隔,并打开发送功能,输入以下命令:

```
config isp-domain <domain> accounting interim-update-accounting interval  
<10-65535>
```

关闭即时计费请求发送功能,输入以下命令:

```
config isp-domain <domain> accounting interim-update-accounting disable
```

默认为 disable (即间隔时间为 0)。

◎ 配置开始计费时是否等待用户获取 IP

接入服务支持与 DHCP Relay 功能相结合, DHCP Relay 在获得了 DHCP Server 传来的用户 IP 之后,会通知设备的 NAS 模块,从而可以通过相关命令察看到某用户动态获得的 IP 地址;当用户主动 release 了自己的 IP 地址之后,我们也可以通过相关命令察看到该用户的 IP 为未知。如果 DHCP Relay 功能打开,并且用户是自动获取 IP 的方式,那么可以配置在发送计费请求报文之前是否获得用户的 IP 地址。

配置发送计费开始请求之前是否必须先得到用户 IP 地址,输入命令:

```
config isp-domain <domain> accounting start-need-ip [enable|disable]
```

参数 enable 表示认证通过之后一定要在得到 IP 地址以后再发计费请求,参数 disable 表示认证通过之后不必得到 IP 地址就可以发计费请求。默认为 disable。

◎ 配置交换机等待用户获取 IP 地址的最长时间:

如果设置为在认证通过之后一定要等到用户获得了 IP 地址再发送计费请求,那么需要

设置经过多长时间之后如果用户还没有得到 IP 地址，则根据超时机制切断该用户的连接，配置命令如下：

```
config isp-domain <domain> accounting wait-ip <100-600>
```

参数<100-600>表示等待的时间，单位是秒，系统默认为等待 100 秒。

◎ 配置系统重新启动后是否向 Radius 服务器发送计费同步报文

如果 Radius 服务器支持计费同步报文，则当 NAS 因发生断电等意外情况而重新启动时，会向域中允许发计费同步报文的所有 Radius 计费服务器发一个计费类型为 Accounting-On 的计费同步报文，Radius 服务器收到该报文后对该 NAS 下的所有用户停止计费。命令格式如下：

```
config isp-domain <domain> accounting sync [enable|disable]
```

默认为 disable。

2.5.4 配置实例

在名为 harbour 的域中，设置在发送计费报文时需要用户的 IP 地址，等待用户端获取 IP 地址的超时时间设为 180 秒，并且使用即时计费功能，计费间隔设为 180 秒。配置步骤具体如下：

```
harbour(config)# service dhcpd enable
```

```
harbour(config)# config isp-domain harbour accounting start-need-ip enable
```

```
harbour(config)# config isp-domain harbour accounting wait-ip 180
```

```
harbour(config)# config isp-domain harbour accounting interim-update-  
accounting interval 180
```

第3章 接入服务应用配置实例

3.1 单域认证

在交换机的接入服务系统中有一个默认的域 default，如果不使用多域功能，则不必创建新的域，直接利用 default 域即可。以下我们将介绍实现单域认证的最小配置。

如图 3-1 所示，Hammer 交换机的端口 23 和端口 24 各连接一个 Radius 服务器，每个服务器均具有认证和计费功能。

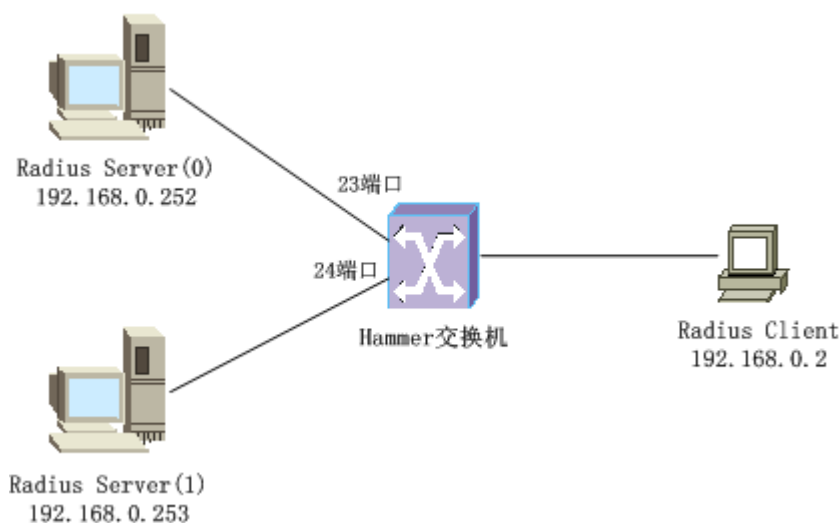


图 3-1 单域认证网络图

配置步骤具体如下：

1. 配置 802.1x

！使能 802.1x 认证服务器

```
Harbour(config)# config dot1x enable
```

！将连接服务器的端口 23 和 24 的认证状态设为 forceauth

```
Harbour(config)# config port 23-24 dot1x authcontrolledportcontrol forceauth
```

2. 配置 Radius

！增加两台认证计费服务器，每台服务器均具有认证计费功能。设 IP 地址为 192.168.0.252 的 Radius Server (0) 的 ID 为 0，IP 地址为 192.168.0.253 的 Radius Server (1) 的 ID 为 1。

```
Harbour(config)# radius authentication add-server id 0 server-ip 192.168.0.252 client-ip 192.168.0.2
```

```
Harbour(config)# radius accounting add-server id 0 server-ip 192.168.0.252
```

```
client-ip 192.168.0.2
```

```
Harbour(config)# radius authentication add-server id 1 server-ip  
192.168.0.253 client-ip 192.168.0.2
```

```
Harbour(config)# radius accounting add-server id 1 server-ip 192.168.0.253  
client-ip 192.168.0.2
```

根据以上配置，由于 Server（0）是首次添加的认证和计费服务器，因此 Server（0）既是主认证服务器，也是主计费服务器。也可以人为地将 Server（1）指定为主认证服务器或主计费服务器。

！ 设置主认证服务器的共享密钥是 “RADIUS-Authentication”

```
Harbour(config)# radius authentication config-server id 0 shared-secret  
RADIUS-Authentication
```

！ 使能 Radius 认证计费功能

```
Harbour(config)# radius authentication enable
```

```
Harbour(config)# radius accounting enable
```

3.2 多域认证

多域认证的 802.1x 及 Radius 配置与单域认证相同，不同的只是创建一些新的域，并把 Radius 服务器分配到相应的域中。以下我们将介绍实现单域认证的最小配置。

如图 3-2 所示，图中的组网形式与图 3-1 相同，只是将两个服务器分别设在两个域（domain1、domain2）中。

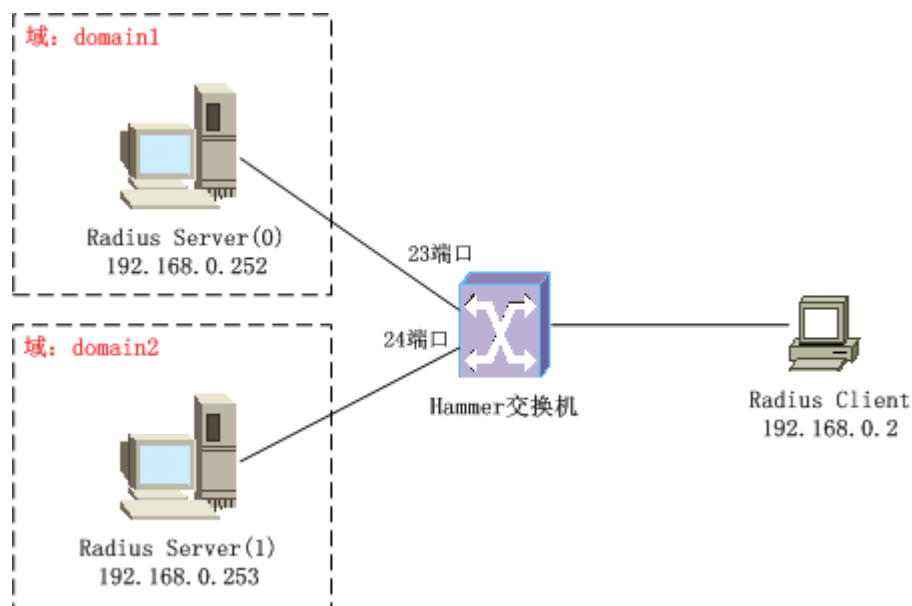


图 3-2 多域认证网络图

配置步骤具体如下：

1. 配置 802.1x

同单域认证配置

2. 配置 Radius

同单域认证配置。

3. 配置域

！ 创建两个域，domain1 和 domain2

```
Harbour(config)# create isp-domain domain1
```

```
Harbour(config)# create isp-domain domain2
```

！ 将两个 Radius 服务器分别添加到 domain1 和 domain2 中

```
Harbour(config)# config isp-domain domain1 authentication add-server id 0
```

```
Harbour(config)# config isp-domain domain1 accounting add-server id 0
```

```
Harbour(config)# config isp-domain domain2 authentication add-server id 1
```

```
Harbour(config)# config isp-domain domain2 accounting add-server id 1
```

根据上述配置，如果用户 user01 要在 Domain2 上通过认证，则需在客户端软件的用户名处输入用户名 user02@Domain2。

3.3 服务器的主备切换

下面以认证服务器的主备切换为例，介绍一下 Radius 服务器主备切换的配置方法。

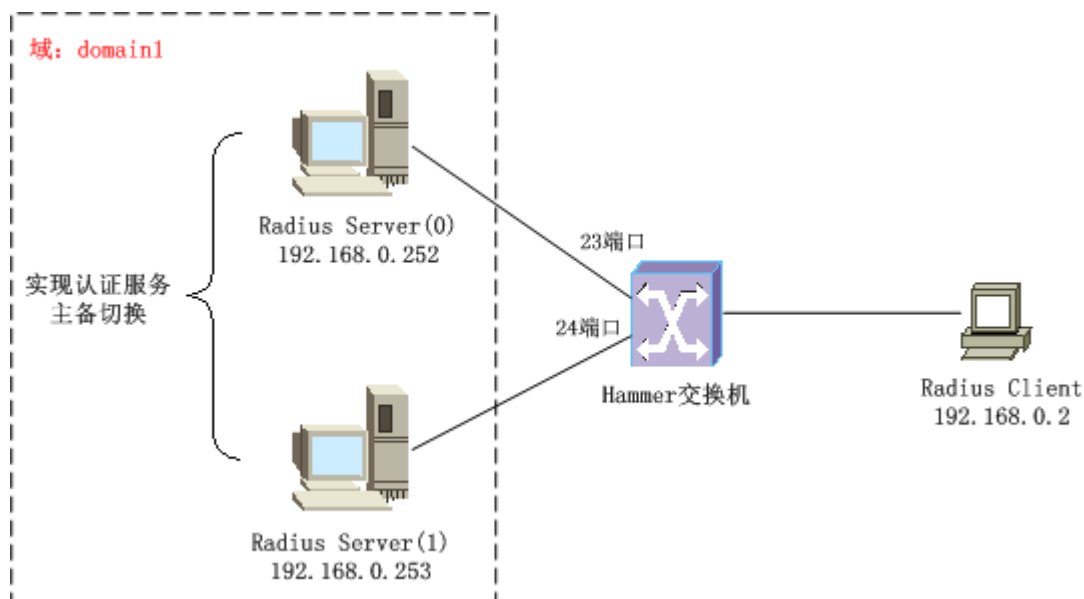


图 3-3 配置认证服务器主备切换

如图 3-3 所示，两台 Radius 服务器在 domain1 域中均为认证服务器，其中，设置 Server（0）为主认证服务器，Server（1）为备用认证服务器。要求在 domain1 域中实现两台服务器主备切换。

配置步骤具体如下：

1. 配置 802.1x

同单域认证配置

2. 配置 Radius

！增加两台认证服务器，设 IP 地址为 192.168.0.252 的 Radius Server（0）的 ID 为 0，IP 地址为 192.168.0.253 的 Radius Server（1）的 ID 为 1。

```
Harbour(config)# radius authentication add-server id 0 server-ip
192.168.0.252 client-ip 192.168.0.2
```

```
Harbour(config)# radius authentication add-server id 1 server-ip
192.168.0.253 client-ip 192.168.0.2
```

！设置认证服务器的共享密钥是“RADIUS-Authentication”

```
Harbour(config)# radius authentication config-server id 0 shared-secret
RADIUS-Authentication
```

```
Harbour(config)# radius authentication config-server id 1 shared-secret
RADIUS-Authentication
```

！使能 Radius 认证功能

```
Harbour(config)# radius authentication enable
```

！启动 Radius 认证服务器主备切换功能

```
Harbour(config)# radius authentication server-switch enable
```

3. 配置域

！创建域 domain1

```
Harbour(config)# create isp-domain domain1
```

！将两个 Radius 服务器添加到 domain1 域中

```
Harbour(config)# config isp-domain domain1 authentication add-server id 0
```

```
Harbour(config)# config isp-domain domain1 authentication add-server id 1
```

！配置域的认证模式为 primary-backup

```
Harbour(config)# config isp-domain domain1 authentication mode
primary-backup
```

3.4 基于 802.1x 的动态限速

！配置 DHCP Relay

略

！设置上行端口，如端口 24（注意：上行端口应与用户端口不在同一个 VLAN）

```
Harbour(config)# config dot1x uplink-port 24
```

！启用 L3 限速功能

```
Harbour(config)# config dot1x access-limit route-engine rate
```

！配置接收带宽值的 Radius 属性。例如，使用 26 号厂商自定义属性携带 Radius 服务器返回的上下行带宽信息，厂商定义的上行带宽为 2，下行带宽为 5，厂商代码是 1234

```
Harbour(config)# radius config-attribute access-bandwidth uplink
vendor-specific 2 1234
```

```
Harbour(config)# radius config-attribute access-bandwidth downlink
vendor-specific 5 1234
```

！查看配置结果

```
Harbour(config)# show radius custom-attributes
```

Attribute	Attribute Type	ValueType	STD/VSA	VendorId
Uplink-Bandwidth	2	integer	VSA	1234
Downlink-Bandwidth	5	integer	VSA	1234
Uplink-Priority	3	integer	VSA	8212(harbour)
Downlink-Priority	4	integer	VSA	8212(harbour)
Intra-Vid	5	integer	VSA	8212(harbour)
Extra-Vid	6	integer	VSA	8212(harbour)

FILTER-ID	7	integer	VSA	8212(harbour)
harbour vlan ip	1	integer	VSA	8212(harbour)
harbour vlan id	32	integer	VSA	8212(harbour)
harbour path track	33	integer	VSA	8212(harbour)

Total 10 custom attributes shown

! Framed Protocol 属性不需配置，默认每个认证和计费报文中都携带此属性，属性值为 PPP(1)

! 返回带宽值的单位默认为 bps，可以配置成 kbps。

显示带宽值的单位，输入命令：

```
Harbour(config)# show radius config-attribute bandwidth-unit
radius access bandwidth unit is bps.
```

若 Radius 服务器返回带宽的单位是 kbps，则可用以下命令配置接收带宽的单位也为 kbps

```
Harbour(config)# radius config-attribute access-bandwidth unit kbps
```

例如，若限制用户的上下行带宽都为 512kbps，则从 Radius 服务器返回的带宽值应为 512，若设置成功将显示如下结果：

```
Harbour(config)#show customer-profile
Customer profile total: 2
```

NAME	IN-BW	VID	PROTO	SIPADDR	DIPADDR	SPORT	DPORT..... (略)
d2560	512	0	NULL	0.0.0.0/0	11.0.0.110/32	0	0
u2560	512	0	NULL	11.0.0.110/32	0.0.0.0/0	0	0

附录 接入服务命令集

命令

config dot1x [enable|disable]

config dot1x access-limit route-engine [rate|acl|disable]

config dot1x binduser [add|delete] port [<portlist>|all] user <username>

config dot1x binduser [enable|disable]

config dot1x binduser clear-all

config dot1x binduser multi-port-per-user [enable|disable]

config dot1x clear-statistic

config dot1x keepalive [enable|disable]

config dot1x keepalive max-no-response-count <2-30>

config dot1x keepalive mechanism [ping-pong|state-machine]

config dot1x keepalive period <10-3600>

config dot1x max-req <1-10>

config dot1x multiple-host-one-port max-host-count <2-512>

config dot1x pae force-logoff IP <A.B.C.D>

config dot1x pae force-logoff all

config dot1x pae force-logoff id <paeid>

config dot1x pae force-logoff isp-domain <domain>

config dot1x pae force-logoff mac <usermac> {port <portno>}*1

config dot1x pae force-logoff port <portno>

config dot1x pae force-logoff username <username>

config dot1x quiet-period <0-32767>

功能描述

使能/关闭 802.1x 认证服务
配置是否启动基于三层模块的限速及访问控制列表功能
在端口处添加或删除绑定的用户

使能或禁止用户绑定功能
清除所有用户绑定信息

使能或关闭一个用户绑定到多个端口的功能

清除 802.1x 统计信息

启动或关闭异常下线检测功能

设置允许客户端未响应的最大次数

设置异常下线检测的方法

设置发送异常下线检测报文的时间间隔

设置交换机向客户端重传数据帧的最大次数

设置一个端口最多允许接入客户端的数目

根据客户端的 IP 地址强制用户退出认证状态

强制所有用户退出认证状态
根据端口访问实体 (PAE) 的 ID 号强制用户退出认证状态

根据 ISP 域名强制用户退出认证状态

根据客户端的 MAC 地址强制用户退出认证状态

根据端口号强制用户退出认证状态

根据用户名强制用户退出认证状态

设置在一次认证失败后的多长时间内认证系统不接收来

<code>config dot1x re-authentication [enable disable]</code>	自客户端系统的认证请求使能/关闭重新认证机制
<code>config dot1x re-authentication period <1-32767></code>	设置重新认证的时间间隔
<code>config dot1x server-timeout <1-32767></code>	设置认证系统接收来自认证服务器数据包的超时时间
<code>config dot1x supp-timeout <1-32767></code>	设置认证系统接收来自客户端系统数据包的超时时间
<code>config dot1x tx-period <1-32767></code>	设置认证系统向客户端系统重传 EAP-Request/Identity 数据帧的时间间隔
<code>config dot1x uplink-port <portno></code>	配置上行端口号
<code>config isp-domain <domain> accounting [add-server delete-server] id <id></code>	向域中添加/删除计费服务器
<code>config isp-domain <domain> accounting [enable disable]</code>	启动/禁止域内的 Radius 计费功能
<code>config isp-domain <domain> accounting config-server id <id> type [primary multi backup]</code>	配置计费服务器在域中的类型
<code>config isp-domain <domain> accounting interim-update-accounting disable</code>	关闭即时计费请求发送功能
<code>config isp-domain <domain> accounting interim-update-accounting interval <10-65535></code>	配置即时计费请求的时间间隔，并打开发送功能
<code>config isp-domain <domain> accounting mode [independent primary-backup multi]</code>	配置域中 Radius 计费服务器的计费模式
<code>config isp-domain <domain> accounting start-need-ip [enable disable]</code>	配置发送计费开始请求之前是否必须先得到用户 IP 地址
<code>config isp-domain <domain> accounting sync [enable disable]</code>	配置交换机重新启动后是否向 Radius 服务器发送计费同步报文
<code>config isp-domain <domain> accounting wait-ip <100-600></code>	配置交换机等待客户端获取 IP 地址的最长时间
<code>config isp-domain <domain> authentication [add-server delete-server] id <id></code>	向域中添加/删除认证服务器
<code>config isp-domain <domain> authentication [enable disable]</code>	启动/禁止域内的 Radius 认证功能
<code>config isp-domain <domain> authentication config-server id <id> type primary</code>	指定主认证服务器
<code>config isp-domain <domain> authentication mode [independent primary-backup]</code>	设置域的认证模式
<code>config isp-domain <domain> authentication type [pap chap eap-md5]</code>	配置域的认证方式
<code>config isp-domain <domain> supplicant-upgrade force-upgrade [enable disable]</code>	使能通过 URL 升级客户端软件的功能
<code>config isp-domain <domain> supplicant-upgrade url [<url> NULL]</code>	设置客户端软件升级的 URL
<code>config isp-domain <domain> username [complete incomplete]</code>	设置是否将完整的用户名发

<code>config port [<portlist> all] dot1x authcontrolledportcontrol</code>	送给 Radius 服务器
<code>[auto forceauth forceunauth]</code>	配置端口的认证状态
<code>config port [<portlist> all] dot1x port-control-mode [MAC-based port-based]</code>	配置端口的控制模式
<code>create isp-domain <domain></code>	创建一个名为<domain>的域
<code>delete isp-domain <domain></code>	删除一个名为<domain>的域
<code>radius [accounting authentication] server-switch [enable disable]</code>	使能/禁止 Radius Server 主备切换功能
<code>radius accounting add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1</code>	增加 Radius 计费服务器
<code>radius accounting config-server id <0-4> max-retransmit-count <2-10></code>	设置向计费服务器重传数据包的最大次数
<code>radius accounting config-server id <0-4> max-retransmit-drop-count <2-30></code>	设置最大重传丢弃数，用于检验计费服务器是否断线
<code>radius accounting config-server id <0-4> max-send-fail-count <2-30></code>	设置最大重传失败数，用于检验计费服务器是否断线
<code>radius accounting config-server id <0-4> retransmit-interval <5-300></code>	设置向计费服务器重传数据包的时间间隔
<code>radius accounting config-server id <0-4> shared-secret <secret></code>	设置计费服务器与客户端之间的共享密钥
<code>radius accounting config-server id <0-4> status activ</code>	设置计费服务器的当前状态为 active
<code>radius accounting delete-server id <0-4></code>	删除 Radius 计费服务器
<code>radius accounting disable</code>	关闭 Radius 计费功能
<code>radius accounting enabled</code>	启动 Radius 计费功能
<code>radius accounting session-timeout-type [logoff reauthenticate]</code>	设置 Session Timeout 的处理机制
<code>radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1</code>	增加 Radius 认证服务器
<code>radius authentication config-server id <0-4> max-retransmit-count <2-10></code>	设置向认证服务器重传数据包的最大次数
<code>radius authentication config-server id <0-4> max-retransmit-drop-count <2-30></code>	设置最大重传丢弃数，用于检验认证服务器是否断线
<code>radius authentication config-server id <0-4> max-send-fail-count <2-30></code>	设置最大重传失败数，用于检验认证服务器是否断线
<code>radius authentication config-server id <0-4> retransmit-interval <5-300></code>	设置向认证服务器重传数据包的时间间隔
<code>radius authentication config-server id <0-4> shared-secret <secret></code>	设置认证服务器与客户端之间的共享密钥
<code>radius authentication config-server id <0-4> status active</code>	设置认证服务器的当前状态

radius authentication delete-server id <0-4>	为 active 删除 Radius 认证服务器
radius authentication disable	关闭 Radius 认证功能
radius authentication enable	启动 Radius 认证功能
radius config-attribute access-bandwidth [uplink downlink] Vendor-Specific <VendorType> {<VendorId>}*1	从 26 号厂商自定义属性接收 Radius 服务器返回的上下行带宽值
radius config-attribute access-bandwidth [uplink downlink] default-value	设置上下行带宽属性类型的默认值
radius config-attribute access-bandwidth [uplink downlink] standard <1-255>	从标准属性中接收 Radius 服务器返回的上下行带宽值
radius config-attribute access-bandwidth unit [bps kbps]	配置 Radius 服务器返回带宽值的单位
radius config-attribute all default-value	恢复所有可配置的 Radius 属性类型的默认值
radius config-attribute filter-id Vendor-Specific <VendorType> {<VendorId>}*1	从 26 号厂商自定义属性接收 Radius 服务器返回的用户 ACL ID
radius config-attribute filter-id default-value	设置访问控制列表属性类型的默认值
radius config-attribute filter-id standard <1-255>	从标准属性中接收 Radius 服务器返回的用户 ACL ID
radius config-attribute frame-protocol <0-255>	配置 Frame-Protocol 的属性值
radius config-attribute frame-protocol default	设置 frame-protocol 属性的默认值
radius config-attribute nas-port-type <0-255>	配置 nas-port-type 的属性值
radius config-attribute nas-port-type default	设置 frame-protocol 属性的默认值
radius config-attribute path-track Vendor-Specific <VendorType> {<VendorId>}*1	使用 26 号厂商自定义属性传递端口反查信息到 Radius 服务器
radius config-attribute path-track default-value	设置端口反查属性类型的默认值
radius config-attribute path-track standard <1-255>	使用标准属性传递用户的端口反查信息到 Radius 服务器
radius config-attribute source-mac standard <100-255>	使用标准属性向 Radius 服务器传递用户的 MAC 信息
radius config-attribute vlan-id Vendor-Specific <VendorType> {<VendorId>}*1	设置通过厂商属性携带

radius config-attribute vlan-id default-value	VLAN ID 信息 设置 VLAN ID 属性的默认值
radius config-attribute vlan-id standard <1-255>	设置用标准属性类型 <1-255>中的哪个属性携带 VLAN ID 信息
radius config-attribute vlan-ip Vendor-Specific <VendorType> {<VendorId>}*1	使用 26 号厂商自定义属性 传递用户 VLAN IP 到 Radius 服务器
radius config-attribute vlan-ip default-value	设置 VLAN IP 属性的默认值
radius config-attribute vlan-ip standard <1-255>	使用标准属性传递用户的 VLAN IP 到 Radius 服务器
radius cut add-server [authentication accounting] id <0-4> {udp-port <1-6500>}*1	向列表中增加一个认证或计 费服务器
radius cut delete-server [authentication accounting] id <0-4>	从列表中删除一个认证或计 费服务器
radius cut disable	关闭接收 CUT 报文功能
radius cut enable	启动接收 CUT 报文功能
radius cut process-by [reauthentication logoff]	设置处理 CUT 请求机制
radius cut verify-by [authenticator message-authenticator none]	设置校验 CUT 报文的方式
config radius serverswitch-notify [enable disable]	设置是否将主备切换信息通 知给 dot1x 模块
show dot1x	显示 802.1x 功能开启或关 闭的状态以及相关的参数配 置信息
show dot1x access-limit route-engine	显示基于三层模块的限速及 访问控制列表功能的配置信 息
show dot1x binduser multi-port-per-user status	显示绑定多个端口的用户信 息
show dot1x binduser port [<portlist> all]	显示某一端口上的用户绑定 信息
show dot1x binduser status	显示全部端口绑定信息
show dot1x binduser user <username>	根据用户名显示端口绑定信 息
show dot1x pae all	显示所有 PAE
show dot1x pae id <id>	根据 PAE ID 索引值显示与之 对应的 PAE 信息
show dot1x pae isp-domain <domain>	根据所在的域显示 PAE
show dot1x pae mac <address> {port <portno>}*1	根据 mac 地址显示对应的端 口访问实体 PAE 绑定的用户 mac 地址、Authenticator 状态、后台认证状态、重认

	证状态等信息
show dot1x pae port <portno>	根据端口号显示与之相关联的所有创建的 PAE 信息，以及 PAE 总数
show dot1x pae username <username>	根据用户名显示与之对应的端口访问实体 PAE 相关信息
show dot1x statistic	显示 802.1x 统计信息
show dot1x uplink-port	查看上行端口
show dot1x vlan <vlanname> pae	根据 VLAN 显示 PAE
show dot1x vlan <vlanname> user-count	显示 VLAN 中的认证用户数
show nas accounting-statistic	显示计费统计信息
show nas version	显示 NAS 版本信息
show port [<portlist> all] dot1x	显示一组端口对应的 802.1x 相关信息，包括端口号、当前创建的 PAE 实体的个数以及在某一时刻曾经创建过最多的 PAE 实体的个数
show radius [accounting authentication] server-switch	显示 Radius 认证或计费服务器的主备倒换功能是否启用
show radius accounting session-timeout-type	显示计费服务器的 Session Timeout 类型
show radius config-attribute bandwidth-unit	显示 Radius 服务器返回带宽值的单位
show radius config-attribute frame-protocol	显示 Frame-Protocol 属性的值
show radius config-attribute nas-port-type	显示 Nas-Port-Type 属性的值
show radius custom-attributes	显示 Radius 属性类型
show radius cut process-way	显示 CUT 请求处理机制
show radius cut verify-way	显示 CUT 报文校验方式
show radius idpool	显示 Radius 服务器 ID 号的使用情况，用于调试
show radius {configuration}*1	显示 Radius 配置信息