802.1X 认证基础

文档版本	01
发布日期	2019-05-20

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 802.1X 认证简介

定义

802.1X协议是一种基于端口的网络接入控制协议（Port based networkaccess 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验证用户身份并控制其访问权限。

优点

- 802.1X协议为二层协议，不需要到达三层，对接入设备的整体性能要求不高，可以有效降低建网成本。
- 认证报文和数据报文通过逻辑接口分离，提高安全性。

802.1X 认证系统

如图1-1所示，802.1X系统为典型的Client/Server结构，包括三个实体：客户端、接入设备和认证服务器。

图 1-1 802.1X 认证系统

- 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。客户端必须支持局域网上的可扩展认证协议EAPoL（Extensible Authentication Protocol over LANs）。
- 接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，充当客户端和认证服务器之间的中介，从客户端请求身份信息，并与认证服务器验证该信息。根据客户端的身份验证状态控制其对网络的访问权限。
- 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服务器。

2 802.1X 认证协议

简介

802.1X认证系统使用可扩展认证协议EAP（Extensible Authentication Protocol）来实现客户端、设备端和认证服务器之间的信息交互。EAP协议可以运行在各种底层，包括数据链路层和上层协议（如UDP、TCP等），而不需要IP地址。因此使用EAP协议的802.1X认证具有良好的灵活性。

- 在客户端与设备端之间，EAP协议报文使用EAPoL（EAP over LANs）封装格式，直接承载于LAN环境中。
- 在设备端与认证服务器之间，用户可以根据客户端支持情况和网络安全要求来决定采用的认证方式。
  - EAP终结方式中，EAP报文在设备端终结并重新封装到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。
  - EAP中继方式中，EAP报文被直接封装到RADIUS报文中（EAP over RADIUS，简称为EAPoR），以便穿越复杂的网络到达认证服务器。

EAP 报文

图 2-1 EAP 报文

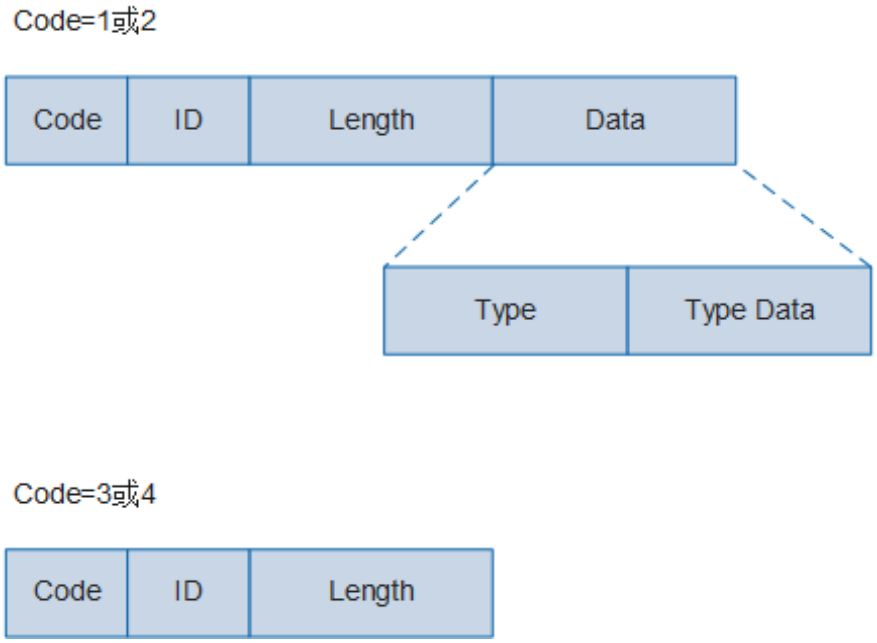


表 2-1 EAP 报文字段解释

字段	字节数	含义
Code	1	表示EAP数据包的类型，共有以下几种 ● 1（Request）：请求。 ● 2（Response）：响应。 ● 3（Success）：成功。 ● 4（Failure）：失败。
ID	1	用于匹配Request和Response。
Length	2	表示EAP数据包的长度，包括Code、ID、Length以及Data各字段。超出Length域范围的字节应该视为数据链路层填充，在接收时应该被忽略掉。
Data	0或多个字节	Data字段的格式由Code的值来决定。 ● 当Code取值为1或者2时，EAP为Request和Response报文，Data包含Type、Type Data两个字段，如上图所示。其中，Type为一个字节，表示Request或Response的类型。Type Data为多个字节，内容由Type字段的值决定。 ● 当Code取值为3或者4时，EAP为Success和Failure报文，没有Data字段。

表 2-2 Type 常用取值

Type字段值	类型	含义
1	Identity	要求客户端发送用户输入的用户名信息。
2	Notification	非必须的通知消息，传送一些警告消息，例如密码已过期、账号被锁等。
3	NAK	仅用于Response帧，表示否定确认。例如设备用了客户端不支持的认证方法发起请求，客户端可利用Response/NAK消息以告知设备其支持的认证方法。
4	MD5-Challenge	认证方法为MD5质询法。
5	OTP（One-Time Password）	认证方法为一次性密码，例如网银付费时系统会通过短信发送一个一次性密码。
6	GTC（Generic Token Card）	认证方法为通用令牌卡。跟OTP类似，只不过GTC往往对应一个实际的设备，例如许多国内银行都会给申请网银的用户一个动态口令牌，这个令牌就是GTC。
13	EAP-TLS	认证方法为EAP-TLS。
21	EAP-TTLS	认证方法为EAP-TTLS。
25	EAP-PEAP	认证方法为EAP-PEAP。
254	Expanded Types	扩展类型，支持厂商自定义的类型。
255	Experimental use	实验新的类型时做测试用的类型。

EAPoL

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之间传送EAP协议报文，以允许EAP协议报文在LAN上传送。其报文结构如下：

图 2-2 EAPoL 报文

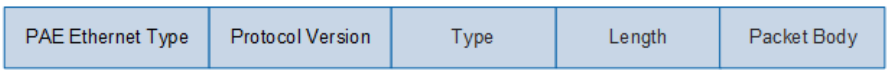


表 2-3 EAPoL 报文字段解释

字段	字节数	含义
PAE Ethernet Type	2	表示协议类型，值为0x888E。

字段	字节数	含义
Protocol Version	1	表示EAPoL帧的发送方所支持的协议版本号。 ● 0x01：802.1X-2001。 ● 0x02：802.1X-2004。 ● 0x03：802.1X-2010。
Type	1	表示EAPoL数据帧类型，有四种取值： ● 00：EAP-Packet，认证报文数据，用于承载认证信息。 ● 01：EAPoL-Start，认证开始报文，用于用户主动发起认证过程。 ● 02：EAPoL-Logoff，下线请求报文，用于用户主动发起下线请求。 ● 03：EAPoL-Key，密钥信息报文。 EAPoL-Start，EAPoL-Logoff和EAPoL-Key仅在客户端和设备端之间存在。
Length	2	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Packet Body字段。EAPoL-Start和EAPoL-Logoff报文的Length值都为0。
Packet Body	2	表示数据内容。

EAPoR

为支持EAP中继方式，RADIUS协议增加了两个属性：EAP-Message（EAP消息）和Message-Authenticator（消息认证码）。其中，EAP-Message属性用来封装EAP报文，Message-Authenticator属性用于对认证报文进行认证和校验，防止非法报文欺骗。其报文结构如下：

图 2-3 EAPoR 报文

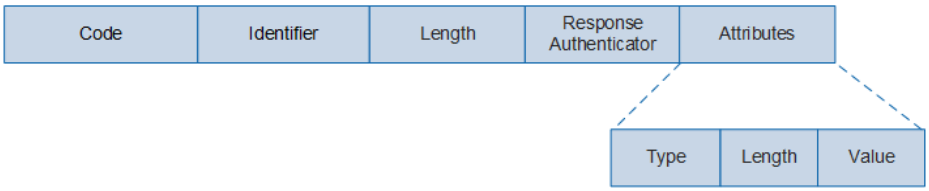


表 2-4 EAPoR 报文字段解释

字段	字节数	含义
Code	1	表示RADIUS报文的类型。

字段	字节数	含义
Identifier	1	用来匹配请求报文和响应报文，以及检测在一段时间内重发的请求报文。客户端发送请求报文后，服务器返回的响应报文中的Identifier值应与请求报文中的Identifier值相同。
Length	2	指定RADIUS报文的长度。超过Length取值的字节将作为填充字符而忽略。如果接收到的报文的实际长度小于Length的取值，则该报文会被丢弃。
Response Authenticator	16	验证RADIUS服务器的响应报文，同时还用于用户密码的加密。
Attributes	长度不确定	Attribute为报文的内容主体，用来携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。Attribute可以包括多个属性，每一个属性都采用（Type、Length、Value）三元组的结构来表示。 ● 类型（Type），1个字节，取值为1～255，用于表示属性的类型。 ● 长度（Length），表示该属性（包括类型、长度和属性值）的长度，单位为字节。 ● 属性值（Value），表示该属性的信息，其格式和内容由类型和长度决定，最大长度为253字节。

认证方式选择

- EAP中继方式的优点是设备端处理更简单，支持更多的认证方法，缺点则是认证服务器必须支持EAP，且处理能力要足够强。对于常用的EAP-TLS、EAP-TTLS、EAP-PEAP三种认证方式，EAP-TLS需要在客户端和服务器上加载证书，安全性最高，EAP-TTLS、EAP-PEAP需要在服务器上加载证书，但不需要在客户端加载证书，部署相对灵活，安全性较EAP-TLS低。
- EAP终结方式的优点是现有的RADIUS服务器基本均支持PAP和CHAP认证，无需升级服务器，但设备端的工作比较繁重，因为在这种认证方式中，设备端不仅要从来自客户端的EAP报文中提取客户端认证信息，还要通过标准的RAIUDS协议对这些信息进行封装，且不能支持除MD5-Challenge之外的其它EAP认证方法。PAP与CHAP的主要区别是CHAP密码通过密文方式传输，而PAP密码通过明文的方式传输。因而PAP方式认证的安全性较低，实际应用通常采用CHAP方式认证。

3 802.1X 认证流程

802.1X 认证的触发方式

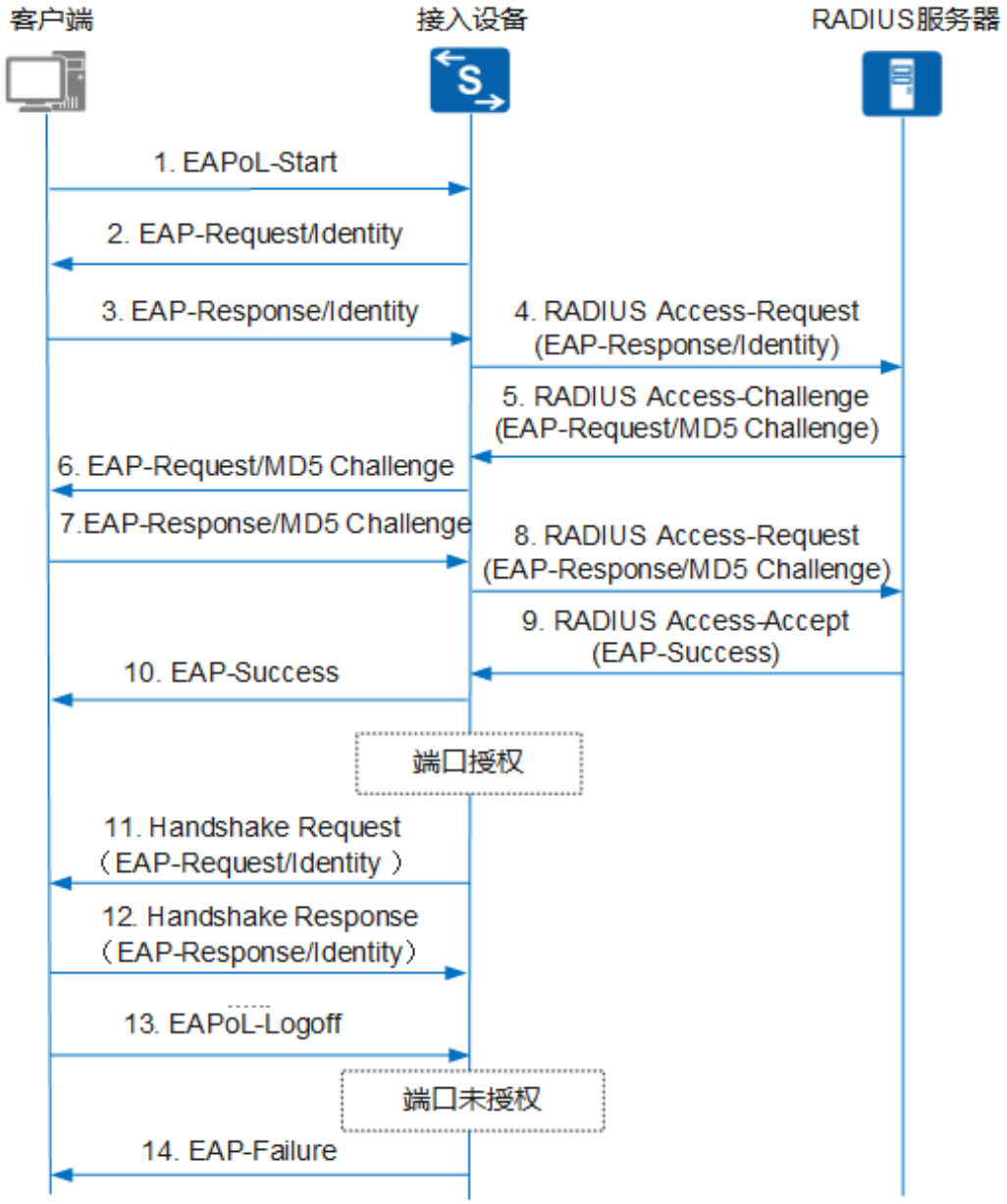
802.1X认证有以下触发方式：

- 客户端发送EAPoL-Start报文触发认证。
- 客户端发送DHCP/ARP/DHCPv6/ND或任意报文触发认证。
- 设备发送EAP-Request/Identity报文触发认证。

EAP 中继和 EAP 终结的认证流程

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。以客户端发送EAPoL-Start报文触发认证为例，EAP中继方式和EAP终结方式的802.1X认证流程分别如图3-1与图3-2所示。

图 3-1 EAP 中继认证流程

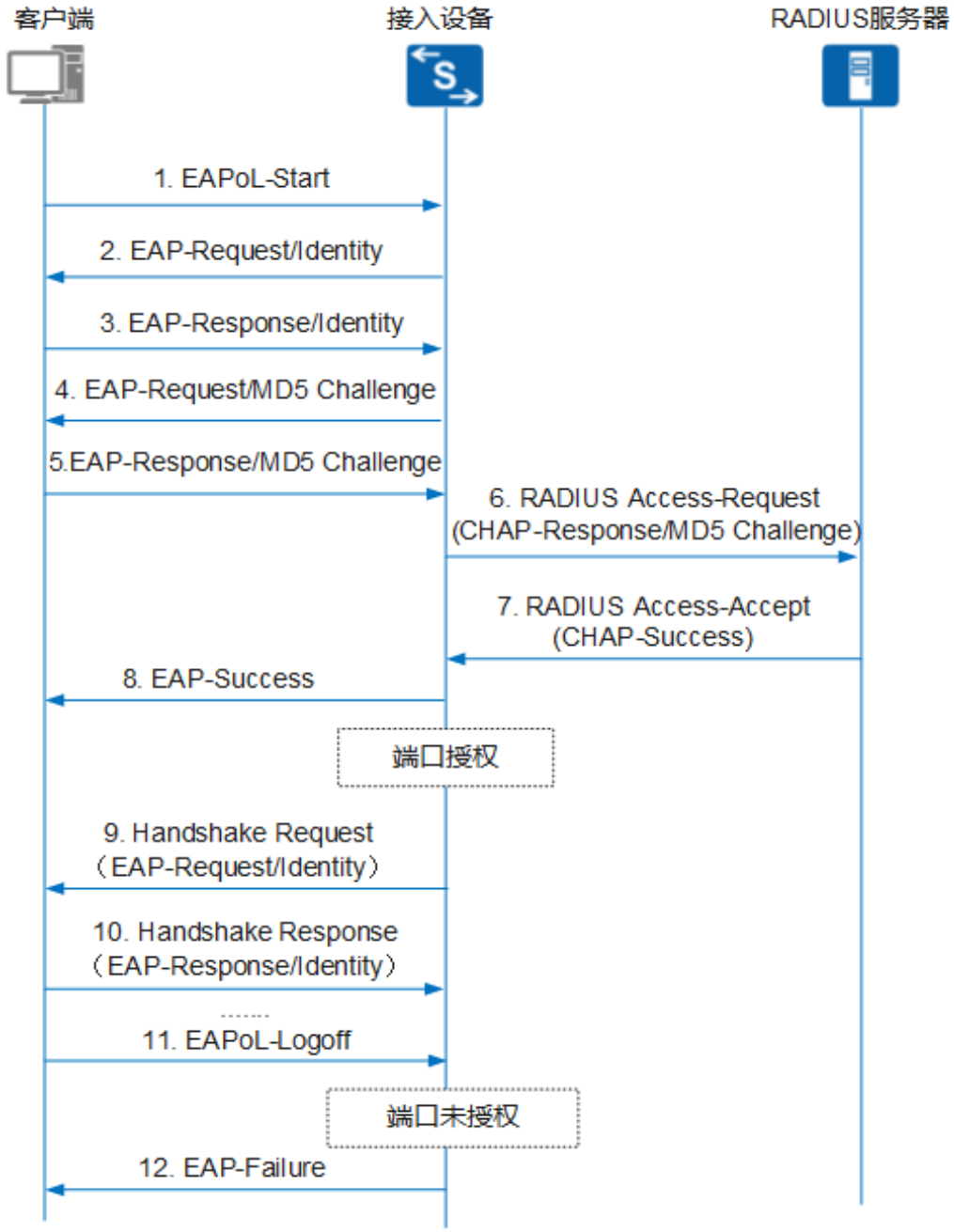


1. 当用户需要访问外部网络时打开802.1X客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求。此时，客户端程序将向设备端发出认证请求报文（EAPoL-Start），开始启动一次认证过程。
2. 设备端收到认证请求报文后，将发出一个Identity类型的请求报文（EAP-Request/Identity）要求用户的客户端程序发送输入的用户名。
3. 客户端程序响应设备端发出的请求，将用户名信息通过Identity类型的响应报文（EAP-Response/Identity）发送给设备端。
4. 设备端将客户端发送的响应报文中的EAP报文封装在RADIUS报文（RADIUS Access-Request）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报文（EAP-Success），并将端口改为授权状态，允许用户通过该端口访问网络。
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报文给设备端，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。

图 3-2 EAP 终结认证流程



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。而在EAP中继方式中，用来对用户密码进行加密处理的挑战字由认证服务器生成，设备端只是负责将EAP报文封装在RADIUS报文中透传认证服务器，整个认证处理都由认证服务器来完成。

4 802.1X 授权

认证用于确认尝试接入网络的用户身份是否合法，而授权则用于指定身份合法的用户所能拥有的网络访问权限，即用户能够访问哪些资源。授权最基础也是最常使用的授权参数是VLAN、ACL和UCL组，此处以RADIUS授权进行说明，其他授权方式的授权方法以及更多可授权的参数请参见AAA授权方案。

VLAN

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的VLAN。用户认证成功后，认证服务器将指定VLAN授权给用户。此时，设备会将用户所属的VLAN修改为授权的VLAN，授权的VLAN并不改变接口的配置。但是，授权的VLAN优先级高于用户配置的VLAN，即用户认证成功后生效的VLAN是授权的VLAN，用户配置的VLAN在用户下线后生效。RADIUS服务器授权VLAN时，必须同时使用以下RADIUS标准属性：

- **Tunnel-Type**：必须配置为“VLAN”或“13”
- **Tunnel-Medium-Type**：必须配置为“802”或“6”
- **Tunnel-Private-Group-ID**：可以是VLAN ID、VLAN描述

ACL

用户认证成功后，认证服务器将指定ACL授权给用户，则设备会根据该ACL对用户报文进行控制。

- 如果用户报文匹配到该ACL中动作为permit的规则，则允许其通过。
- 如果用户报文匹配到该ACL中动作为deny的规则，则将其丢弃。

RADIUS服务器授权ACL有两种方法：

- 授权静态ACL：RADIUS服务器通过RADIUS标准属性**Filter-Id**将ACL ID授权给用户。为使授权的ACL生效，需要提前在设备上配置相应的ACL及规则。
- 授权动态ACL：RADIUS服务器通过华为RADIUS扩展属性**HW-Data-Filter**将ACL ID及其ACL规则授权给用户。ACL ID及其ACL规则需要在RADIUS服务器上配置，设备上不需要配置。

UCL

用户控制列表UCL组（User Control List）是网络成员的集合。UCL组里面的成员，可以是PC、手机等网络终端设备。借助UCL组，管理员可以将具有相同网络访问策略的

一类用户划分为同一个组，然后为其部署一组网络访问策略，满足该类别所有用户的网络访问需求。相对于为每个用户部署网络访问策略，基于UCL组的网络控制方案能够极大的减少管理员的工作量。RADIUS服务器授权UCL组有两种方式：

- 授权UCL组名称：RADIUS服务器通过RADIUS标准属性**Filter-Id**将UCL组名称授权给指定用户。
- 授权UCL组ID：RADIUS服务器通过华为RADIUS扩展属性**HW-UCL-Group**将UCL组ID授权给指定用户。

无论是哪一种授权UCL组方式，都必须提前在设备上配置相应的UCL组及UCL组的网络访问策略。

free-rule

用户认证成功之前，为满足用户基本的网络访问需求，需要用户认证成功前就能获取部分网络访问权限。可在free-rule模板中配置free-rule规则，满足用户的认证成功前的网络访问需求。

用户的free-rule可以通过普通的free-rule定义，也可以通过ACL定义。普通的free-rule由IP地址、MAC地址、接口、VLAN等参数确定；通过ACL定义的free-rule由ACL规则确定。两种方式定义的free-rule都能够指定用户认证成功前就可以访问的目的IP地址。除此之外，ACL定义的free-rule还能够指定用户认证成功前就可以访问的目的域名。

基于域名定义用户的free-rule有时要比基于IP地址简单方便。例如，某些认证用户由于没有认证账号，必须首先在运营商提供的官方网站上注册申请会员账号；或者通过微博、微信等第三方账号进行登录。这就要求用户认证通过前，能够访问特定的网站。由于用户记忆网站的域名要比记忆其IP地址容易的多，所以，此时可以通过ACL定义的free-rule，指定用户认证成功前即可访问以上网站域名。

5 802.1X 重认证

802.1X 认证成功用户

若管理员在认证服务器上修改了某一用户的访问权限、授权属性等参数，此时如果用户已经在线，则需要及时对该用户进行重认证以确保用户的合法性。配置对在线802.1X用户进行重认证功能后，设备会把保存的在线用户的认证参数（用户上线后，设备上会保存该用户的认证信息）发送到认证服务器进行重认证，若认证服务器上用户的认证信息没有变化，则用户正常在线；若用户的认证信息已更改，则用户将会被下线，此后用户需要重新进行认证。802.1X认证成功用户重认证方式如表5-1所示。

表 5-1 802.1X 认证成功用户重认证方式

配置点	方式	配置命令
在接入设备侧配置	对802.1X认证成功用户进行周期性重认证。	**dot1x reauthenticate** **dot1x timer reauthenticate-period** *reauthenticate-period-value*
	手动对指定MAC地址进行单次重认证。	**dot1x reauthenticate mac-address** *mac-address*
在RADIUS服务器侧配置	对802.1X认证成功的用户下发RADIUS标准属性**Session-Timeout**和**Termination-Action**，其中，**Session-Timeout**属性值为用户在线时长定时器，**Termination-Action**属性值为1表示对用户进行重认证。当用户在线时长达到**Session-Timeout**的属性值时，设备会对用户进行重认证。	无

异常认证状态下的用户

用户在预连接阶段或认证失败阶段，设备会记录用户表项信息，并能够为用户分配受限的网络访问权限。为使用户能够及时认证成功，获取正常的网络访问权限，设备根据用户表项对没有认证成功的用户进行重认证。

在用户表项老化时间到达之前，如果用户重认证没有成功，设备将删除对应的表项信息，并收回授予用户的网络访问权限；如果用户重认证成功，设备将用户加入到认证

成功的用户表项，并授予认证成功后的网络访问权限。该部分用户的重认证方式如表5-2所示。

表 5-2 异常认证状态下的用户重认证方式

用户状态	配置命令
RADIUS服务器Down	**authentication event authen-server-up action re-authen**：配置当RADIUS服务器真正UP时对用户进行重认证。
认证失败	**authentication timer re-authen authen-fail** *re-authen-time*：配置对认证失败用户进行周期性重认证。
预连接	**authentication timer re-authen pre-authen** *re-authen-time*：配置对预连接用户进行周期性重认证。

6 802.1X 认证用户下线

当用户已下线，而接入设备和RADIUS服务器未感知到该用户已下线时，会产生以下问题：

1. RADIUS服务器仍会对该用户进行计费，造成误计费。
2. 存在非法用户仿冒合法用户IP地址和MAC地址接入网络的风险。
3. 已下线用户数量过多的情况下，还会占用设备用户规格，可能会导致其他用户无法接入网络。

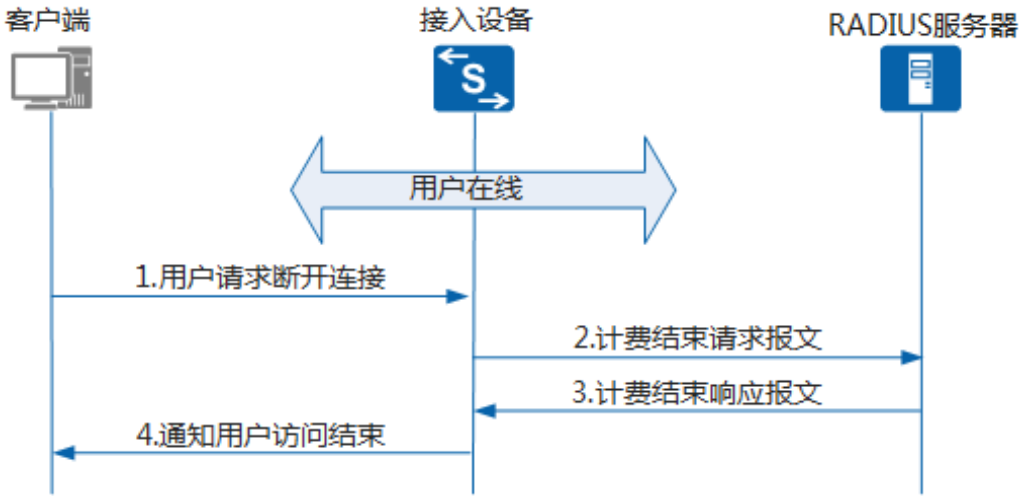
因此，接入设备要能够及时感知到用户已下线，删除该用户表项，并通知RADIUS服务器停止对该用户进行计费。

用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。

客户端主动下线

用户通过客户端软件发送EAPoL-Logoff报文主动下线，设备端会向客户端发一个EAP-Failure的报文，进而将端口状态由授权状态转换为非授权状态。

图 6-1 客户端主动下线的交互流程



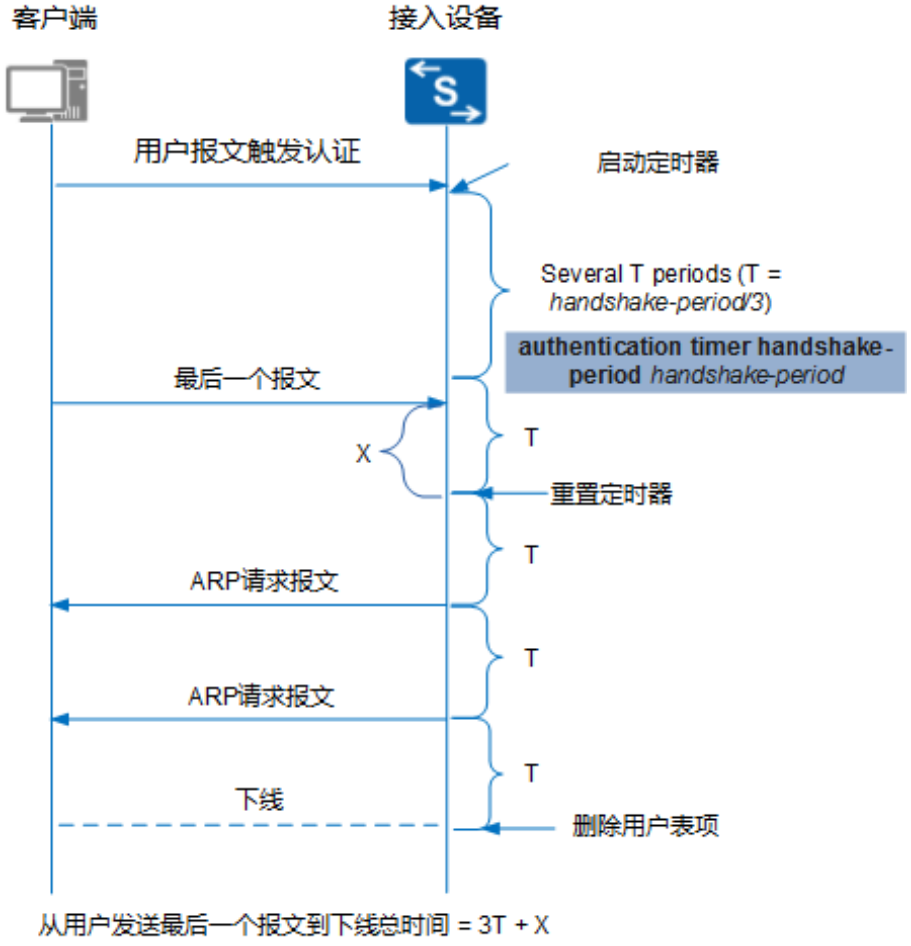
接入设备控制用户下线

接入设备控制用户下线有两种方式：

- 在接入设备上执行命令强制指定用户下线。
- 在接入设备上配置用户探测功能，用于探测用户是否在线。当用户在指定的时间内无响应，则认为用户下线，删除用户表项。

当管理员发现非法用户在线，或在测试中想让某一用户下线后重新上线，可以通过在设备上执行命令强制该用户下线。对于正常接入用户，会通过ARP探测对用户在线状态进行确认，如果探测到用户下线，则进行下线处理，删除用户表项。

图 6-2 用户下线探测流程



假设用户的握手周期为3T。通过命令**authentication timer handshake-period** *handshake-period*配置。T=*handshake-period*/3。

1. 用户发送任意报文触发802.1X认证，同时启动探测定时器。
2. 在若干个T时间内，接入设备均能收到客户端流量，用户在线。
3. 用户最后一次发送报文。在这个T时间结束时，由于有客户端流量，接入设备判断用户在线，并重启定时器。
4. 接入设备在T时间内未收到客户端流量，发送第一次ARP请求，客户端无响应。

5. T时间后，接入设备仍未收到客户端流量，发送第二次ARP请求，客户端无响应。
6. T时间后，接入设备仍未收到客户端流量，探测失败，删除用户表项。

服务器控制用户下线

服务器控制用户下线有以下方式：

- RADIUS服务器可通过DM报文（Disconnect Message）强制用户下线。DM（Disconnect Message）是指用户离线报文，即由RADIUS服务器端主动发起的强迫用户下线的报文。
- RADIUS服务器通过授权RADIUS标准属性Session-Timeout和Termination-Action。其中，Session-Timeout为用户在线时长定时器，Termination-Action属性值为0表示将用户下线。当用户在线的时长达到定时器指定的数值时，设备会将用户下线。

7 802.1X 定时器

802.1X认证中，通过定时器对认证过程进行控制，下面分别介绍一下这几种定时器。

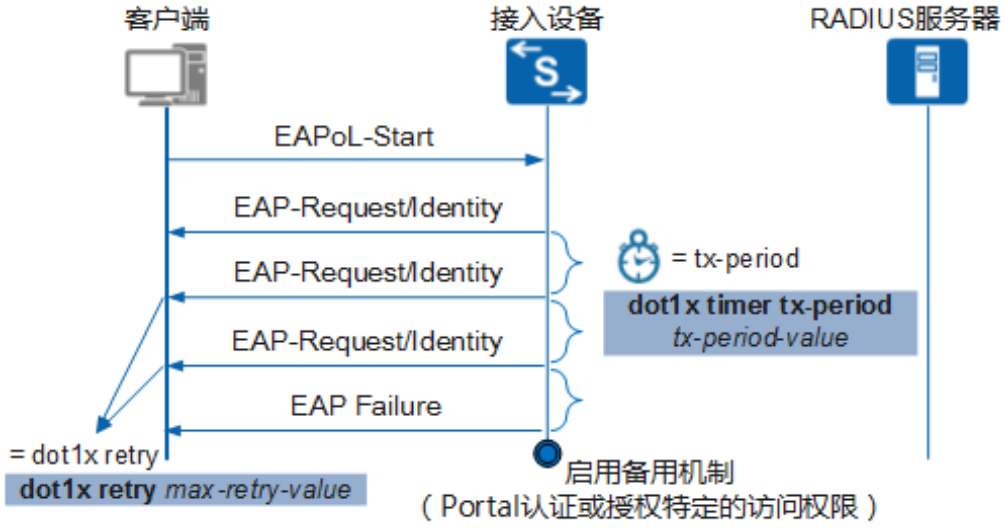
EAP-Request/Identity 请求超时

在802.1X认证中，设备会向客户端发送EAP-Request/Identity报文请求用户名，请求报文的重传次数和时间间隔由命令行控制。

如图7-1所示，设备发送EAP-Request/Identity请求报文超时后，向客户端发送认证失败报文。通常情况下，客户端认证失败时，为使得客户端能够继续访问网络，会在设备上启用备用机制（Portal认证或授权特定访问权限）。

未配置MAC旁路认证时，定时器由命令**dot1x timer tx-period** *tx-period*配置，设备重传请求报文的次数通过命令**dot1x retry** *max-retry-value*配置。EAP-Request/Identity请求超时计算公式为：Timeout = (*max-retry-value* +1) * *tx-period-value*

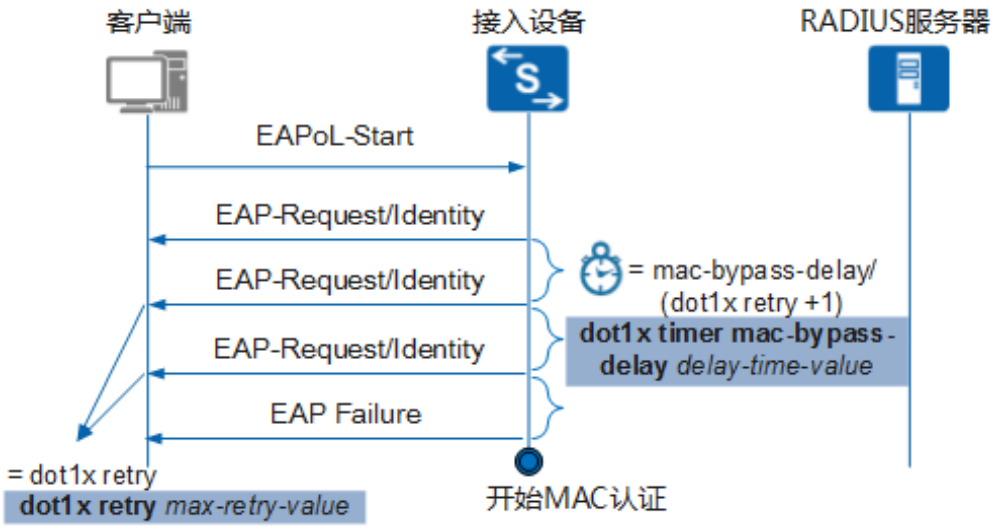
图 7-1 802.1X 认证 EAP-Request/Identity 请求超时



如图7-2所示，当配置MAC旁路认证功能后，设备首先会对用户进行802.1X认证，同时启动命令**dot1x timer mac-bypass-delay** *delay-time-value*配置的定时器。如果定时器时间*delay-time-value*到达而802.1X认证仍未成功，则设备开始对用户进行MAC认证。可

以通过命令**dot1x retry** *max-retry-value*配置设备向802.1X用户发送认证请求的重传次数*max-retry-value*，重传时间间隔为*delay-time-value*/(*max-retry-value*+1)的整数部分。

图 7-2 MAC 旁路认证请求超时



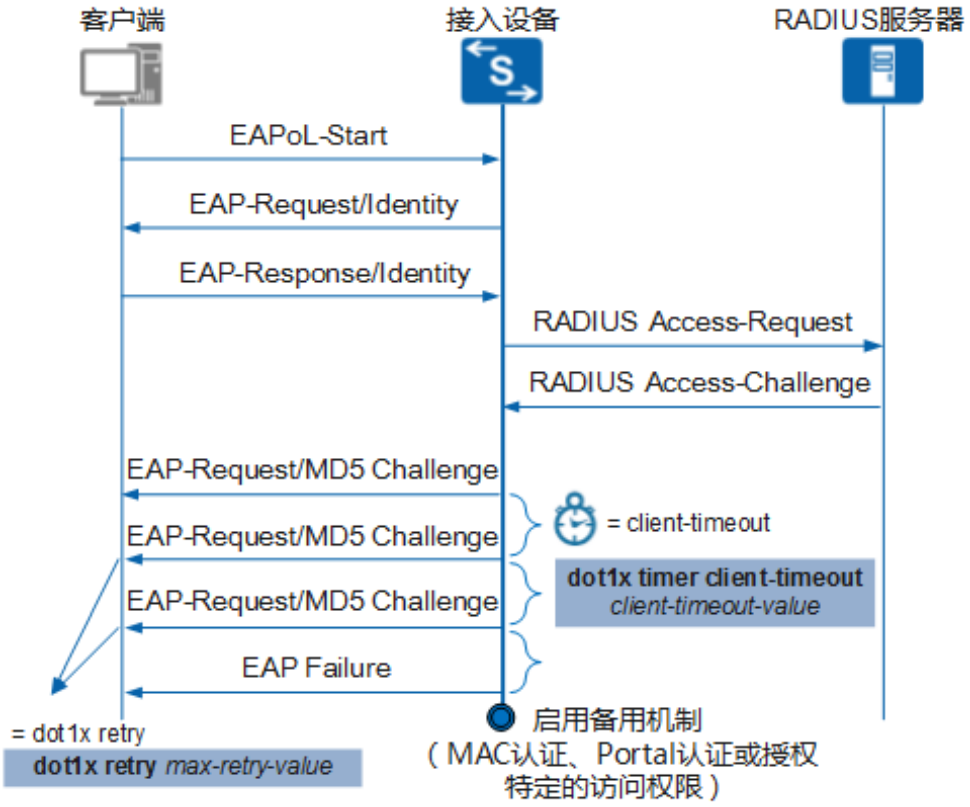
EAP-Request/MD5 Challenge 请求超时

当设备向802.1X客户端发送了EAP-Request/MD5 Challenge请求报文后，设备启动802.1X客户端认证超时定时器。若在该定时器设置的时长内，设备没有收到客户端的响应，则设备将重发该报文。若设备重传请求报文的次数达到配置的最大值（通过命令**dot1x retry** *max-retry-value*配置）后，仍然没有得到用户响应，则停止发送认证请求。这能够避免不断重复向用户发送认证请求报文而占用大量的设备资源。

如图7-3所示，设备发送EAP-Request/MD5 Challenge请求报文超时后，向客户端发送认证失败报文。通常情况下，客户端认证失败时，为使得客户端能够继续访问网络，会在接入设备上启用备用机制（MAC认证、Portal认证或授权特定的访问权限）。EAP-Request/MD5 Challenge请求超时计算公式如下所示：

Timeout = (*max-retry-value* +1) * *client-timeout-value*

图 7-3 802.1X 认证 EAP-Request/MD5 Challenge 请求超时



802.1X 认证静默定时器

使能静默功能后，若某一用户在60秒内认证失败的次数超过命令**dot1x quiet-times** *fail-times*规定的值，则设备会将该用户静默一段时间，该时间由命令**dot1x timer quiet-period** *quiet-period-value*指定，在静默时间内，设备会丢弃该用户的802.1X认证请求，从而避免用户在短时间内频繁认证失败。

图 7-4 802.1X 认证静默定时器