目 录

1 802.1X

说明

- 本章节主要描述了 802.1X 的相关概念及配置步骤。由于通过配置端口安全特性也可以为用户提供 802.1X 认证服务，且还可以提供 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性。而在仅需要 802.1X 特性来完成接入控制的组网环境下，推荐单独使用 802.1X 特性。关于端口安全特性的详细介绍和具体配置请参见“安全配置指导”中的“端口安全”。
- 802.1X 仅在 SAP 板工作在二层模式时支持。

1.1 802.1X简介

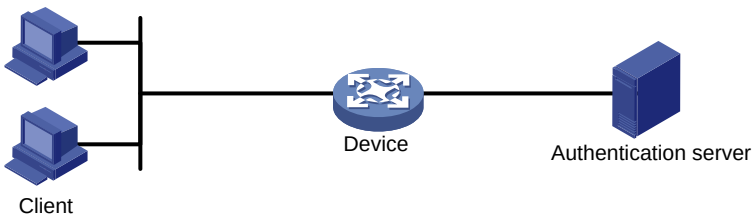
最初，IEEE802 LAN/WAN 委员会为解决无线局域网的网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户设备进行认证，以便控制用户设备对网络资源的访问。

1.1.1 802.1X的体系结构

802.1X系统中包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Authentication server），如图 1-1所示。。

图1-1 802.1X 系统的体系结构图



- 客户端是请求接入局域网的用户终端设备，它由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端是局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口（物理端口或逻辑端口），并通过与服务器的交互来对所连接的客户端进行认证。
- 认证服务器用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户

端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即由设备端对客户端进行本地认证、授权和计费。

1.1.2 802.1X对端口的控制

1. 受控/非受控端口

设备端为客户端提供接入局域网的端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

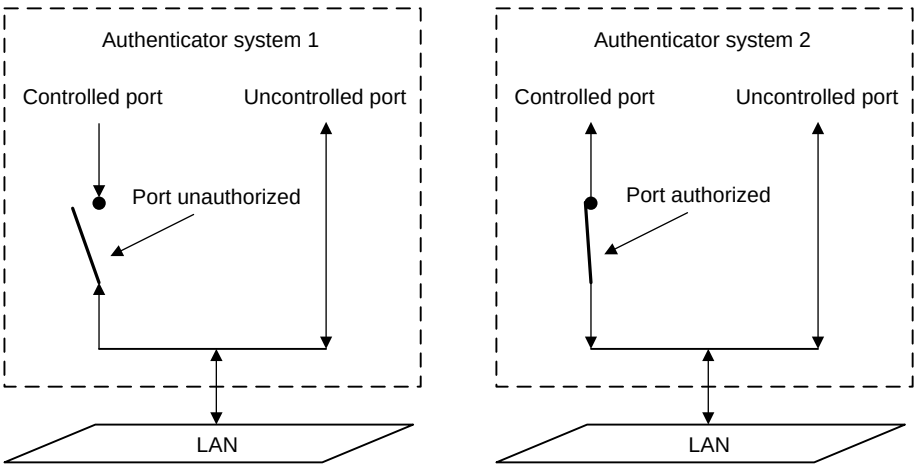
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

1. 授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权状态进行相应地控制。

图 1-2显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X认证系统的端口状态。系统 1 的受控端口处于非授权状态，不允许报文通过；系统 2 的受控端口处于授权状态，允许报文通过。

图1-2 受控端口上授权状态的影响



2. 受控方向

在非授权状态下，受控端口可以处于单向受控或双向受控状态。

- 处于双向受控状态时，禁止帧的发送和接收；
- 处于单向受控状态时，禁止从客户端接收帧，但允许向客户端发送帧。

说明

目前，设备上的受控端口只能处于单向受控状态。

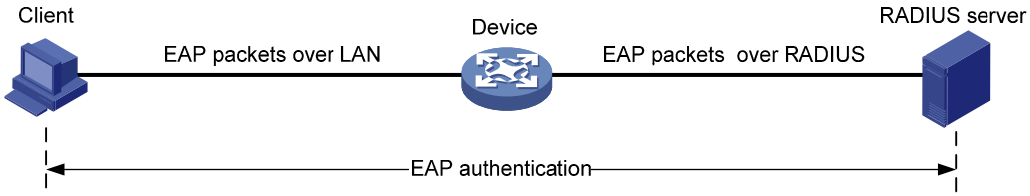
1.1.3 802.1X认证报文的交互机制

802.1X 系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交互。EAP 是一种 C/S 模式的认证框架，它可以支持多种认证方法，例如 MD5-Challenge、EAP-TLS、PEAP 等。在客户端与设备端之间，EAP 报文使用 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）封装格式承载于数据帧中传递。在设备端与 RADIUS 服务器之间，EAP 报文的交互有以下两种处理机制。

1. EAP中继

设备对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器进行认证。

图1-3 EAP 中继原理示意图

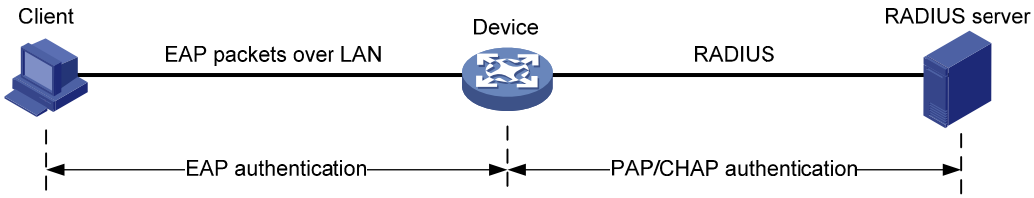


该处理机制下，EAP 认证过程在客户端和 RADIUS 服务器之间进行，RADIUS 服务器作为 EAP 服务器来处理客户端的 EAP 认证请求，设备相当于一个代理，仅对 EAP 报文做中转，因此设备处理简单，并能够支持 EAP 的各种认证方法，但要求 RADIUS 服务器支持相应的 EAP 认证方法。

2. EAP终结

设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）方法进行认证。

图1-4 EAP 终结原理示意图



该处理机制下，由于现有的 RADIUS 服务器基本均可支持 PAP 认证和 CHAP 认证，因此对服务器无特殊要求，但设备处理较为复杂，它需要作为 EAP 服务器来解析与处理客户端的 EAP 报文，且目前仅能支持 MD5-Challenge 类型的 EAP 认证以及 iNode 802.1X 客户端发起的“用户名+密码”方式的 EAP 认证。

说明

如果客户端采用了 MD5-Challenge 类型的 EAP 认证，则设备端只能采用 CHAP 认证；如果 iNode 802.1X 客户端采用了“用户名+密码”方式的 EAP 认证，设备上可选择使用 PAP 认证或 CHAP 认证，从安全性上考虑，通常使用 CHAP 认证。

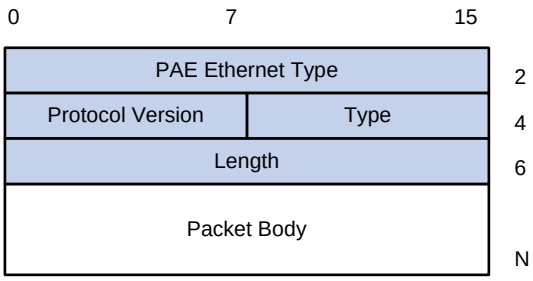
1.1.4 EAP报文的封装

1. EAPOL数据帧的封装

(1) EAPOL 数据帧的格式

EAPOL是 802.1X协议定义的一种承载EAP报文的封装协议，主要用于在局域网中传送客户端和设备端之间的EAP协议报文。EAPOL数据包的格式如图 1-5所示。

图1-5 EAPOL 数据包格式



- PAE Ethernet Type：表示协议类型。EAPOL 的协议类型为 0x888E。
- Protocol Version：表示 EAPOL 数据帧的发送方所支持的 EAPOL 协议版本号。
- Type：表示EAPOL数据帧类型。目前设备上支持的EAPOL数据帧类型见表 1-1。

表1-1 EAPOL 数据帧类型

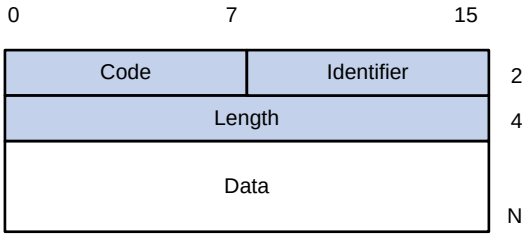
类型值	数据帧类型	说明
0x00	EAP-Packet	认证信息帧，用于承载客户端和设备端之间的EAP报文。 ● 在终结方式下，该帧中的客户端认证信息会被设备端重新封装并承载于 RADIUS 报文中发送给认证服务器 ● 在中继方式下，该帧承载的 EAP 报文会被设备端直接封装在 RADIUS 报文的 EAP 属性中发送给认证服务器
0x01	EAPOL-Start	认证发起帧，用于客户端向设备端发起认证请求
0x02	EAPOL-Logoff	退出请求帧，用于客户端向设备端发起下线请求

- Length：表示数据域的长度，也就是Packet Body字段的长度，单位为字节。当EAPOL数据帧的类型为 EAPOL-Start 或 EAPOL-Logoff 时，该字段值为 0，表示后面没有 Packet Body 字段。
- Packet Body：数据域的内容。

(2) EAP 报文的格式

当EAPOL数据帧的类型为EAP-Packet时，Packet Body字段的内容就是一个EAP报文，格式如图1-6所示。

图1-6 EAP 报文格式



- Code：EAP 报文的类型，包括 Request（1）、Response（2）、Success（3）和 Failure（4）。
- Identifier：用于匹配 Request 消息和 Response 消息的标识符。
- Length：EAP 报文的长度，包含 Code、Identifier、Length 和 Data 域，单位为字节。
- Data：EAP 报文的内容，该字段仅在 EAP 报文的类型为 Request 和 Response 时存在，它由类型域和类型数据两部分组成，例如，类型域为 1 表示 Identity 类型，类型域为 4 表示 MD5 challenge 类型。

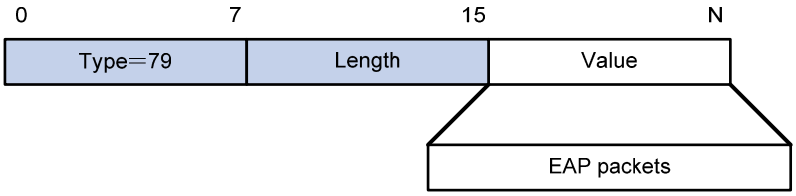
2. EAP报文在RADIUS中的封装

RADIUS 为支持 EAP 认证增加了两个属性：EAP-Message（EAP 消息）和 Message-Authenticator（消息认证码）。在含有 EAP-Message 属性的数据包中，必须同时包含 Message-Authenticator 属性。关于 RADIUS 报文格式的介绍请参见“安全配置指导”中的“AAA”的 RADIUS 协议简介部分。

(1) EAP-Message

如图 1-7所示，EAP-Message属性用来封装EAP报文，Value域最长 253 字节，如果EAP报文长度大于 253 字节，可以对其进行分片，依次封装在多个EAP-Message属性中。

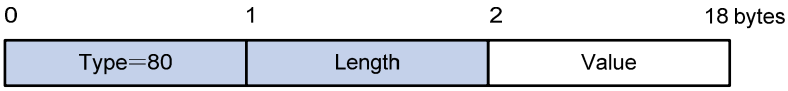
图1-7 EAP-Message 属性封装



(2) Message-Authenticator

如图 1-8所示，Message-Authenticator属性用于在EAP认证过程中验证携带了EAP-Message属性的RADIUS报文的完整性，避免报文被窜改。如果接收端对接收到的RADIUS报文计算出的完整性校验值与报文中携带的Message-Authenticator属性的Value值不一致，该报文会被认为无效而丢弃。

图1-8 Message-Authenticator 属性封装



1.1.5 802.1X的认证触发方式

802.1X 的认证过程可以由客户端主动发起，也可以由设备端发起。

1. 客户端主动触发方式

- 组播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。
- 广播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文的目的地址为广播 MAC 地址。该方式可解决由于网络中有些设备不支持上述的组播报文，而造成认证设备无法收到客户端认证请求的问题。

说明

目前，iNode 的 802.1X 客户端可支持广播触发方式。

2. 设备端主动触发方式

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 组播触发：设备每隔 N 秒（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。
- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

1.1.6 802.1X的认证过程

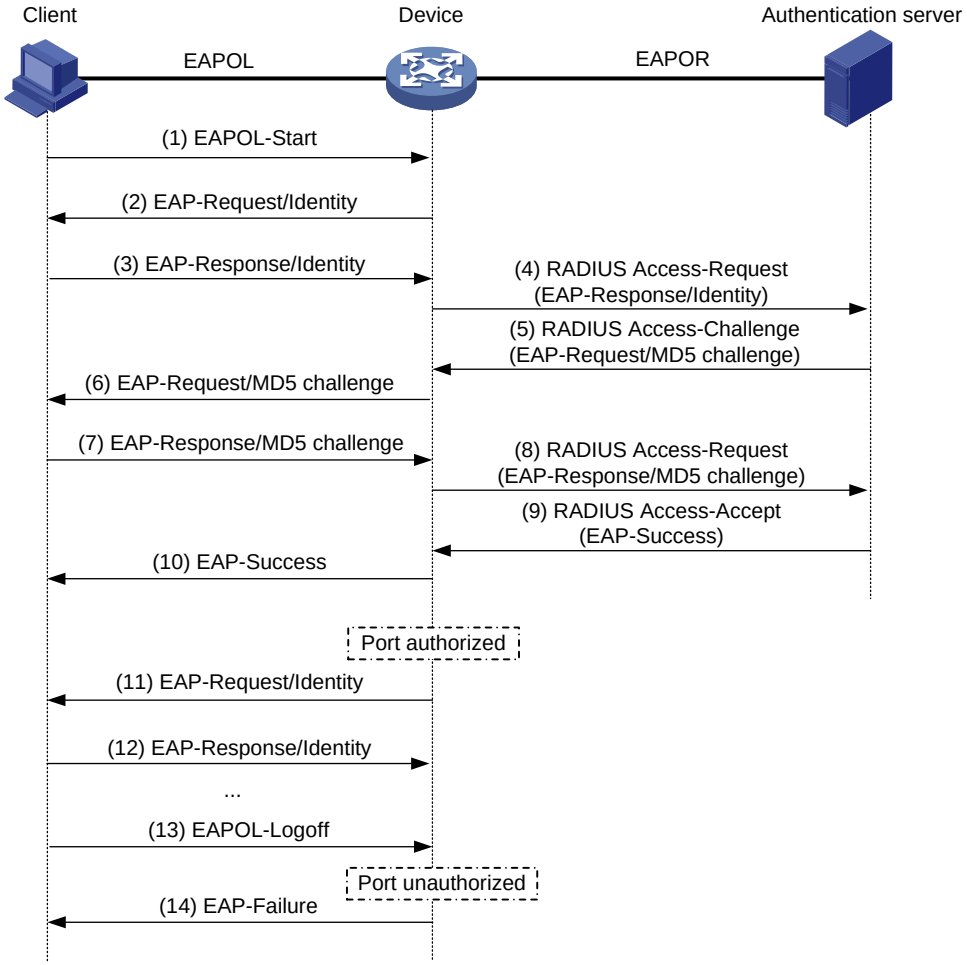
802.1X 系统支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP 承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以MD5-Challenge认证方法为例介绍基本业务流程，认证过程如图 1-9所示。

图1-9 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



(1) 当用户需要访问外部网络时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求。此时，客户端程序将向设备端发出认证请求帧（EAPOL-Start），开始启动一次认证过程。

(2) 设备端收到认证请求帧后，将发出一个 Identity 类型的请求帧（EAP-Request/Identity）要求用户的客户端程序发送输入的用户名。

(3) 客户端程序响应设备端发出的请求，将用户名信息通过 Identity 类型的响应帧（EAP-Response/Identity）发送给设备端。

(4) 设备端将客户端发送的响应帧中的 EAP 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给认证服务器进行处理。

(5) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名列表中对比，找到该用户名对应的密码信息，用随机生成的一个 MD5 Challenge 对密码进行加密处理，同时将此 MD5 Challenge 通过 RADIUS Access-Challenge 报文发送给设备端。

(6) 设备端将 RADIUS 服务器发送的 MD5 Challenge 转发给客户端。

(7) 客户端收到由设备端传来的 MD5 Challenge 后，用该 Challenge 对密码部分进行加密处理，生成 EAP-Response/MD5 Challenge 报文，并发送给设备端。

(8) 设备端将此 EAP-Response/MD5 Challenge 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给 RADIUS 服务器。

(9) RADIUS 服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，并向设备端发送认证通过报文（RADIUS Access-Accept）。

(10) 设备收到认证通过报文后向客户端发送认证成功帧（EAP-Success），并将端口改为授权状态，允许用户通过端口访问网络。

(11) 用户在线期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。

(12) 客户端收到握手报文后，向设备发送应答报文，表示用户仍然在线。缺省情况下，若设备端发送的两次握手请求报文都未得到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

(13) 客户端可以发送 EAPOL-Logoff 帧给设备端，主动要求下线。

(14) 设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

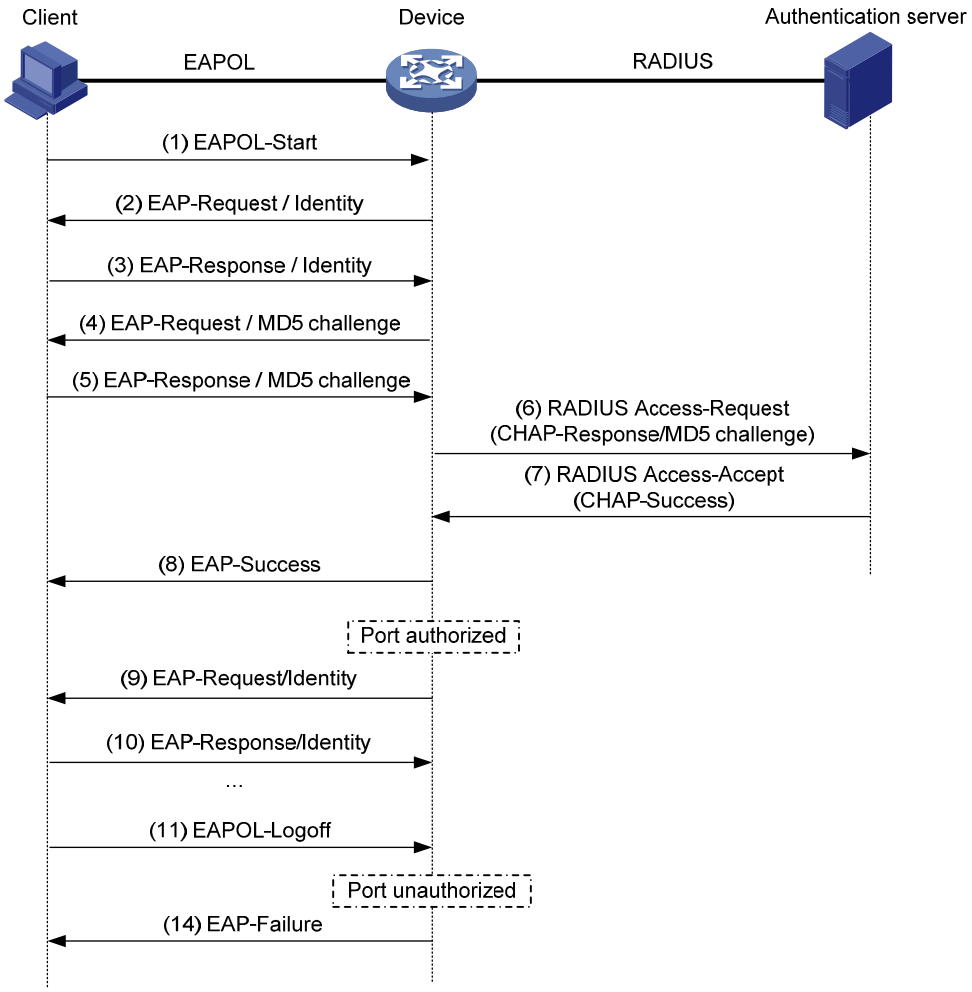
说明

EAP 中继方式下，需要保证在客户端和 RADIUS 服务器上选择一致的 EAP 认证方法，而在设备上，只需要通过 **dot1x authentication-method eap** 命令启动 EAP 中继方式即可。

2. EAP终结方式

这种方式将EAP报文在设备端终结并映射到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。设备端与RADIUS服务器之间可以采用PAP或者CHAP认证方法。下面以CHAP认证方法为例介绍基本业务流程，如图 1-10所示。

图1-10 IEEE 802.1X 认证系统的 EAP 终结方式业务流程



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于步骤(4)中用来对用户密码信息进行加密处理的 MD5 challenge 由设备端生成，之后设备端会把用户名、MD5 challenge 和客户端加密后的密码信息一起送给 RADIUS 服务器，进行相关的认证处理。

1.1.7 802.1X的接入控制方式

设备不仅支持协议所规定的基于端口的接入认证方式（Port-based），还对其进行了扩展、优化，支持基于 MAC 的接入控制方式（MAC-based）。

- 当采用基于端口的接入控制方式时，只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 采用基于 MAC 的接入控制方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。

1.2 802.1X扩展功能

1.2.1 支持VLAN下发

802.1X 用户在服务器上通过认证时，服务器会把授权信息传送给设备端。如果服务器上指定了授权给该用户的下发 VLAN，则服务器发送给设备的授权信息中将含有下发的 VLAN 信息，设备根据用户认证上线的端口链路类型，按以下三种情况将端口加入下发 VLAN 中。

表1-1 不同类型的端口加入下发的 VLAN

接入控制方式	Access 端口	Trunk 端口	Hybrid 端口
Port-based	端口离开用户配置的VLAN，加入下发的VLAN	端口允许下发的VLAN通过，并且将缺省VLAN修改为下发的VLAN	端口允许下发的VLAN以不携带Tag的方式通过，并且将缺省VLAN修改为下发的VLAN
MAC-based	端口离开用户配置的VLAN，加入第一个通过认证的用户的下发VLAN	端口允许下发的VLAN通过，并且将缺省VLAN修改为第一个通过认证的用户的下发VLAN	端口允许下发的VLAN以不携带Tag的方式通过 • 若端口上开启了 MAC VLAN 功能，则根据下发的 VLAN 动态地创建基于用户 MAC 的 VLAN，而端口的缺省 VLAN ID 并不改变 • 若端口上未开启 MAC VLAN 功能，则端口的缺省 VLAN ID 修改为第一个通过认证的用户的下发 VLAN 的 VLAN ID
	说明：只有开启了MAC VLAN功能的端口上才允许给不同的用户MAC下发不同的VLAN。其它情况下，下发给所有用户的VLAN必须相同，否则仅第一个通过认证的用户的可以认证成功。		

下发的 VLAN 并不影响端口的配置。但是，下发的 VLAN 的优先级高于用户配置的 VLAN，即通过认证后起作用的 VLAN 是下发的 VLAN，用户配置的 VLAN 在用户下线后生效。

说明

- 对于 Hybrid 端口，不建议把服务器将要下发或已经下发的 VLAN 配置为携带 Tag 的方式加入端口。
- 在启动了 802.1X 周期性重认证功能的 Hybrid 端口上，若用户在 MAC VLAN 功能开启之前上线，则 MAC VLAN 功能不能对该用户生效，即系统不会根据服务器下发的 VLAN 生成该用户的 MAC VLAN 表项，只有该在线用户重认证成功且服务器下发的 VLAN 发生变化时，MAC VLAN 功能才会对它生效。MAC VLAN 功能的详细介绍请参考“二层技术-以太网交换配置指导”中的“VLAN”。

1.2.2 Guest VLAN

Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。这个特定的 VLAN 称之为 Guest VLAN，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。

根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。SR6600 目前仅支持端口的接入控制方式为 Port-based。

在接入控制方式为Port-based的端口上配置Guest VLAN后，若在一定的时间内（默认 90 秒），该端口上无客户端进行认证，则该端口将被加入Guest VLAN，所有在该端口接入的用户将被授权访问Guest VLAN里的资源。不同链路类型的端口加入Guest VLAN的情况有所不同，具体情况与端口加入服务器下发的VLAN类似，请参见“1.2.1 支持VLAN下发”。

当端口上处于Guest VLAN中的用户发起认证且失败时：如果端口配置了Auth-Fail VLAN，则该端口会被加入Auth-Fail VLAN；如果端口未配置Auth-Fail VLAN，则该端口仍然处于Guest VLAN内。关于Auth-Fail VLAN的具体介绍请参见“1.2.3 Auth-Fail VLAN”。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

1.2.3 Auth-Fail VLAN

Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Auth-Fail VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

根据端口的接入控制方式不同，Auth-Fail VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port-based

在接入控制方式为 Port-based 的端口上配置 Auth-Fail VLAN 后，若该端口上有用户认证失败，则该端口会被加入到 Auth-Fail VLAN，所有在该端口接入的用户将被授权访问 Auth-Fail VLAN 里的资源。端口加入 Auth-Fail VLAN 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

当加入 Auth-Fail VLAN 端口上有用户发起认证并失败时，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口会离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Auth-Fail VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

(2) 端口的接入控制方式为 MAC-based

在接入控制方式为 MAC-based 的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的 VLAN 中，或回到加入 Auth-Fail VLAN 之前端口所在的初始 VLAN；如果认证失败，则该用户仍然留在该 VLAN 中。

1.1.2 Critical VLAN

Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port-based

在接入控制方式为 Port-based 的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到 Critical VLAN，之后所有在该端口接入的用户将被授权访问 Critical VLAN 里的资源。端口加入 Critical VLAN 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

(2) 端口的接入控制方式为 MAC-based

在接入控制方式为 MAC-based 的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果满足以下任意一个条件，端口将会离开 Critical VLAN：

- 用于认证用户的 ISP 域中的认证服务器配置有所变化，包括修改、新增或删除服务器。
- RADIUS 认证服务器恢复为 active 状态。
- 通过命令行将 RADIUS 认证服务器的状态置为 active。
- 配置了 RADIUS 认证服务器探测功能，且探测结果表示某认证服务器可达。

如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN 则，则该端口将会加入 Auth-Fail VLAN；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口会离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Critical VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

说明

- 只采用 RADIUS 认证方式的情况下，在认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。
- RADIUS 服务器相关的配置请参见“安全配置指导”中的“AAA”。

1.2.4 支持ACL下发

802.1X 支持 ACL（Access Control List，访问控制列表）下发功能提供了对上线用户访问网络资源的过滤与控制功能。当用户上线时，如果 RADIUS 服务器上指定了要下发给该用户的授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行过滤，仅允许 ACL 规则中允许的数据流通过该端口。由于服务器上指定的是授权 ACL 的编号，因此还需要在设备上创建该 ACL 并配置该对应的 ACL 规则。管理员可以通过改变服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

1.3 802.1X配置任务简介

表1-2 802.1X 配置任务简介

配置任务	说明	详细配置
开启802.1X特性	必选	1.4.2
配置802.1X系统的认证方法	若采用EAP中继模式，则必选 若采用EAP终结模式，则可选	1.4.3
配置端口的授权状态	可选	1.4.4
配置端口接入控制方式	可选	1.4.5
配置端口同时接入用户数的最大值	可选	1.4.6
配置设备向接入用户发送认证请求报文的最大次数	可选	1.4.7
配置802.1X认证超时定时器	可选	1.4.8
配置在线用户握手功能	可选	1.4.9
配置代理检测与控制功能	可选	1.4.10
开启认证触发功能	可选	1.4.11
配置端口的强制认证域	可选	1.4.12
配置静默功能	可选	1.4.13
配置重认证功能	可选	1.4.14
配置Guest VLAN	可选	1.4.15
配置Auth-Fail VLAN	可选	1.4.16
配置Critical VLAN	可选	1.4.17
配置802.1X支持的域名分隔符	可选	1.4.18

1.4 配置802.1X

1.4.1 配置准备

802.1X 需要 AAA 的配合才能实现对用户的身份认证。因此，需要首先完成以下配置任务：

- 配置 802.1X 用户所属的 ISP 认证域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。
- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在设备上手动添加认证的用户名和密码。配置本地认证时，用户使用的服务类型必须设置为 **lan-access**。

1.4.2 开启 802.1X特性

说明

- 在用户端设备发送不携带 Tag 数据流的情况下，若接入端口配置了 Voice VLAN 功能，则端口的 802.1X 功能不生效。关于 Voice VLAN 特性请参见“二层技术-以太网交换配置指导”中的“Voice VLAN”。
- 端口启动 802.1X 与端口加入聚合组及端口加入业务环回组互斥。

只有同时开启全局和端口的 802.1X 特性后，802.1X 的配置才能在端口上生效。

表1-3 开启 802.1X 特性

配置步骤		命令	说明
进入系统视图		**system-view**	-
开启全局的802.1X特性		**dot1x**	必选 缺省情况下，全局的802.1X特性为关闭状态
开启端口的802.1X特性	在系统视图下	**dot1x interface** *interface-list*	二者必选其一 缺省情况下，端口的802.1X特性为关闭状态
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x	

说明

端口上同时仅使能了 802.1X 和 MAC 地址认证的情况下，首次接入的 802.1X 用户将直接进行 802.1X 认证，非 802.1X 用户的报文将在 30 秒之后触发 MAC 地址认证。

1.4.3 配置 802.1X系统的认证方法

设备上的 802.1X 系统采用的认证方法与设备对于 EAP 报文的处理机制有关，具体如下：

- EAP 中继方式下，设备端对客户端发送的 EAP 报文进行中继处理，设备上需指定 **authentication-method** 为 **eap** 来启用 EAP 中继方式，并支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。
- EAP 终结方式下，设备端对客户端发送的 EAP 报文进行本地终结，设备上需指定 **authentication-method** 为 **chap** 或 **pap** 来启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 CHAP 或 PAP 类型的认证方法。

表1-4 配置 802.1X 系统的认证方法

配置步骤	命令	说明
进入系统视图	**system-view**	-

配置步骤	命令	说明
配置802.1X系统的认证方法	**dot1x authentication-method { chap | eap | pap }**	可选 缺省情况下，设备启用EAP终结方式，并采用CHAP认证方法

如果采用 EAP 中继认证方式，则设备会把客户端输入的内容直接封装后发给服务器，这种情况下 **user-name-format** 命令的设置无效，**user-name-format** 的介绍请参见“安全命令参考”中的“AAA”。

1.4.4 配置端口的授权状态

通过配置端口的授权状态，可以控制端口上接入的用户是否需要经过认证来访问网络资源。端口支持以下三种授权状态：

- 强制授权（**authorized-force**）：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权（**unauthorized-force**）：表示端口始终处于非授权状态，不允许用户进行认证。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别（**auto**）：表示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。

在系统视图和接口视图下均可进行端口授权状态的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的授权状态进行了配置，则最后执行的配置生效。

表1-5 配置端口的授权状态

配置步骤		命令	说明
进入系统视图		**system-view**	-
配置端口的授权状态	在系统视图下	**dot1x port-control { authorized-force | auto | unauthorized-force } [interface** *interface-list*]	二者可选其一 缺省情况下，端口的授权状态为**auto**
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x port-control { authorized-force | auto | unauthorized-force }	

1.4.5 配置端口接入控制方式

设备支持两种端口接入控制方式：基于端口控制（**portbased**）和基于 MAC 控制（**macbased**）。

在系统视图和接口视图下均可进行端口接入控制方式的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的接入控制方式进行了配置，则最后执行的配置生效。

表1-6 配置端口接入控制方式

配置步骤		命令	说明
进入系统视图		**system-view**	-
配置端口接入控制方式	在系统视图下	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	二者可选其一 缺省情况下，802.1X在端口上进行接入控制方式为**macbased**
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x port-method { **macbased** | **portbased** }	

1.4.6 配置端口同时接入用户数的最大值

在系统视图和接口视图下均可进行端口接入用户数最大值的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的最大接入用户数进行了配置，则最后执行的配置生效。

表1-7 配置端口同时接入用户数的最大值

配置步骤		命令	说明
进入系统视图		**system-view**	-
配置端口同时接入用户数的最大值	在系统视图下	**dot1x max-user** *user-number* [**interface** *interface-list*]	二者可选其一 缺省情况下，端口同时接入用户数的最大值为1024
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x max-user *user-number*	

1.4.7 配置设备向接入用户发送认证请求报文的最大次数

如果设备向用户发送认证请求报文后，在规定的时间里（可通过命令 **dot1x timer tx-period** 或者 **dot1x timer supp-timeout** 设定）没有收到用户的响应，则设备将向用户重发该认证请求报文，若设备累计发送认证请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。

表1-8 配置设备向接入用户发送认证请求报文的最大次数

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置设备向接入用户发送认证请求报文的最大次数	**dot1x retry** *max-retry-value*	可选 缺省情况下，设备最多可向接入用户发送2次认证请求报文

1.4.8 配置 802.1X认证超时定时器

802.1X 认证过程中会启动多个定时器以控制接入用户、设备以及 RADIUS 服务器之间进行合理、有序的交互。可配置的 802.1X 认证定时器包括以下两种：

- 客户端认证超时定时器：当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，设备端将重发该报文。
- 认证服务器超时定时器：当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到认证服务器的响应，设备端将重发认证请求报文。

表1-9 配置 802.1X 定时器参数

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置客户端认证超时定时器	**dot1x timer supp-timeout** *supp-timeout-value*	可选 缺省情况下，客户端认证超时定时器的值为30秒
配置认证服务器超时定时器	**dot1x timer server-timeout** *server-timeout-value*	可选 缺省情况下，认证服务器超时定时器的值为100秒

说明

一般情况下，无需改变认证超时定时器的值，除非在一些特殊或恶劣的网络环境下，才需要通过命令来调节。例如，用户网络状况比较差的情况下，可以适当地将客户端认证超时定时器值调大一些；还可以通过调节认证服务器超时定时器的值来适应不同认证服务器的性能差异。

1.4.9 配置在线用户握手功能

开启设备的在线用户握手功能后，设备会定期（时间间隔通过命令 **dot1x timer handshake-period** 设置）向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次（通过命令 **dot1x retry** 设置）没有收到客户端的响应报文，则会将用户置为下线状态。

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。开启了在线用户握手安全功能的设备通过检验客户端上传的握手报文中携带的验证信息，来确认用户是否使用 iNode 客户端进行握手报文的交互。如果握手检验不通过，则会将用户置为下线状态。

需要注意的是：在线用户握手安全功能的实现依赖于在线用户握手功能。为使在线用户握手安全功能生效，请保证在线用户握手功能处于开启状态。

表1-10 配置在线用户握手功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置握手定时器	**dot1x timer handshake-period** *handshake-period-value*	可选 缺省情况下，握手定时器的值为15秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启在线用户握手功能	**dot1x handshake**	可选 缺省情况下，在线用户握手功能处于开启状态
开启在线用户握手功能的安全功能	**dot1x handshake secure**	可选 缺省情况下，在线用户握手安全功能处于关闭状态

- 关闭在线用户握手功能之前，必须先关闭代理检测与控制功能。
- 部分 802.1X 客户端不支持与设备进行握手报文的交互，因此建议在这种情况下，关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 建议在线用户握手安全功能与 iNode 客户端以及 iMC 服务器配合使用，以保证该功能可以正常运行。

1.4.10 配置代理检测与控制功能

该功能用于实现设备对通过代理登录设备的用户的检测及接入控制，可以防止其他非法用户使用已认证的 802.1X 客户端作为代理服务器访问网络资源或逃避监控、计费。如果检测结果为用户代理上网，则设备可以给网管发送 Trap 信息或者通过发送下线消息强制该用户下线，这两种方式也可以同时使用。

需要注意的是：

- 该功能依赖于在线用户握手功能。在配置代理检测功能之前，必须先开启在线用户握手功能。在线握手功能的配置请参考“1.4.9 配置在线用户握手功能”。
- 必须同时开启全局和指定端口的代理用户检测与控制，该功能才可以在端口上生效。
- 若在不同视图下先后对同一个端口的代理检测与控制功能进行了配置，则最后执行的配置生效。

表1-11 配置代理检测与控制功能

配置步骤	命令	说明
进入系统视图	**system-view**	-

配置步骤		命令	说明
开启全局的代理用户检测与控制		**dot1x supp-proxy-check** { **logoff** | **trap** }	必选 缺省情况下，未开启对代理用户的检测及接入控制
开启端口的代理用户检测与控制	在系统视图下	**dot1x supp-proxy-check** { **logoff** | **trap** } **interface** *interface-list*	二者必选其一 缺省情况下，未开启对代理用户的检测及接入控制
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x supp-proxy-check { **logoff** | **trap** }	

说明

该功能的实现需要 H3C iNode 客户端程序的配合。

1.4.11 开启认证触发功能

端口上开启认证触发功能后，设备会主动向该端口上的客户端发送认证请求来触发认证，以支持不能主动发送 EAPOL-Start 报文来发起认证的客户端。设备提供了以下两种类型的认证触发功能：

- 组播触发功能：启用了该功能的端口会定期（间隔时间通过命令 **dot1x timer tx-period** 设置）向客户端组播发送 EAP-Request/Identity 报文来检测客户端并触发认证。该功能用于支持不能主动发起认证的客户端。
- 单播触发功能：当启用了该功能的端口收到源 MAC 地址未知的报文时，会主动向该 MAC 地址单播发送 EAP-Request/Identity 报文，若端口在指定的时间内（通过命令 **dot1x timer tx-period** 设置）没有收到客户端的响应，则重发该报文（重发次数通过命令 **dot1x retry** 设置）。该功能适用于客户端不支持主动认证，且仅部分客户端需要进行认证的组网环境，可避免不希望认证或已认证的客户端收到多余的认证触发报文。

表1-12 开启认证触发功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置用户名请求超时定时器	**dot1x timer tx-period** *tx-period-value*	可选 缺省情况下，用户名请求超时定时器的值为30秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启认证触发功能	**dot1x** { **multicast-trigger** | **unicast-trigger** }	可选 缺省情况下，组播触发功能处于开启状态，单播触发功能处于关闭状态

说明

建议组播触发功能和单播触发功能不要同时开启，以免认证报文重复发送。

1.4.12 配置端口的强制认证域

配置端口的强制认证域（mandatory domain）为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

表1-13 配置端口的强制认证域

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的强制认证域	**dot1x mandatory-domain** *domain-name*	必选 缺省情况下，未定义强制认证域

1.4.13 配置静默功能

当 802.1X 用户认证失败以后，设备需要静默一段时间（通过命令 **dot1x timer quiet-period** 设置）后再重新发起认证，在静默期间，设备不进行 802.1X 认证的相关处理。

表1-14 开启静默定时器功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置静默定时器	**dot1x timer quiet-period** *quiet-period-value*	可选 缺省情况下，静默定时器的值为60秒
开启静默定时器功能	**dot1x quiet-period**	必选 缺省情况下，静默定时器功能处于关闭状态

说明

在网络处在风险位置，容易受攻击的情况下，可以适当地将静默定时器值调大一些，反之，可以将其调小一些来提高对用户认证请求的响应速度。

1.4.14 配置重认证功能

端口启动了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器设定的时间间隔（由命令 **dot1x timer reauth-period** 设置）定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

表1-15 配置重认证功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置周期性重认证定时器	**dot1x timer reauth-period** *reauth-period-value*	可选 缺省情况下，周期性重认证定时器的值为3600秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启周期性重认证功能	**dot1x re-authenticate**	必选 缺省情况下，周期性重认证功能处于关闭状态

说明

- 认证服务器可以通过下发 RADIUS 属性（session-timeout）来指定用户的重认证周期，且该功能不需要设备上开启周期性重认证功能来配合，属性下发成功即可生效。802.1X 用户认证通过后，如果认证服务器对该用户下发了重认证周期，则设备上配置的周期性重认证时间无效，服务器下发的重认证周期生效。认证服务器下发重认证时间的具体配置以及是否可以下发重认证周期的情况与服务器类型有关，请参考具体的认证服务器实现。
- 在用户名不改变的情况下，端口允许重认证前后服务器向该用户下发不同内容的 VLAN；但是，若重认证前端口下发了 VLAN，而重认证后未下发 VLAN，则重认证失败，用户下线，反之同样处理。
- 当端口向在线的 802.1X 用户发起重认证或者重认证过程中发现没有可达的服务器时，如果该端口上配置了 Critical VLAN，则重认证将会中止，用户保持在线，且不离开当前所在 VLAN；如果端口上没有配置 Critical VLAN，则在线用户将会下线。

1.4.15 配置Guest VLAN

注意

- 如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 Guest VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Guest VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 Guest VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Guest VLAN 的 VLAN。
- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。

表1-16 配置 Guest VLAN

配置步骤		命令	说明
进入系统视图		**system-view**	-
配置指定端口的Guest VLAN	在系统视图下	**dot1x guest-vlan** *guest-vlan-id* [**interface** *interface-list*]	二者必选其一 缺省情况下，端口没有配置Guest VLAN 不同的端口可以配置不同的Guest VLAN，但一个端口最多只能配置一个Guest VLAN
	在以太网接口视图下	**interface** *interface-type interface-number*	
		dot1x guest-vlan *guest-vlan-id*	

1.4.16 配置Auth-Fail VLAN

注意

- 如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 Auth-Fail VLAN，为保证各种功能的正常使用，请为端口的缺省 VLAN 和 802.1X 的 Auth-Fail VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Auth-Fail VLAN；同样，如果某个 VLAN 被指定为某个端口的 Auth-Fail VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 Auth-Fail VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Auth-Fail VLAN 的 VLAN。
- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。

- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Auth-Fail VLAN 修改为携带 Tag 的方式。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。

表1-17 配置 Auth-Fail VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置指定端口的Auth-Fail VLAN	**dot1x auth-fail vlan** *authfail-vlan-id*	必选 缺省情况下，端口没有配置Auth-Fail VLAN 不同的端口可以配置不同的Auth-Fail VLAN，但一个端口最多只能配置一个Auth-Fail VLAN

说明

在接入控制方式为 MAC-based 的端口上生成的 Auth-Fail VLAN 表项会覆盖已生成的阻塞 MAC 表项，但如果端口因检测到非法报文而关闭，则 802.1X 的 Auth-Fail VLAN 功能无法生效。关于端口入侵检测关闭功能的具体介绍请参见“安全配置指导”中的“端口安全”。

1.4.17 配置Critical VLAN

注意

- 如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 Critical VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Critical VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 Critical VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Critical VLAN 的 VLAN。
- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。
- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Critical VLAN 修改为携带 Tag 的方式。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。

当端口加入 Critical VLAN 后，如果发现有认证服务器可达，可通过配置端口的恢复动作为 **reinitialize** 来通知 802.1X 客户端进行认证。根据端口的接入控制方式不同，具体实现有所不同：

- 接入控制方式为 MAC-based 时，当发现有认证服务器可达后，处于 Critical VLAN 的端口会主动向已加入 Critical VLAN 的 MAC 地址发送单播报文触发其进行 802.1X 认证。
- 接入控制方式为 Port-based 时，当发现有认证服务器可达后，处于 Critical VLAN 的端口会主动发送组播报文，触发端口上的客户端进行 802.1X 认证。

表1-2 配置 Critical VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置指定端口的Critical VLAN	**dot1x critical vlan** *vlan-id*	必选 缺省情况下，端口没有配置Critical VLAN 不同的端口可以配置不同的Critical VLAN，但一个端口最多只能配置一个Critical VLAN
配置指定端口的恢复动作	**dot1x critical recovery-action reinitialize**	可选 缺省情况下，设备检测到服务器恢复为可达状态后，端口仅仅离开Critical VLAN，不会对用户主动进行认证

说明

- 若端口已经位于 802.1X 的 Guest VLAN 或 Auth-Fail VLAN，则当所有认证服务器都不可达时，端口并不会离开当前的 VLAN 而加入 Critical VLAN。
- 若端口已经位于 MAC 地址认证的 Guest VLAN，则当所有认证服务器都不可达时，端口会离开当前的 VLAN 并加入 Critical VLAN。

1.4.18 配置 802.1X支持的域名分隔符

设备对用户的管理是基于 ISP 域的，每个接入用户都属于一个 ISP 域。用户所属的 ISP 域是由用户登录时提供的用户名决定的，若用户名中携带域名，则设备使用该域中的 AAA 配置对用户进行认证、授权和计费，否则使用系统中的缺省域；若设备指定了 802.1X 的强制认证域，则无论用户名中是否携带域名，设备均使用指定的强制认证域。因此，设备能够准确解析用户名中的纯用户名和域名对于为用户提供认证服务非常重要。由于不同的 802.1X 客户端所支持的用户名域名分隔符不同，为了更好地管理和控制不同用户名格式的 802.1X 用户接入，需要在设备上指定 802.1X 可支持的域名分隔符。

目前，802.1X 支持的域名分隔符包括@、\和/，对应的用户名格式分别为 *username@domain-name*，*domain-name\username* 和 *username/domain-name*，其中 *username* 为纯用户名、*domain-name*

为域名。如果用户名中包含有多个域名分隔符字符，则设备仅将第一个出现的域名分隔符识别为实际使用的域名分隔符，其它字符都被认为是域名中的一部分，例如，用户输入的用户名为123/22\@abc，则认为纯用户名为 123，域名分隔符为/，域名为 22\@abc。

如果用户输入的用户名中不包含任何 802.1X 可支持的域名分隔符，则设备会认为该用户名并未携带域名，则使用系统中的缺省域对该用户进行认证。

表1-3 指定 802.1X 支持的域名分隔符

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定802.1X支持的域名分隔符	**dot1x domain-delimiter** *string*	可选 缺省情况下，仅支持域名分隔符@

说明

若设备上指定发送给认证服务器的用户名携带域名（**user-name-format with-domain**），则发送给认证服务器的用户名中携带该用户使用的认证域的域名，并采用设备上指定的 802.1X 支持的域名分隔符，若设备上指定了多个域名分隔符，则选择的优先级由高到低依次为@、/、\。另外，为保证用户信息可在认证服务器上被准确匹配到，设备上指定的 802.1X 支持的域名分隔符必须与认证服务器支持的域名分隔符保持一致，否则可能会因为服务器匹配用户失败而导致用户认证失败。相关命令的具体介绍请参考“安全命令参考”中的“AAA”。

1.5 802.1X显示和维护

在完成上述配置后，在任意视图下执行 **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** 命令可以清除 802.1X 的统计信息。

表1-18 802.1X 显示和维护

操作	命令
显示802.1X的会话连接信息、相关统计信息或配置信息	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除802.1X的统计信息	**reset dot1x statistics** [**interface** *interface-list*]

1.6 802.1X典型配置举例

1.6.1 802.1X认证配置举例

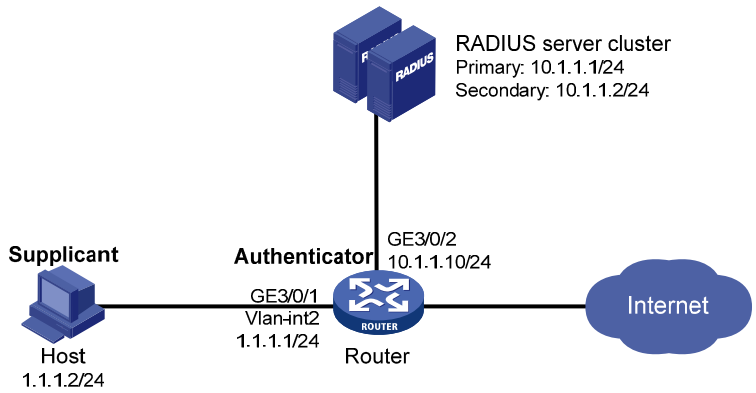
1. 组网需求

用户通过 Router 的端口 GigabitEthernet3/0/1 接入网络，设备对该端口接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- 由两台 RADIUS 服务器组成的服务器组与 Router 相连，其 IP 地址分别为 10.1.1.1/24 和 10.1.1.2/24，使用前者作为主认证/计费服务器，使用后者作为备份认证/计费服务器。
- 端口 GigabitEthernet3/0/1 下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。
- 认证时，首先进行 RADIUS 认证，如果 RADIUS 服务器没有响应则进行本地认证；计费时，如果 RADIUS 计费失败则切断用户连接使其下线。
- 所有接入用户都属于同一个 ISP 域 aabbcc.net，该域中最多可容纳 30 个用户。
- Router 与 RADIUS 认证服务器交互报文时的共享密钥为 name、与 RADIUS 计费服务器交互报文时的共享密钥为 money。

2. 组网图

图1-11 802.1X 认证组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 完成 802.1X 客户端的配置。若使用 H3C iNode 802.1X 客户端，为保证备选的本地认证可成功进行，请确认 802.1X 连接属性中的“上传客户端版本号”选项未被选中。
- 完成 RADIUS 服务器的配置，添加用户帐户，保证用户的认证/授权/计费功能正常运行。

(1) 配置各接口的 IP 地址（略）

(2) 配置本地用户

添加本地用户，用户名为 localuser，密码为明文输入的 localpass。（此处添加的本地用户的用户名和密码需要与服务器端配置的用户名和密码保持一致，本例中的 localuser 仅为示例，请根据实际情况配置）

```
<Router> system-view
[Router] local-user localuser
[Router-luser-localuser] service-type lan-access
[Router-luser-localuser] password simple localpass
```

启动闲置切断功能，并指定正常连接时用户空闲时间超过 20 分钟，则切断其连接。

```
[Router-luser-localuser] authorization-attribute idle-cut 20
[Router-luser-localuser] quit
```

(3) 配置 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[Router] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址。

```
[Router-radius-radius1] primary authentication 10.1.1.1
[Router-radius-radius1] primary accounting 10.1.1.1
```

配置备份认证/计费 RADIUS 服务器的 IP 地址。

```
[Router-radius-radius1] secondary authentication 10.1.1.2
[Router-radius-radius1] secondary accounting 10.1.1.2
```

配置 Router 与认证/计费 RADIUS 服务器交互报文时的共享密钥。

```
[Router-radius-radius1] key authentication name
[Router-radius-radius1] key accounting money
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Router-radius-radius1] user-name-format without-domain
[Router-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名以及服务器端的配置有关：

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Router 上指定不携带用户名（**without-domain**）；
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Router 上指定携带用户名（**with-domain**）。

(4) 配置 ISP 域

创建域 aabbcc.net 并进入其视图。

```
[Router] domain aabbcc.net
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费，并采用 local 作为备选方法。

```
[Router-isp-aabbcc.net] authentication lan-access radius-scheme radius1 local
[Router-isp-aabbcc.net] authorization lan-access radius-scheme radius1 local
[Router-isp-aabbcc.net] accounting lan-access radius-scheme radius1 local
```

配置该域最多可容纳 30 个用户。

```
[Router-isp-aabbcc.net] access-limit enable 30
```

启动闲置切断功能，并指定正常连接时用户空闲时间超过 20 分钟，则切断其连接。

```
[Router-isp-aabbcc.net] idle-cut enable 20
[Router-isp-aabbcc.net] quit
```

指定域 aabbcc.net 为缺省的 ISP 域。如果用户在登录时没有提供 ISP 域名，系统将把它归于该缺省的 ISP 域。

```
[Router] domain default enable aabbcc.net
```

(5) 配置 802.1X

开启全局 802.1X 特性。

```
[Router] dot1x
```

开启指定端口 GigabitEthernet3/0/1 的 802.1X 特性。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] dot1x
[Router-GigabitEthernet3/0/1] quit
```

配置基于 MAC 地址的接入控制方式（该配置可选，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

```
[Router] dot1x port-method macbased interface gigabitethernet 3/0/1
```

4. 验证配置结果

使用命令 **display dot1x interface** gigabitethernet 3/0/1 可以查看 802.1X 的配置情况。当 802.1X 用户输入正确的用户名和密码成功通过 RADIUS 认证上线后，可使用命令 **display connetion** 查看到上线用户的连接情况。若 RADIUS 服务器无响应，则进行本地认证。

1.6.2 802.1X认证配合Guest VLAN、VLAN下发配置举例

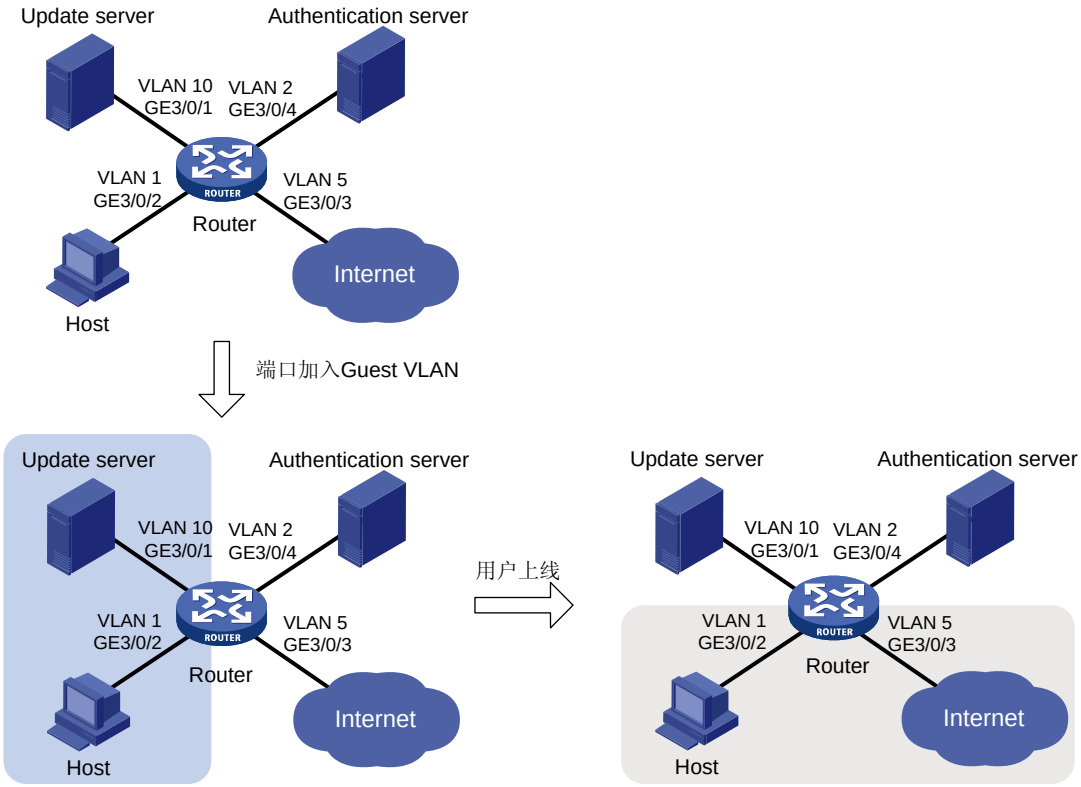
1. 组网需求

如图 1-12所示，一台主机通过 802.1X认证接入网络，认证服务器为RADIUS服务器。Host接入Router的端口GigabitEthernet3/0/2 在VLAN 1 内；认证服务器在VLAN 2 内；Update Server是用于客户端软件下载和升级的服务器，在VLAN 10 内；Router连接Internet网络的端口GigabitEthernet3/0/3 在VLAN 5 内。现有如下组网需求：

- 若一定的时间内端口上无客户端进行认证，则将该端口 GigabitEthernet3/0/2 加入 Guest VLAN（VLAN 10）中，此时 Host 和 Update Server 都在 VLAN 10 内，Host 可以访问 Update Server 并下载 802.1X 客户端。
- 用户认证成功上线后，认证服务器下发 VLAN 5，此时 Host 和连接 Internet 网络的端口 GigabitEthernet3/0/3 都在 VLAN 5 内，Host 可以访问 Internet。

2. 组网图

图1-12 Guest VLAN 及 VLAN 下发组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 保证接入端口加入 Guest VLAN 或授权 VLAN 之后，802.1X 客户端能够及时更新 IP 地址，以实现与相应网络资源的互通。
- 完成 RADIUS 服务器的配置，添加用户帐户，指定要授权下发的 VLAN（本例中为 VLAN 5），并保证用户的认证/授权/计费功能正常运行。

(1) 创建 VLAN 并将端口加入对应 VLAN

```
<Router> system-view
[Router] vlan 1
[Router-vlan1] port gigabitethernet 3/0/2
[Router-vlan1] quit
[Router] vlan 10
[Router-vlan10] port gigabitethernet 3/0/1
[Router-vlan10] quit
[Router] vlan 2
[Router-vlan2] port gigabitethernet 3/0/4
```

```
[Router-vlan2] quit
[Router] vlan 5
[Router-vlan5] port gigabitethernet 3/0/3
[Router-vlan5] quit
```

(2) 配置 RADIUS 方案

创建 RADIUS 方案 2000 并进入其视图。

```
[Router] radius scheme 2000
```

配置主认证/计费 RADIUS 服务器及其共享密钥。

```
[Router-radius-2000] primary authentication 10.11.1.1 1812
[Router-radius-2000] primary accouting 10.11.1.1 1813
[Router-radius-2000] key authentication abc
[Router-radius-2000] key accouting abc
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Router-radius-2000] user-name-format without-domain
[Router-radius-2000] quit
```

(3) 配置 ISP 域

创建域 bbb 并进入其视图。

```
[Router] domaim bbb
```

配置 802.1X 用户使用 RADIUS 方案 2000 进行认证、授权、计费。

```
[Router-isp-bbb] authentication lan-access radius-scheme 2000
[Router-isp-bbb] authorization  lan-access radius-scheme 2000
[Router-isp-bbb] accounting lan-access radius-scheme 2000
[Router-isp-bbb] quit
```

(4) 配置 802.1X

开启全局 802.1X 特性。

```
[Router] dot1x
```

开启指定端口的 802.1X 特性。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] dot1x
```

配置端口上进行接入控制的方式为 **portbased**。

```
[Router-GigabitEthernet3/0/2] dot1x port-method portbased
```

配置端口的授权状态为 **auto**。（此配置可选，端口的授权状态缺省为 **auto**）

```
[Router-GigabitEthernet3/0/2] dot1x port-control auto
[Router-GigabitEthernet3/0/2] quit
```

配置指定端口的 Guest VLAN。

```
[Router] dot1x guest-vlan 10 interface gigabitethernet 3/0/2
```

4. 验证配置结果

通过命令 **display dot1x interface** gigabitethernet 3/0/2 可以查看端口 GigabitEthernet3/0/2 上 Guest VLAN 的配置情况。若在指定的时间之内无客户端进行认证或者无客户端认证成功，则通过命令 **display vlan** 10 可以查看到端口 GigabitEthernet3/0/2 加入了配置的 Guest VLAN。

在用户认证成功之后，通过 **display interface** gigabitethernet 3/0/2 可以看到用户接入的端口 GigabitEthernet3/0/2 加入了认证服务器下发的 VLAN 5 中。

1.6.3 802.1X认证配合下发ACL配置举例

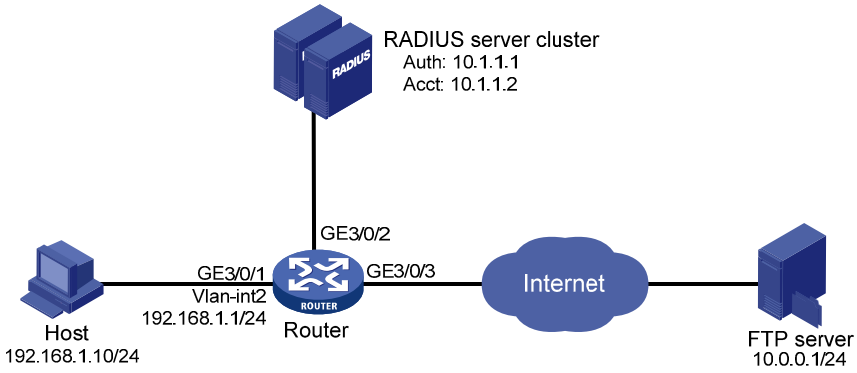
1. 组网需求

用户通过 Router 的端口 GigabitEthernet3/0/1 接入网络，Router 对该端口接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- 使用 RADIUS 服务器 10.1.1.1/24 作为认证/授权服务器，RADIUS 服务器 10.1.1.2/24 作为计费服务器；
- 通过认证服务器下发 ACL，禁止上线的 802.1X 用户在工作日的工作时间（8:00～18:00）访问 IP 地址为 10.0.0.1/24 的 FTP 服务器。

2. 组网图

图1-13 下发 ACL 典型组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 完成 802.1X 客户端的配置，并保证接入端口加入 Guest VLAN 或授权 VLAN 之后客户端能够及时更新 IP 地址，以实现与相应网络资源的互通。
- 完成 RADIUS 服务器的配置，添加用户帐户，指定要授权下发的 ACL（本例中为 ACL 3000），并保证用户的认证/授权/计费功能正常运行。

配置各接口的 IP 地址（略）。

配置 RADIUS 方案。

```
<Router> system-view
[Router] radius scheme 2000
[Router-radius-2000] primary authentication 10.1.1.1 1812
[Router-radius-2000] primary accounting 10.1.1.2 1813
[Router-radius-2000] key authentication abc
[Router-radius-2000] key accounting abc
[Router-radius-2000] user-name-format without-domain
[Router-radius-2000] quit
```

配置 ISP 域的 AAA 方法。

```
[Router] domaim 2000
[Router-isp-2000] authentication default radius-scheme 2000
[Router-isp-2000] authorization  default radius-scheme 2000
[Router-isp-2000] accounting default radius-scheme 2000
[Router-isp-2000] quit
```

配置名为 ftp 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

配置 ACL 3000，拒绝用户在工作日的工作时间内访问 FTP 服务器 10.0.0.1 的报文通过。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Router-acl-adv-3000] quit
```

开启全局 802.1X 特性。

```
[Router] dot1x
```

开启指定端口的 802.1X 特性。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] dot1x
```

4. 验证配置结果

当用户认证成功上线后，在工作日的工作时间 Ping FTP 服务器。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

由以上过程可知，用户无法 **ping** 通 FTP 服务器，说明认证服务器下发的 ACL 已对该用户生效。

2 802.1X支持EAD快速部署配置

说明

本特性仅在 SAP 板工作在二层模式时支持。

2.1 802.1X支持EAD快速部署简介

2.1.1 概述

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个特定的 IP 地址段，并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.1.2 实现机制

802.1X 支持的 EAD 快速部署是通过以下两个功能配合实现的。

1. 未认证用户可访问免认证网段（Free IP）

802.1X 终端用户在认证成功之前，可以访问一个免认证的 IP 地址段，也称为 Free IP。该 IP 地址段中可以配置一个或多个特定服务器，用于提供 EAD 客户端的下载升级或者动态地址分配等服务。

2. 用户HTTP访问URL的重定向

802.1X 终端用户在认证成功之前，如果使用浏览器访问网络，设备会将用户访问的 URL 重定向到已配置的 URL（例如，重定向到 EAD 客户端下载界面），这样只要用户打开浏览器，就必须进入管理员预设的界面。提供重定向 URL 的服务器必须位于用户受限访问的特定网段内。

2.2 配置EAD快速部署

说明

目前，MAC 地址认证和端口安全特性不支持 EAD 的快速部署功能，全局使能 MAC 认证或端口安全功能将会使 EAD 快速部署功能失效。

2.2.1 配置准备

- 开启全局 802.1X 特性
- 开启指定端口的 802.1X 特性，并指定端口的授权模式为 **auto**

2.2.2 配置Free IP

配置 Free IP 网段之后，EAD 的快速部署功能将立即处于使能状态。未通过认证的 802.1X 终端用户可以访问该 IP 地址段中的网络资源。

表2-1 配置用户可访问的免认证网段

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置Free IP	**dot1x free-ip** *ip-address* { *mask-address* **|** *mask-length* }	必选 缺省情况下，未定义Free IP

说明

- MAC 地址认证、端口安全功能与 Free IP 配置互斥。
- 在同时配置了 Free IP 与 Guest VLAN 功能、Auth-Fail VLAN 功能的情况下，请保证 Free IP 为 Guest VLAN 和 Auth-Fail VLAN 可允许访问的网络资源。这种情况下，用户只能访问 Free IP，不能访问其它资源。
- 未通过 802.1X 认证的用户若要通过外网的 DHCP 服务器动态获得 IP 地址，则需要保证该 DHCP 服务器的 IP 地址在配置的 Free IP 内。

2.2.3 配置用户HTTP访问的重定向URL

终端用户在 802.1X 认证成功之前（包括认证失败）发起的 HTTP 访问请求都会被设备重定向到本命令配置的 URL。

表2-2 配置用户 HTTP 访问的重定向 URL

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置用户HTTP访问的重定向URL	**dot1x url** *url-string*	必选 缺省情况下，未定义重定向URL

说明

重定向的 URL 必须处于 Free IP 网段内，否则无法实现重定向。

2.2.4 配置EAD规则的老化时间

EAD 快速部署功能通过制订 EAD 规则（通常为 ACL 规则）来给予未通过认证的终端用户受限制的网络访问权限，在用户认证成功后，所占用的 ACL 将被释放。由于设备支持的 ACL 数量有限，当大量用户同时上线时，ACL 资源将迅速被占用，如果没有用户认证成功，将出现 ACL 数量不足的情况，这样会导致一部分新接入的用户无法上线。

管理员可以通过配置 EAD 规则的老化时间来控制用户对 ACL 资源的占用，当用户访问网络时该定时器即开始计时，在定时器超时或者用户下载客户端并成功通过认证之后，该用户所占用的 ACL 资源即被删除，这样那些在老化时间内未进行任何操作的用户所占用的 ACL 资源会及时得到释放。在接入用户数量较多时，可以将超时时间适当缩短，以提高 ACL 的使用效率。

表2-3 配置 EAD 规则老化时间

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置EAD规则老化时间	**dot1x timer ead-timeout** *ead-timeout-value*	可选 缺省情况下，EAD规则老化时间为30分钟

2.3 EAD快速部署显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 EAD 快速部署的运行情况，通过查看显示信息验证配置的效果。

表2-4 EAD 快速部署显示和维护

操作	命令
显示802.1X的会话连接信息、相关统计信息或配置信息	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]

2.4 EAD快速部署典型配置举例

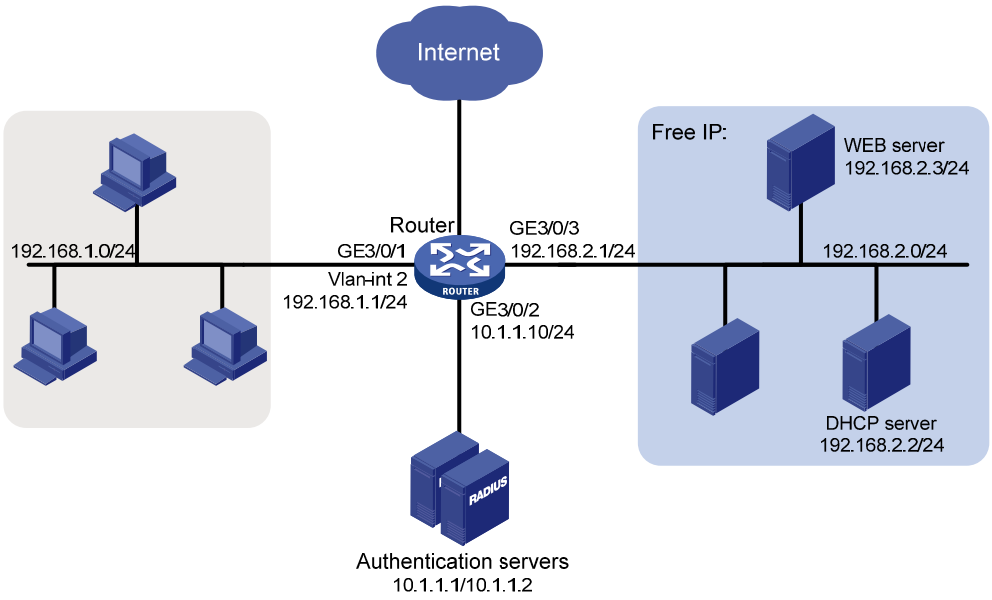
1. 组网需求

某公司用户主机通过 Router 接入 Internet，并通过 DHCP 服务器动态获取 IP 地址。目前，公司部署 EAD 解决方案，要求所有用户主机通过 802.1X 认证上网，因此需要所有主机上安装配套的 802.1X 客户端。由于网络中的用户主机数量较大，为减轻网络管理员安装以及升级 802.1X 客户端的工作量，在 192.168.2.0/24 网段部署一台 Web 服务器专门提供客户端软件下载。具体要求如下：

- 未进行 802.1X 认证或者 802.1X 认证失败的用户，只能访问 192.168.2.0/24 网段，并可通过该网段内的 DHCP 服务器动态获取 192.168.1.0/24 网段的 IP 地址。
- 未进行 802.1X 认证或者 802.1X 认证失败的用户通过浏览器访问非 192.168.2.0/24 网段的外部网络时，用户访问的页面均会被 Router 重定向至管理员预设的 Web 服务器页面，该 Web 服务器页面将提示用户进行 802.1X 客户端的下载。
- 用户成功通过 802.1X 认证之后，可正常访问网络。

2. 组网图

图2-1 EAD 快速部署典型配置组网图



3. 配置步骤

说明

- 完成 DHCP 服务器的配置，保证用户可成功获取 192.168.1.0/24 网段的 IP 地址。
- 完成 Web 服务器的配置，保证用户可成功登录预置的 Web 页面进行 802.1X 客户端的下载。
- 完成认证服务器的配置，保证用户的认证/授权/计费功能正常运行。

(1) 配置各接口的 IP 地址（略）

(2) 配置 DHCP 中继

使能 DHCP 服务。

```
<Router> system-view
[Router] dhcp enable
```

配置 DHCP 服务器的地址。

```
[Router] dhcp relay server-group 1 ip 192.168.2.2
```

配置接口接口 Vlan-interface2 工作在 DHCP 中继模式。

```
[Router] interface vlan-interface 2
[Router-Vlan-interface2] dhcp select relay
```

配置接口接口 Vlan-interface2 对应 DHCP 服务器组 1。

```
[Router-Vlan-interface2] dhcp relay server-select 1
[Router-Vlan-interface2] quit
```

(3) 配置 RADIUS 方案和 ISP 域

请参见“1.6.1 802.1X认证配置举例”。

(4) 配置 802.1X

配置 Free IP。

```
[Router] dot1x free-ip 192.168.2.0 24
```

配置 IE 访问的重定向 URL。

```
[Router] dot1x url http://192.168.2.3
```

开启全局 802.1X 特性。

```
[Router] dot1x
```

开启指定端口的 802.1X 特性。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] dot1x
```

4. 验证配置结果

以上配置完成之后，执行命令 **display dot1x** 可以查看 802.1X 的配置情况。用户主机成功获得 DHCP 服务器分配的 IP 地址之后，在 Windows XP 操作系统的主机上执行 **ping** Free IP 中的地址，可验证在 802.1X 认证成功之前是否可以访问免认证网段 192.168.2.0/24。

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

用户在 802.1X 认证成功之前，通过浏览器访问任何非 Free IP 的外部网站地址时，都会被重定向到 Web server 页面，此页面提供 802.1X 客户端的下载服务。需要注意的是，地址栏内输入的地址应该为非 Free IP 地址才有效，例如 3.3.3.3 或者 http://3.3.3.3。

2.5 常见配置错误举例

2.5.1 用户通过浏览器访问外部网络不能正确重定向

1. 故障现象

用户在浏览器中输入地址，但该 HTTP 访问不能被正确重定向到指定的 URL 服务器。

2. 故障分析

- 用户在浏览器地址栏内输入了字符串类型的地址。由于用户主机使用的操作系统首先会将这个字符串地址作为名字进行网络地址解析，如果解析不成功通常会以非 X.X.X.X 形式的网络地址发送 ARP 请求，这样的请求不能进行重定向；
- 用户在 IE 地址栏内输入了 Free IP 内的任意地址。设备会认为用户试图访问 Free IP 内的某台主机，而不对其进行重定向，即使这台主机不存在；

- 用户在配置和组网时没有将服务器加入 Free IP，或者配置的 URL 为不存在的地址，或者该 URL 指向的服务器没有提供 Web 服务。

3. 处理过程

- 地址栏内输入的地址应该为 X.X.X.X（点分十进制格式）的非 Free IP 地址才有效。
- 确保设备及服务器上的配置正确且有效。