目 录

802.1X

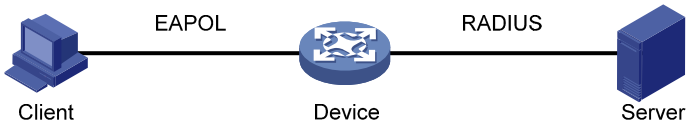
IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议（port based network access control protocol）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1X 的体系结构

802.1X系统为典型的Client/Server结构，如 图 1所示，包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Server）。

图 1 802.1X 认证系统的体系结构



- 客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起 802.1X 认证。客户端必须支持 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。
- 设备端是位于局域网段一端的另一个实体，对所连接的客户端进行认证。设备端通常为支持 802.1X 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器是为设备端提供认证服务的实体。认证服务器用于实现对用户进行认证、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。

802.1X 的认证方式

802.1X 认证系统使用 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换。

- 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。
- 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设备端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocal，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

802.1X 的基本概念

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，这个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。

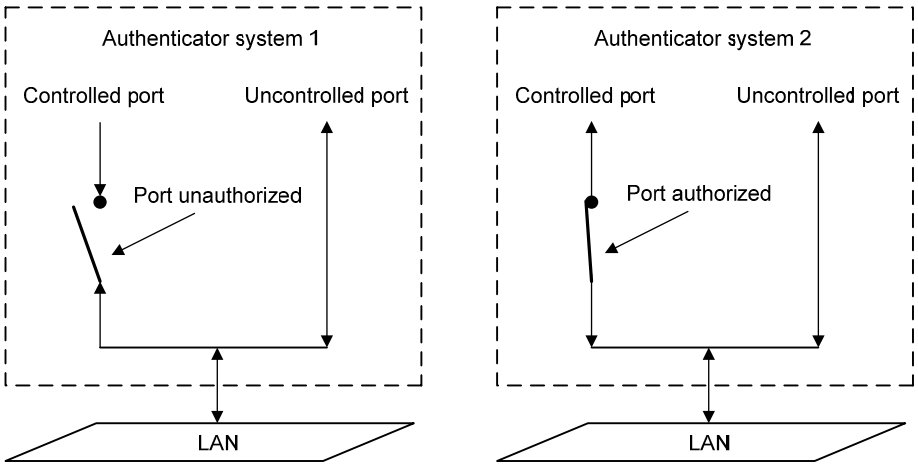
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

2. 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执行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权/非授权状态进行相应地控制。

图 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（相当于端口开关打开），系统 2 的受控端口处于授权状态（相当于端口开关关闭）。

图 2 受控端口上授权状态的影响



用户可以通过在端口下配置的接入控制的模式来控制端口的授权状态。端口支持以下三种接入控制模式：

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

3. 受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。

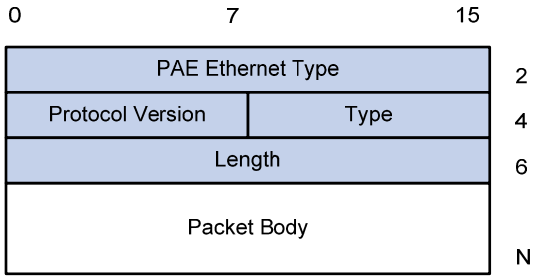
- 实行双向受控时，禁止帧的发送和接收；
- 实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

EAPOL 消息的封装

1. EAPOL 数据包的格式

EAPOL是 802.1X协议定义的一种报文封装格式，主要用于在客户端和设备端之间传送EAP协议报文，以允许EAP协议报文在LAN上传送。EAPOL数据包的格式如 图 3所示。

图 3 EAPOL 数据包格式



PAE Ethernet Type：表示协议类型，为 0x888E。

Protocol Version：表示 EAPOL 帧的发送方所支持的协议版本号。

Type：表示EAPOL数据帧类型，目前设备上支持的数据类型见 表 1。

表 1 EAPOL 数据类型

类型	说明
EAP-Packet（值为 0x00）：认证信息帧，用于承载认证信息	该帧在设备端重新封装并承载于 RADIUS 协议上，便于穿越复杂的网络到达认证服务器
EAPOL-Start（值为 0x01）：认证发起帧	这两种类型的帧仅在客户端和设备端之间存在
EAPOL-Logoff（值为 0x02）：退出请求帧	

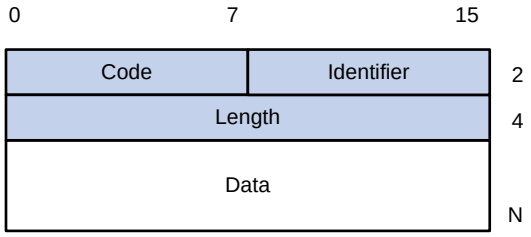
Length：表示数据长度，也就是“Packet Body”字段的长度，单位为字节。如果为 0，则表示没有后面的数据域。

Packet Body：表示数据内容，根据不同的 Type 有不同的格式。

2. EAP 数据包的格式

当EAPOL数据包格式Type域为EAP-Packet时，Packet Body为EAP数据包结构，如 图 4所示。

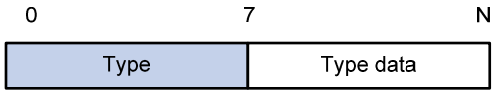
图 4 EAP 数据包格式



Code：指明 EAP 包的类型，共有 4 种：Request、Response、Success、Failure。

- Success 和 Failure 类型的包没有 Data 域，相应的 Length 域的值为 4。
- Request和Response类型数据包的Data域的格式如 图 5所示。Type为EAP的认证类型，Type data的内容由类型决定。例如，Type值为 1 时代表Identity，用来查询对方的身份；Type值为 4 时，代表MD5-Challenge，类似于PPP CHAP协议，包含质询消息。

图 5 Request 和 Response 类型数据包的 Data 域的格式



Identifier：用于匹配 Request 消息和 Response 消息。

Length：EAP 包的长度，包含 Code、Identifier、Length 和 Data 域，单位为字节。

Data：EAP 包的内容，由 Code 类型决定。

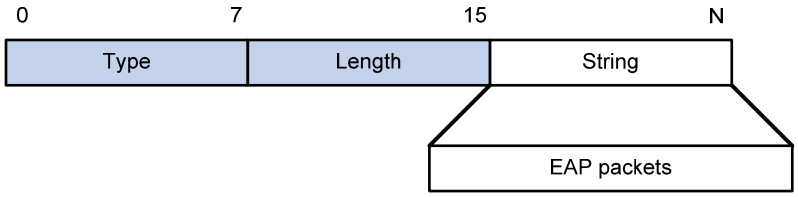
EAP 属性的封装

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）。

1. EAP-Message

如 图 6所示，这个属性用来封装EAP数据包，类型代码为 79，String域最长 253 字节，如果EAP数据包长度大于 253 字节，可以对其进行分片，依次封装在多个EAP-Message属性中。

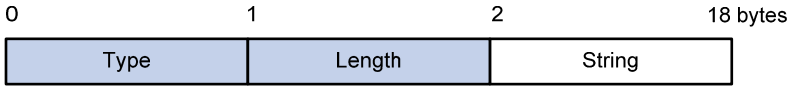
图 6 EAP-Message 属性封装



2. Message-Authenticator

如 图 7所示，这个属性用于在使用EAP、CHAP等认证方法的过程中，避免接入请求包被窃听。在含有EAP-Message属性的数据包中，必须同时也包含Message-Authenticator，否则该数据包会被认为无效而被丢弃。

图 7 Message-Authenticator 属性



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。设备支持的认证触发方式包括以下两种：

1. 客户端主动触发方式

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 IEEE 802.1X 协议分配的一个组播 MAC 地址：01-80-C2-00-00-03。

另外，由于网络中有些设备不支持上述的组播报文，使得认证设备无法收到客户端的认证请求，因此设备端还支持广播触发方式，即，可以接收客户端发送的目的地址为广播 MAC 地址的 EAPOL-Start 报文。这种触发方式需要 H3C iNode 的 802.1X 客户端的配合。

2. 设备端主动触发方式

设备会每隔 N 秒（例如 30 秒）主动向客户端发送 EAP-Request/Identity 报文来触发认证，这种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。

802.1X 的认证过程

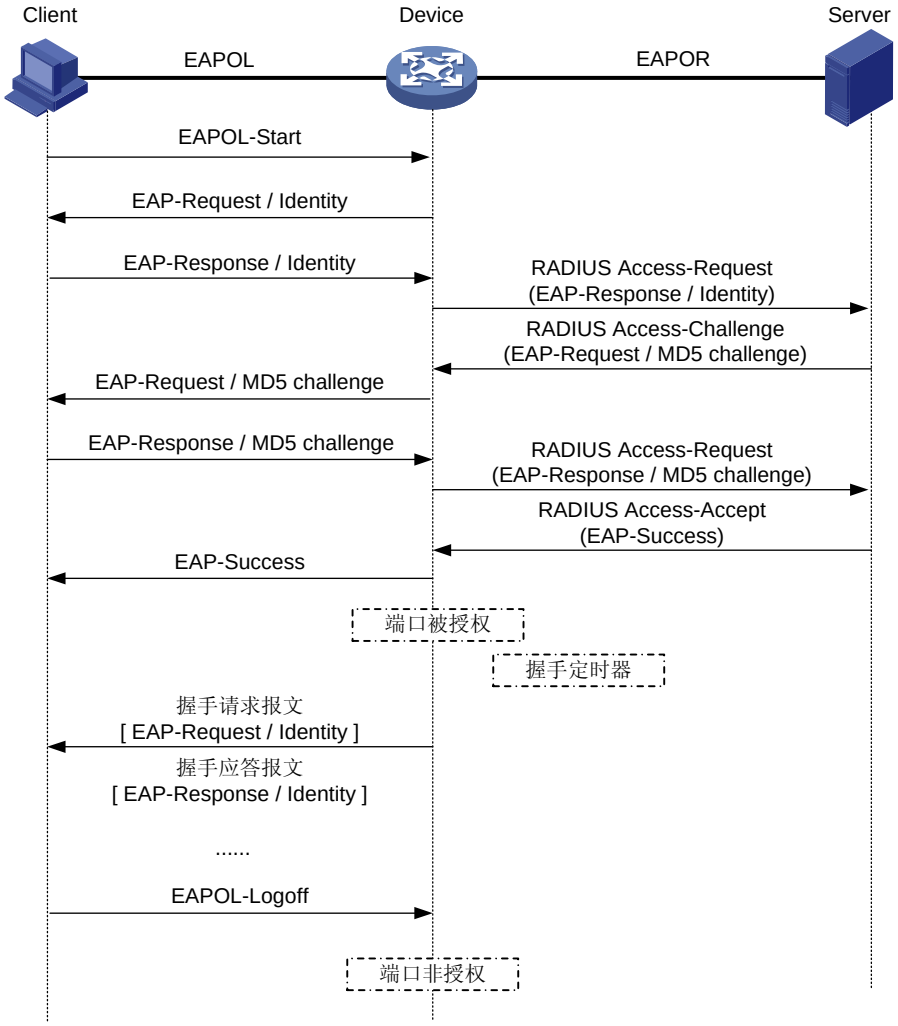
802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP（可扩展认证协议）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，EAP 中继方式需要 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EAP-MD5 方式为例介绍基本业务流程，如 图 8所示。

图 8 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



认证过程如下：

(1) 当用户有访问网络需求时打开 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（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

(2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）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，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

(4) 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表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。

(5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的），生成 EAP-Response/MD5 Challenge 报文，并通过设备端传给认证服务器。

(6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）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，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

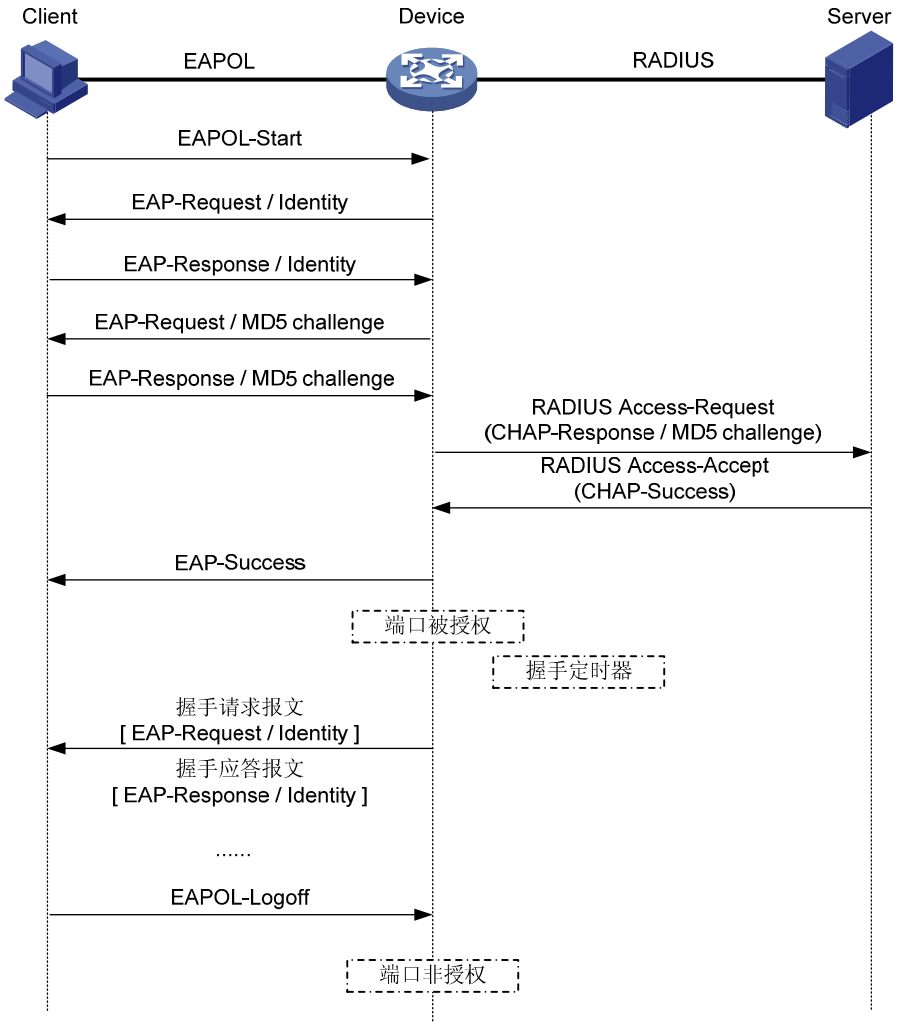
(7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

(8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线。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。

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。以下以CHAP认证方法为例介绍基本业务流程，如 图 9所示。

图 9 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，不同之处在于用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息一起送给 RADIUS 服务器，进行相关的认证处理。

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，还对其进行了扩展、优化，支持基于 MAC 的接入控制方式。

- 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。

802.1X 的定时器

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。802.1X 的定时器主要有以下几种：

- 用户名请求超时定时器（**tx-period**）：该定时器定义了两个时间间隔。其一，当设备端向客户端发送 EAP-Request/Identity 请求报文后，设备端启动该定时器，若在 **tx-period** 设置的时间间隔内，设备端没有收到客户端的响应，则设备端将重发认证请求报文；其二，为了兼容不主动发送 EAPOL-Start 连接请求报文的客户端，设备会定期组播 EAP-Request/Identity 请求报文来检测客户端。**tx-period** 定义了该组播报文的发送时间间隔。
- 客户端认证超时定时器（**supp-timeout**）：当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动此定时器，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（**server-timeout**）：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 **server-timeout** 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。
- 握手定时器（**handshake-period**）：此定时器是在用户认证成功后启动的，设备端以此间隔为周期发送握手请求报文，以定期检测用户的在线情况。如果配置发送次数为 N，则当设备端连续 N 次没有收到客户端的响应报文，就认为用户已经下线。
- 静默定时器（**quiet-period**）：对用户认证失败以后，设备端需要静默一段时间（该时间由静默定时器设置），在静默期间，设备端不处理该用户的认证请求。
- 周期性重认证定时器（**reauth-period**）：如果端口下开启了周期性重认证功能，设备端以此定时器设置的时间间隔为周期对该端口在线用户发起重认证。

和 802.1X 配合使用的特性

1. 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。如果服务器上配置了下发 VLAN 功能，则授权信息中含有授权下发的 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。

- 端口的链路类型为 Access，当前 Access 端口离开用户配置的 VLAN 并加入授权下发的 VLAN 中。
- 端口的链路类型为 Trunk，设备允许授权下发的 VLAN 通过当前 Trunk 端口，并且端口的缺省 VLAN ID 为下发 VLAN 的 VLAN ID。
- 端口的链路类型为 Hybrid，设备允许授权下发的 VLAN 以不携带 Tag 的方式通过当前 Hybrid 端口，并且端口的缺省 VLAN ID 为下发 VLAN 的 VLAN ID。需要注意的是，若当前 Hybrid 端口上配置了基于 MAC 的 VLAN，则设备将根据认证服务器下发的授权 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。

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

2. Guest VLAN

Guest VLAN 功能允许用户在未认证的情况下，可以访问某一特定 VLAN 中的资源，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为 Guest VLAN。

根据端口的接入控制方式不同，可以将 Guest VLAN 划分基于端口的 Guest VLAN 和基于 MAC 的 Guest VLAN。

(1) PGV（Port-based Guest VLAN）

在接入控制方式为 portbased 的端口上配置的 Guest VLAN 称为 PGV。若在一定的时间内（默认 90 秒），配置了 PGV 的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。端口加入 Guest VLAN 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

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“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。

(2) MGV（MAC-based Guest VLAN）

在接入控制方式为 macbased 的端口上配置的 Guest VLAN 称为 MGV。配置了 MGV 的端口上未认证的用户被授权访问 Guest VLAN 里的资源。

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，则认证失败的用户将被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该用户将仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，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 Guest VLAN 之前端口所在的初始 VLAN。

3. Auth-Fail VLAN

Auth-Fail VLAN 功能允许用户在认证失败的情况下可以访问某一特定 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。

与 Guest VLAN 类似，根据端口的接入控制方式不同，可以将 Auth-Fail VLAN 划分为基于端口的 Auth-Fail VLAN 和基于 MAC 的 Auth-Fail VLAN。

(1) PAFV（Port-based Auth-Fail VLAN）

在接入控制方式为 portbased 的端口上配置的 Auth-Fail VLAN 称为 PAFV。在配置了 PAFV 的端口上，若有用户认证失败，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。

当端口上处于 Auth-Fail VLAN 中的用户再次发起认证时：如果认证失败，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 为端口加入任何授权 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) MAFV（MAC-based Auth-Fail VLAN）

在接入控制方式为 macbased 的端口上配置的 Auth-Fail VLAN 称为 MAFV。在配置了 MAFV 的端口上，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。

4. ACL 下发

ACL（Access Control List，访问控制列表）提供了控制用户访问网络资源和限制用户访问权限的功能。当用户上线时，如果 RADIUS 服务器上配置了授权 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控制；在服务器上配置授权 ACL 之前，需要在设备上配置相应的规则。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。

5. 指定端口的强制认证域

指定端口的强制认证域（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 用户将被强制使用该认证域来进行认证、授权和计费，可以防止用户通过恶意假冒其它域账号来接入网络。

另外，对于采用证书的 EAP 中继方式的 802.1X 认证来说，接入用户的客户端证书决定了用户的域名。因此，即使所有端口上客户端的用户证书隶属于同一证书颁发机构，即输入的用户域名相同，管理员也可以通过配置强制认证域对不同端口指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

802.1X 支持 EAD 快速部署配置

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 快速部署就可以解决以上问题，可为所有接入网络的终端用户提供自动下载并安装 EAD 客户端的方便途径。

2. 实现机制

802.1X 支持的 EAD 快速部署是通过以下两个功能的配合工作实现的：

(1) 用户受限访问

802.1X 认证成功之前（包括认证失败），终端用户只能访问一个特定的 IP 地址段。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 重定向

终端用户在 802.1X 认证成功之前（包括认证失败），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。