

第 6 篇 园区网安全技术

第 23 章 园区网安全概述

第 24 章 AAA、RADIUS 和 TACACS+

第 25 章 端口接入控制

第 26 章 网络访问控制

第 27 章 SSH

第23章 园区网安全概述

园区网络在功能和性能日益提升的同时，安全问题也逐渐突出，常见的安全威胁有非法接入网络、非法访问网络资源、报文窃听、MAC 地址欺骗等。本章首先介绍网络安全的概念，然后对上述园区网络中的安全威胁进行介绍，最后介绍对应的安全防范措施，包括安全架构、端口接入控制、访问控制和安全连接等。

23.1 本章目标

课程目标

● 学习完本课程，您应该能够：


- 了解网络安全的概念
- 了解园区网常见的安全威胁
- 掌握园区网涉及的安全技术



www.h3c.com

23.2 网络安全概述

网络安全概念



紫光集团 H3C
核心企业 | 数字化解决方案领导者

- **两层含义**
 - 保证内部局域网的安全
 - 保证内网和外网数据交换的安全
- **关注的内容**
 - 保护网络设备、物理线路不会轻易遭受攻击
 - 有效识别合法和非法用户
 - 访问控制、病毒防范等
- **目标**
 - 明确要保护什么、明确可能的网络安全威胁、明确可采取的安全防护措施

www.h3c.com

网络安全是 Internet 必须面对的一个实际问题，也是一个综合性技术。网络安全具有两层含义：保证内部局域网的安全以及保证内网与外网数据交换的安全。

常常从如下几个方面综合考虑整个网络的安全：

- 保护物理网络线路不会轻易遭受攻击；
- 有效识别合法的和非法的用户；
- 实现有效的访问控制；
- 保证内部网络的隐蔽性；
- 有效的防伪手段，重要的数据重点保护；
- 对网络设备、网络拓扑的有效管理；
- 病毒防范。

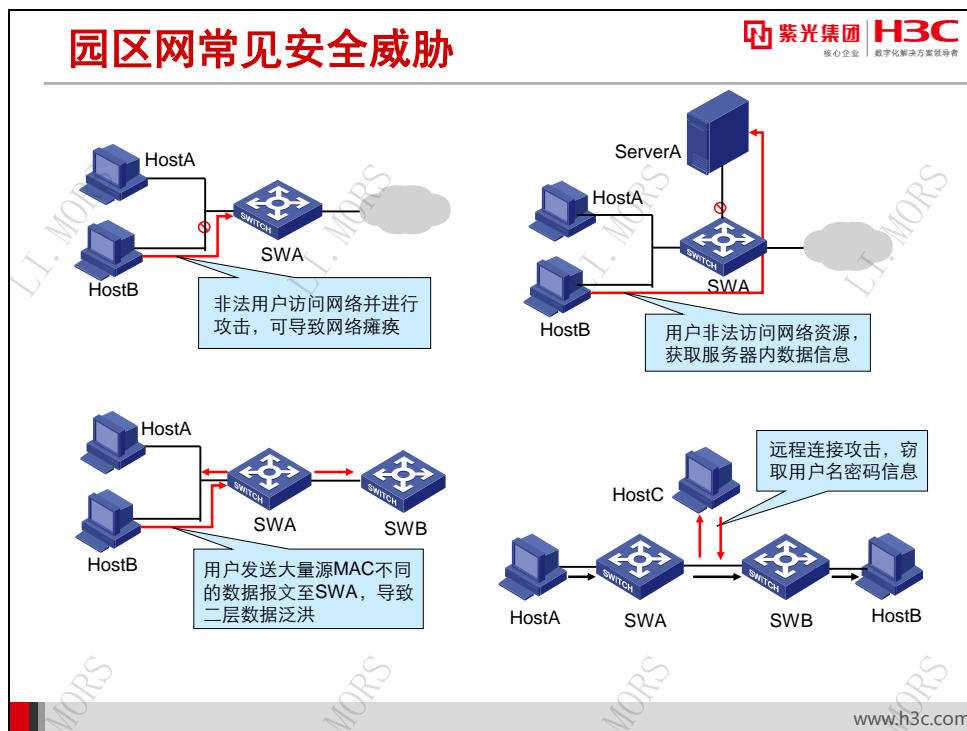
需要保护的资源

- 网络设备：路由器、交换机
- 运行信息：路由表、MAC地址表
- 带宽资源：带宽、速率
- 网络终端：服务器、用户主机
- 网络数据：IP包
- 用户信息：用户ID、密码等

从网络安全关注的内容中可以看出，需要保护的资源包括：

- 网络设备：能够抵御攻击，可以进行正常的流量转发；
- 运行信息：网络设备能够正常维持内部转发表项，不会出现数据包泛洪的情况；
- 带宽资源：能够抵御流量攻击；
- 网络终端：抵御非法访问，关闭服务器漏洞，避免服务器因受到破坏而无法正常工作；
- 网络数据：保护网络数据包的内容不被篡改，验证报文来自真正的对方；
- 用户信息：保护用户的 ID、密码不被窃听。

23.3 园区网常见安全威胁

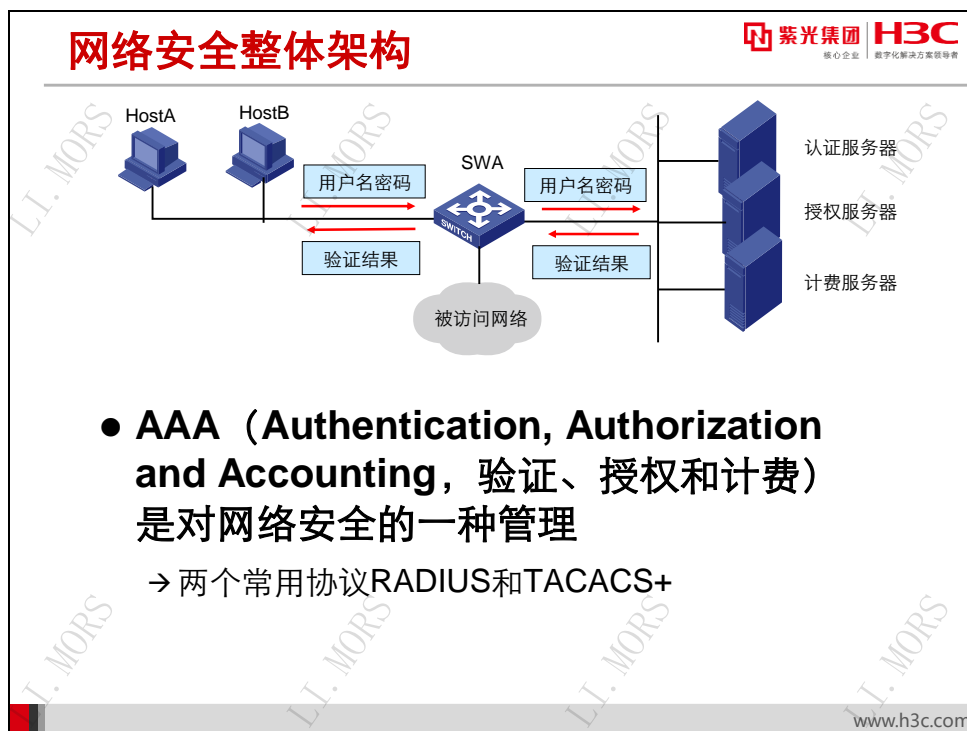


园区网常见的安全威胁包括非法接入网络、非法访问网络资源、MAC 地址欺骗和泛洪、报文窃听等。

- **非法接入网络：**是非法访问网络资源的前提。即使接入网络后不访问网络资源，攻击者也可以采用 DoS 攻击等手段导致网络瘫痪。
- **非法访问网络资源：**指非法用户在没有被授权的情况下访问局域网设备或数据，修改网络设备的配置和运行状态，获取数据。
- **MAC 地址欺骗和泛洪：**是通过发送大量源 MAC 地址不同的数据报文，使得交换机端口 MAC 地址表学习达到上限，无法学习新的 MAC 地址，从而导致二层数据泛洪。
- **远程连接攻击：**对 TELNET 等连接进行攻击，包括截取用户名密码等用户信息或数据信息，篡改数据并重新投放到网络上等。

23.4 园区网安全防范措施

23.4.1 安全网络整体架构




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

AAA 的实现常采用两种协议：RADIUS 和 TACACS+。

- **RADIUS (Remote Authentication Dial In User Service, 远程认证拨号用户服务)** 是一种分布式的、客户端/服务器模式的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。
- **TACACS+ (Terminal Access Controller Access Control System Plus, 终端访问控制器控制系统协议+)** 与 RADIUS 协议类似，采用客户端/服务器模式实现网络接入设备与 TACACS 服务器之间的通信。其典型应用是对需要登录到设备上进行操作的用户进行认证、授权和计费。交换机作为 TACACS+ 的客户端，将用户名和密码发给 TACACS+ 服务器进行验证。用户验证通过并得到授权之后可以登录到设备上进行操作。

23.4.2 端口接入控制

端口接入控制

 紫光集团 **H3C**
核心企业 | 数字化解决方案领导者

- **端口接入控制技术包括802.1X、MAC地址认证和端口安全等基于端口的安全技术**
 - 802.1X协议要求主机端安装802.1X客户端软件
 - MAC地址认证以主机MAC地址作为用户名进行认证，无需特殊软件
 - 端口安全是在802.1X和MAC认证基础之上的灵活扩展应用



```
graph LR; HostA[HostA] --- SWA[SWA]; HostB[HostB] --- SWA; SWA --- RADIUS[RADIUS服务器];
```

www.h3c.com

针对非法接入网络，可以采用端口接入控制技术来进行防范。端口接入技术包括 802.1X 技术、MAC 地址认证和端口安全。

802.1X 协议是一种基于端口的网络接入控制协议，在局域网接入设备的端口这一级对所接入的用户进行认证和控制。连接在端口上的用户如果能够通过认证，就可以访问局域网的资源；如果认证失败，这无法访问局域网的资源。802.1X 系统为典型的客户端/服务器模式，包括三个实体：客户端、设备端和认证服务器。用户可以通过启动客户端软件发起 802.1X 认证，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。

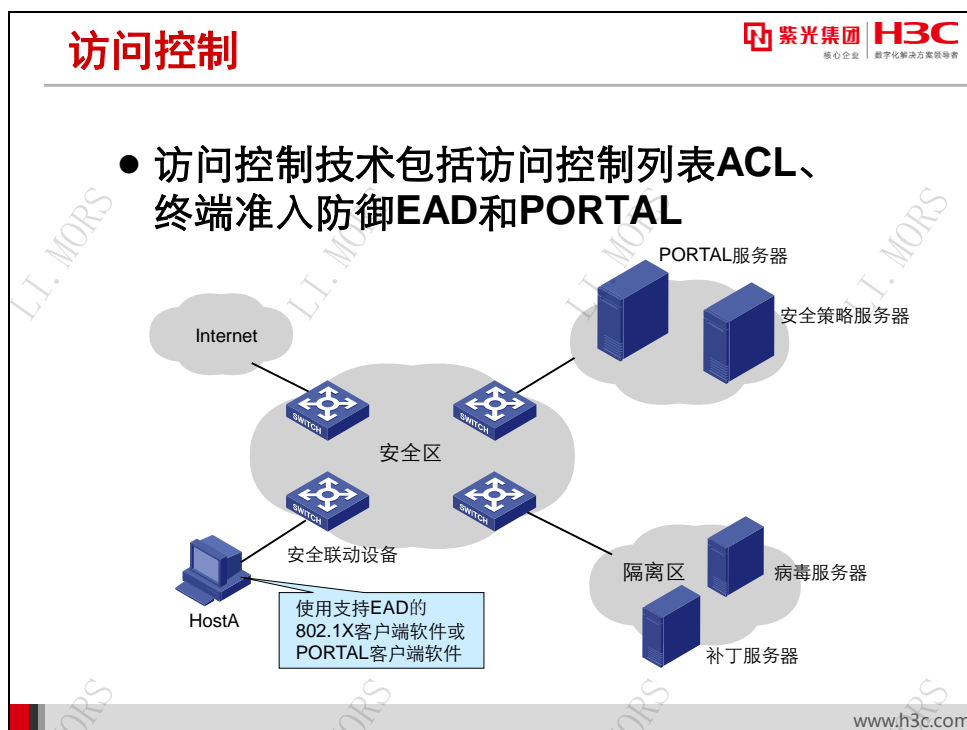
MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何软件。设备在首次检测到用户的 MAC 地址后，即启动对该用户的认证操作。认证过程中也不需要输入用户名和密码。

端口安全特性是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。通过定义各种端口安全模式，让设备学习到合法的安全 MAC 地址，以达到相应的网络管理效果。提供了 802.1X 和 MAC 地址认证的扩展和组合应用。

注意：

由于端口安全特性通过多种安全模式提供了 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。

23.4.3 访问控制



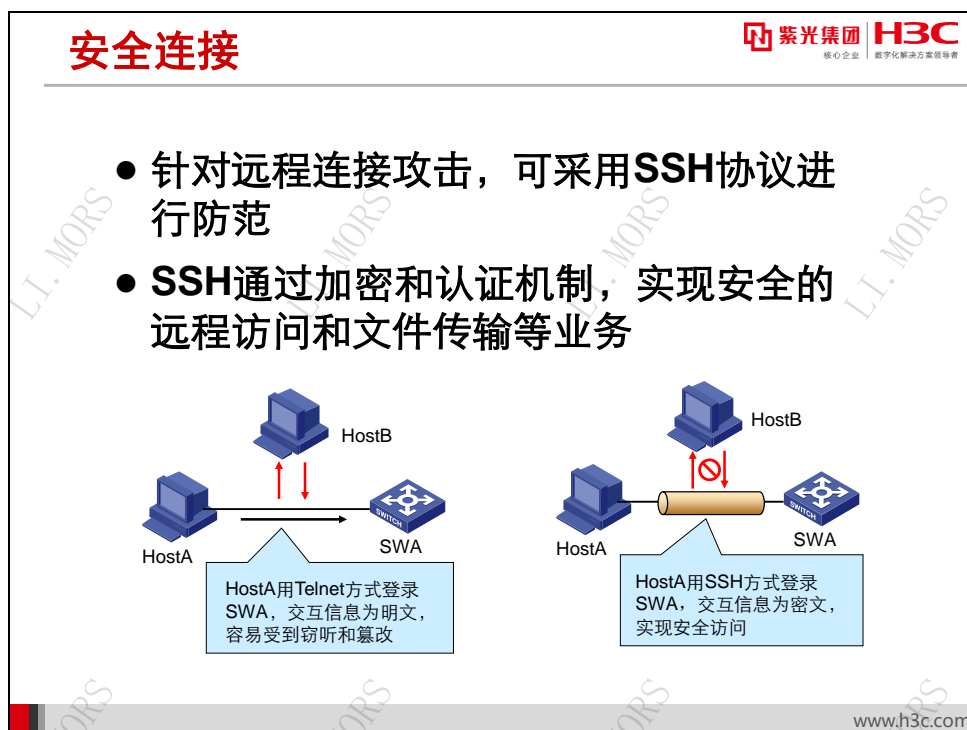
针对非法访问网络资源，可以采用网络访问控制技术进行防范，常用的包括访问控制列表ACL、终端准入防御EAD和PORTAL。

ACL（Access Control List，访问控制列表）可以实现流识别功能，配置一系列的匹配条件对报文进行分类，达到过滤报文的目的，匹配条件可以是报文的源地址、目的地址、端口号等。设备可以通过在用户接入的端口配置恰当的ACL，来抵御用户访问非法网络资源。

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，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。当EAD客户端进行安全认证失败时，只能访问隔离区域，进行软件升级和病毒库升级操作；当安全认证成功时，可以访问安全区的网络资源。

PORTAL认证通常被称为WEB认证，即必须通过门户网站的认证，才能够访问网络资源。PORTAL的扩展功能包括通过强制接入终端实施补丁和防病毒策略，加强网络终端对病毒抗攻击的主动防御能力。

23.4.4 安全连接




针对远程连接攻击，可以采用 **SSH** 进行防范。用户在一个不安全的网络环境中远程登录到设备时，**SSH**（**Secure Shell**，安全外壳）可以利用加密和强大的认证功能提供安全保障，保证设备不受 IP 欺诈、明文密码截取等攻击。

SSH 提供了三种机制，以构成它所提供的服务的基础：

- 一个传输层协议：提供了服务器鉴别、数据保密性、数据完整性功能；
- 一个用户鉴别协议：用于服务器鉴别用户；
- 一个链接协议：可以在一条底层 **SSH** 连接上复用多条逻辑通信通道。

23.4.5 其他安全防范措施

其他安全防范措施



核心企业 | 数字化解决方案领导者

- 防火墙是一种高级访问控制设备
 - 根据相应的安全策略控制进出网络的访问行为
- **IPS (Intrusion Protection System, 入侵防御系统)** 主要对网络进行监控, 尽可能发现各种攻击行为并进行防御
- **VPN (Virtual Private Network, 虚拟专用网)** 实现在公用网络上构建私人专用网络

www.h3c.com

园区网中还会涉及到其他的安全技术, 包括防火墙、IDS、VPN 技术等。

防火墙是一种高级访问控制设备, 一方面可以阻止来自因特网的、对受保护网络的未授权访问, 另一方面允许内部网络用户对因特网进行 WEB 访问或收发电子邮件等。同时防火墙还有其他特点, 例如进行身份鉴别、对信息进行安全加密处理等。

IPS (Intrusion Protection System, 入侵防御系统) 依照一定的安全策略, 对网络系统的运行情况进行监视, 尽可能发现各种攻击企图、攻击行为并采取有效的防御措施, 以保证网络系统资源的机密性、完整性和可用性, 是一种主动保护。

VPN (Virtual Private Network, 虚拟专用网) 利用公共网络来构建私人专用网络。在公共网上传输数据, 必须提供隧道、加密以及报文的验证, 因此 VPN 能够像私有网络一样提供安全性、可靠性、可管理性和服务质量。

23.5 本章总结

本章总结

- 园区网的安全概念包含两层含义
- 常见的安全威胁有非法接入、非法访问网络资源、**MAC**地址欺骗和泛洪、报文窃听
- 常用的安全防范措施包括端口接入控制、访问控制、安全连接等

23.6 习题和解答

23.6.1 习题

1. 什么是网络安全？（ ）
 - A. 保证用户可以随意使用网络资源
 - B. 保证内部局域网的安全
 - C. 保证内部局域网不被非法侵入
 - D. 保证内网与外网数据交换的安全
2. 以下哪几种行为属于网络威胁或者黑客行为？（ ）
 - A. 利用现成的软件后门，获取网络管理员的密码
 - B. 进入自己的计算机并修改数据
 - C. 利用电子窃听技术，获取要害部门的口令
 - D. 利用工具软件，非法攻击网络设备
3. AAA 架构常使用如下哪些协议？（ ）
 - A. RADIUS 协议
 - B. PPPOE 协议
 - C. 802.1X 协议
 - D. TACACS+ 协议
4. 我司常用的接入协议有（ ）？
 - A. 802.1X 协议
 - B. Portal 认证
 - C. MAC 认证
 - D. 端口安全
5. 如下哪些技术或措施可用于园区网的安全防护？（ ）
 - A. SSH
 - B. VPN
 - C. EAD
 - D. 远程 TELNET

23.6.2 习题答案

1. BCD
2. B
3. AD
4. ABCD
5. ABC

第24章 AAA、RADIUS 和 TACACS+

AAA（Authentication, Authorization and Accounting，认证、授权和计费）是一个综合的安全架构。和其他一些安全技术配合使用，可以提升网络和设备的安全性。本章对 AAA 架构以及常用的 AAA 协议 RADIUS 和 TACACS+进行介绍。

AAA 是一种管理框架，它提供了授权部分实体去访问特定的资源，同时可以记录这些实体操作行为的一种安全机制，具有良好的可扩展性，容易实现用户信息的集中管理，目前被广泛使用。

24.1 本章目标

课程目标

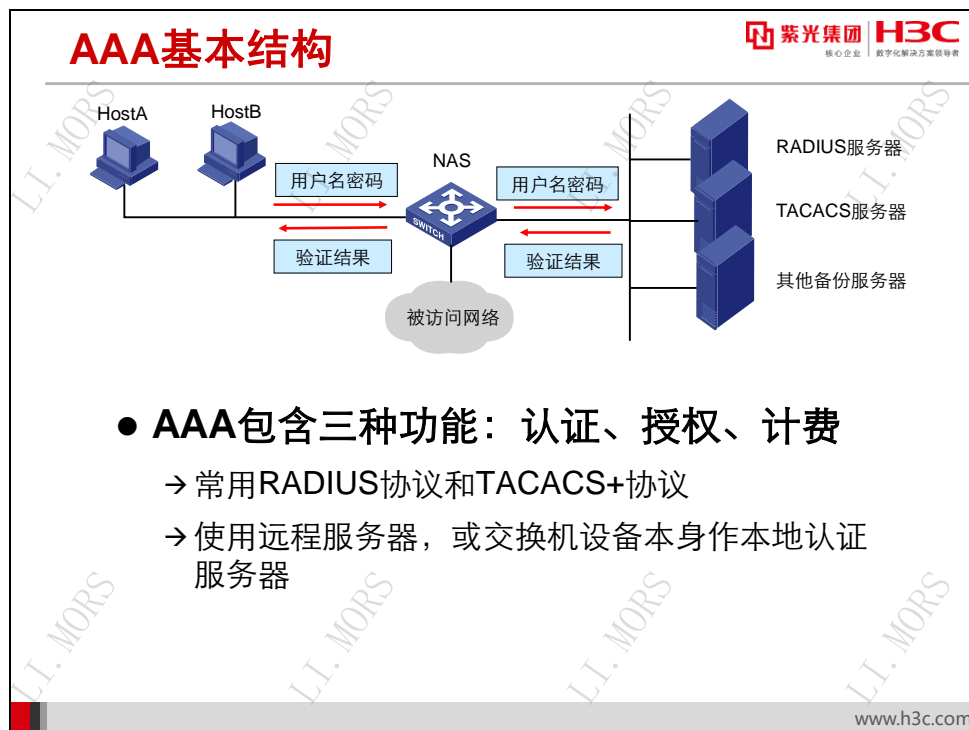
学习完本课程，您应该能够：

- 掌握AAA认证架构
- 掌握RADIUS、TACACS+认证原理
- 熟悉AAA、RADIUS和HWTACACS相关配置命令



24.2 AAA架构

24.2.1 AAA 基本结构



● AAA包含三种功能：认证、授权、计费

- 常用RADIUS协议和TACACS+协议
- 使用远程服务器，或交换机设备本身作本地认证服务器

AAA（Authentication, Authorization and Accounting，认证、授权和计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。AAA 一般采用客户机/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，服务器则集中管理用户信息。

AAA 的三种安全功能具体作用如下：


- **认证**：确认远端访问用户的身份，判断访问者是否为合法的网络用户。
- **授权**：对认证通过的不同用户赋予不同的权限，限制用户可以使用的服务。例如用户成功登录服务器后，管理员可以授权用户对服务器中的文件进行访问和打印操作。
- **计费**：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等，它不仅是一种计费手段，也对网络安全起到了监视作用。

AAA 可以通过多种协议来实现，目前常用的是 RADIUS 协议和 TACACS+协议。RADIUS 协议和 TACACS+协议规定了 NAS 与服务器之间如何传递用户信息。二者在结构上都采取客户机/服务器模式，都使用公共密钥对传输的用户信息进行加密，都有较好的灵活性和可扩展性。两者之间存在的区别主要体现在传输协议的使用、信息包加密、认证授权分离、多协议支持等。

H3C 交换机也提供本地认证功能，即将用户信息（包括用户名、密码和各种属性）配置在设备上，此认证类型的优点是认证速度快。

如上图 AAA 基本结构图中，用户可以根据实际组网需要来决定认证、授权、计费功能分别由使用哪种协议的服务器来承担，其中 NAS 负责把用户的认证、授权、计费信息透传给服务器（RADIUS 服务器或 TACACS+服务器）。例如可以用 TACACS+服务器实现认证和授权，用 RADIUS 服务器实现计费。当然用户也可以只使用 AAA 提供的一种或两种安全服务。

AAA支持的服务



- **AAA通过对服务器的详细配置，对多种服务提供安全保证**
 - 支持FTP、TELNET、PPP、端口接入
- **验证动作包含核对用户名、密码、证书**
- **授权表现为下发用户权限、访问目录、用户级别等**
- **计费表现为记录用户上网流量、时长等**

www.h3c.com



通过对认证、授权、计费服务器进行详细配置，AAA 能够对多种服务提供安全保证，包括 FTP 服务、TELNET 服务、PPP、端口控制等。

在 AAA 中，三种安全功能三个独立的业务流程，其中：

- **认证：**完成各接入或服务请求的用户名、密码、用户信息的交互过程，它不会下发授权信息给用户，也不会触动计费流程。
- **授权：**发送授权请求给所配置的授权服务器，授权通过后向用户下发授权信息。例如为 TELNET 用户、SSH 用户下发访问级别，为 FTP 用户设定访问目录等。授权为可选配置。
- **计费：**发送计费开始、计费更新、计费结束请求报文给所配置的计费服务器。计费不是必须使用的。

24.2.2 AAA 配置

配置AAA

 紫光集团  H3C
核心企业 | 数字化解决方案领导者

- **AAA认证方案：配置本地认证或远程认证方案**
 → 远程认证需要配置RADIUS方案或TACACS+方案

- **AAA实现方法：在ISP域中引用已经配置的AAA方案**

```
[sysname-isp-ispname] authentication default { hwtacacs-
scheme hwtacacs-scheme-name [ local ] | local | none | radius-
scheme radius-scheme-name [ local ] }
```

www.h3c.com

AAA 的配置可以分为两部分：

第1步：根据需要配置本地认证或远程认证方案，远程认证时需要配置 RADIUS 方案或 TACACS+方案：

- 本地认证：需要在交换机上配置本地用户名，并设置相应的密码和用户级别。

```
[sysname] local-user username
```

- RADIUS 方案(radius-scheme)：通过引用已配置的 RADIUS 方案来实现认证、授权、计费。

```
[sysname] radius scheme radius-scheme-name
```

- TACACS+方案(hwtacacs-scheme)：通过引用已配置的 TACACS+方案来实现认证、授权、计费。

```
[sysname] hwtacacs scheme hwtacacs-scheme-name
```

第2步：创建用户所属的 ISP（Internet Service Provider，Internet 服务提供商），并在 ISP 域中引用已经配置的 AAA 方案。以认证方法为例：

```
[sysname] domain isp-name
```

```
[sysname-isp-ispname] authentication default { hwtacacs-scheme hwtacacs-
scheme-name [local] | local | none | radius-scheme radius-scheme-name [local] }
```

其中主要参数含义如下：

- **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**]: 指定 TACACS+方案;
 - **local**: 本地认证;
 - **none**: 不进行认证;
 - **radius-scheme** *radius-scheme-name* [**local**]: 指定 RADIUS 方案。
-

注意:

如果配置了 **radius-scheme** *radius-scheme-name* **local** 或 **hwtacacs-scheme** *hwtacacs-scheme-name* **local**, 则 **local** 为 RADIUS 服务器或 TACACS+服务器没有正常响应后的备选认证方案。

在 AAA 方案认证域中, 引用认证方案的同时, 还必须引用授权方案和计费方案。

24.3 RADIUS 协议

24.3.1 RADIUS 协议概述

RADIUS 协议概述

- **RADIUS (Remote Authentication Dial-In User Service, 远程认证拨号系统)** 是分布式的交互协议
- **客户端/服务器结构**
- **基于UDP传输, 1812、1813端口**
- **共享密钥、多种认证方式**
- **TLV结构, 利于扩展**

www.h3c.com

RADIUS (Remote Authentication Dial-In User Service, 远程认证拨号用户服务) 是一种分布式、客户端/服务器结构的信息交互协议, 能保护网络不受未经授权访问的干扰, 常应用在其要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了基于 UDP 端口 1812、1813 分别作为认证、计费端口。

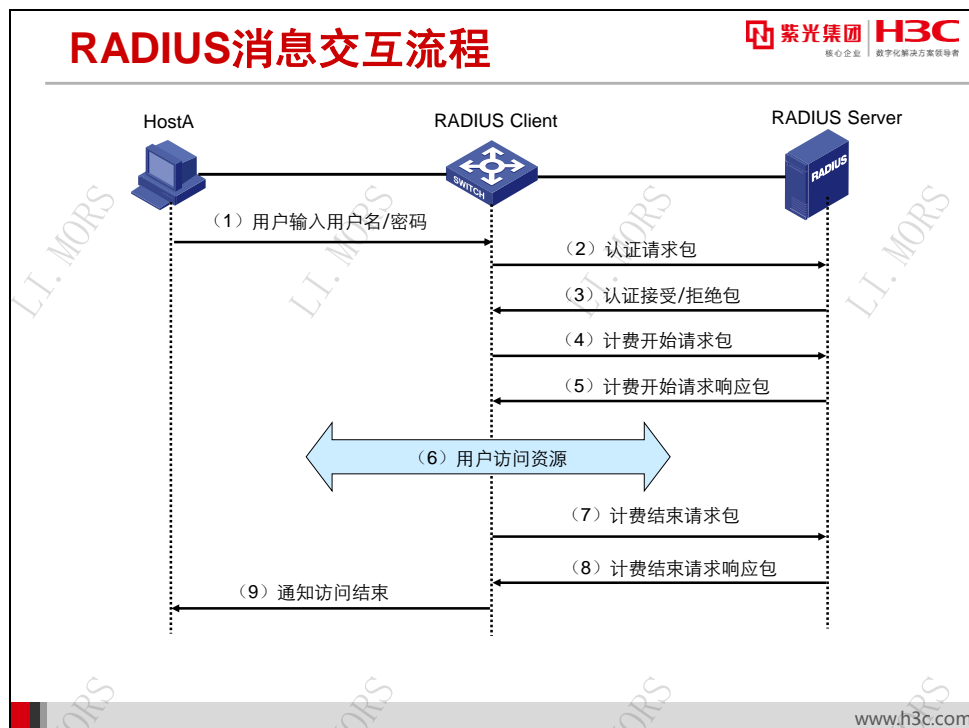
RADIUS 最初仅是针对拨号用户的 AAA 协议, 后来随着用户接入方式的多样化发展, RADIUS 也适应多种用户接入方式, 如以太网接入、ADSL 接入。它通过认证授权来提供接入服务, 通过计费来收集、记录用户对网络资源的使用。

RADIUS 的客户端/服务器模式为:

- NAS 设备作为 RADIUS 客户端, 负责传输用户信息到指定的 RADIUS 服务器上, 然后根据从服务器返回的信息进行相应处理 (如接入/挂断用户);
- RADIUS 服务器负责接收用户连接请求, 认证用户, 给设备返回所需要的信息。

RADIUS 客户端与服务器之间认证消息的交互是通过共享密钥的参与来完成, 并且共享密钥不能通过网络来传输, 增强了信息交互的安全性, 同时在传输过程中对用户密码进行了加密。RADIUS 服务器支持多种方法来认证用户, 如基于 PPP 的 PAP、CHAP 认证等。

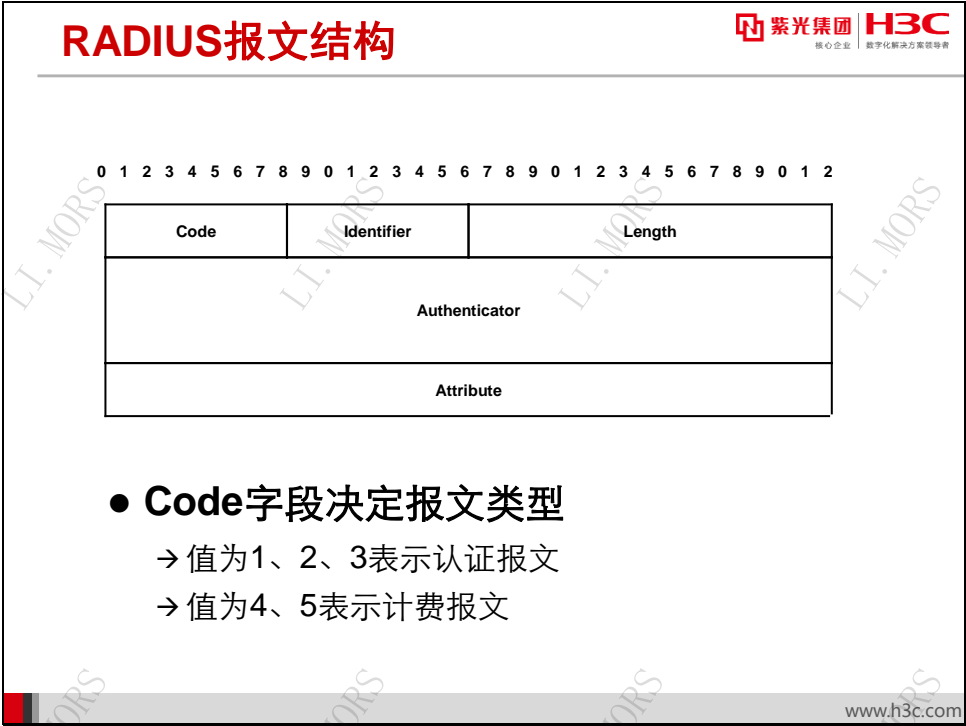
24.3.2 RADIUS 消息交互流程



RADIUS 消息交互流程如下：

- 1) 用户发起连接请求，输入用户名和密码；
- 2) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），密码在共享密钥的参与下进行加密处理；
- 3) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept），同时也包含用户的授权信息；如果认证失败，则返回认证拒绝包（Access-Reject）；
- 4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 RADIUS 客户端向服务器发送计费开始请求包（Accounting-Request）；
- 5) RADIUS 服务器返回计费开始响应包（Accounting-Response），并开始计费；
- 6) 用户开始访问网络资源；
- 7) 用户请求断开连接，RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）；
- 8) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费；
- 9) 用户结束访问网络资源。


24.3.3 RADIUS 报文结构




- Identifier 字段（1 字节）用于匹配请求包和响应包，以及检测一段时间内重发的请求包；
- Length 字段（2 字节）指明整个 RADIUS 数据包的长度；
- Authenticator 字段（16 字节）用于验证 RADIUS 服务器的应答，还用于密码的加密；
- Attribute 字段（不定长度）携带认证、授权和计费信息，提供请求和响应报文的配置细节，可包括多个属性，采用 TLV 的三元组形式。

24.3.4 RADIUS 属性

RADIUS属性

 紫光集团

 H3C

核心企业 | 数字化解决方案领导者

- Attribute 字段携带认证、授权、计费信息
- 采用（Type, Length, Value）三元组格式
- 常用属性

编号	属性名称	编号	属性名称
1	User-Name	11	Filter-ID
2	User-Password	15	Login-Service
4	NAS-IP-Address	26	Vendor-Specific
8	Framed-IP-Address	31	Calling-Station-ID

www.h3c.com

RADIUS 报文中 Attribute（属性）字段专门携带认证、授权和计费信息，请求提供和相应报文的配置细节，该字段采用 TLV（Type, Length, Value，类型、长度、值）三元组的形式提供。

- 类型（Type）字段 1 个字节，取值为 1~255，用于指明属性的类型，表 24-2 列出了 RADIUS 认证、授权常用的属性；
- 长度（Length）字段 1 个字节，指明此属性的长度，单位为字节，包括类型字段、长度字段和属性字段；
- 属性值（Value）字段包括该属性的信息，其格式和内容由类型字段和长度字段决定，最大长度为 253 字节。

表24-2 常用 RADIUS 标准属性

属性编号	属性名称	描述
1	User-Name	需要进行认证的用户名称
2	User-Password	需要进行PAP方式认证的用户密码，在采用PAP方式认证时，该属性仅出现在Access-Request报文中
3	CHAP-Password	需要进行CHAP方式认证的用户密码摘要。在采用CHAP方式认证时，该属性出现在Access-Request报文中
4	NAS-IP-Address	Server通过不同的IP地址来标识不同的Client，通常Client采用本地一个接口IP地址来唯一标识自己，即NAS-IP-Address。该属性指示当前发起请求的Client的NAS-IP-Address，仅出现在Access-Request报文中
5	NAS-Port	用户接入NAS的物理端口号
6	Service-Type	用户申请认证的业务类型
8	Framed-IP-Address	为用户所配置的IP地址
11	Filter-ID	访问控制列表的名称
15	Login-Service	用户登录设备时采用的服务类型
26	Vendor-Specific	厂商自定义的私有属性。一个报文中可以有一个或多个私有属性，每个私有属性中可以有一个或多个子属性
31	Calling-Station-ID	NAS用于向Server告知标识用户的号码，在H3C设备提供的LAN-Access业务中，该字段填充的是用户MAC地址，采用的“HHHH-HHHH-HHHH”格式封装

RADIUS扩展属性

0

1

2

3

4

5

6

7

8

9

0

1

2

3

4

5

6

7

8

9

0

1

2

3

4

5

6

7

8

9

0

1

2

Type	Length	Vendor-ID	
VendorID		Type (Specified)	Length (Specified)
Specified attribute Value.....			

www.h3c.com

RADIUS 协议具有良好的可扩展性，协议中定义的 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 进行扩展，以实现标准 RADIUS 没有定义的功能。

在扩展属性的 RADIUS 报文结构中，Vendor-ID 字段占 4 个字节，代表厂商号，厂商可以封装多个自己定义的 TLV 子属性，从而在应用中得以扩展。


表24-3 H3C RADIUS 扩展属性

子属性编号	子属性名称	描述
1	Input-Peak-Rate	用户接入到NAS的峰值速率，以bps为单位
5	Output-Average-Rate	从NAS到用户的平均速率，以bps为单位
28	Ftp_Directory	FTP用户工作目录
29	Exec_Privilege	EXEC用户优先级
59	NAS_Startup_Timestamp	NAS系统启动时刻，以秒为单位
60	IP_Host_Addr	认证请求和计费请求报文中携带的用户IP地址和MAC地址，格式为“A.B.C.D hh:hh:hh:hh:hh:hh”
61	User_Notify	服务器需要透传到客户端的信息

- 534 -

24.3.5 RADIUS 配置

RADIUS配置



紫光集团 H3C
核心企业 数字化转型方案领导者

- 创建RADIUS方案

```
[sysname] radius scheme radius-scheme-name
```

- 配置RADIUS主认证授权、计费服务器

```
[sysname-radius-name] { primary | secondary } { accounting  
| authentication } ip-address [ port-number ]
```

- 配置RADIUS共享密钥

```
[sysname-radius-name] key { authentication | accounting }  
string
```

www.h3c.com

配置 RADIUS 以方案（scheme）为单位来进行。当创建一个新的 RADIUS 方案后，需要对属于此方案的 RADIUS 服务器的 IP 地址和端口号进行设置，这包括认证/授权服务器和计费服务器。其中每种服务器又有主服务器和从服务器的区别。

RADIUS 方案（scheme）仅定义了设备和服务器之间进行信息交互所必需的一些参数，为了使这些参数能够生效，还必须在某个 ISP 域视图下指定该域应用的 RADIUS 方案，其具体配置请参见 24.2 AAA 架构。

RADIUS 配置步骤如下：

第1步：创建 RADIUS 方案：

```
[sysname] radius scheme radius-scheme-name
```

第2步：配置主、从认证/授权服务器的 IP 地址和端口号：

```
[sysname-radius-name] primary authentication ip-address [port-number]
```

```
[sysname-radius-name] secondary authentication ip-address [port-number]
```

缺省情况下，主、从认证/授权服务的 IP 地址为 0.0.0.0，UDP 端口号为 1812。

第3步：配置主、从计费服务器的 IP 地址和端口号，以及相关参数：

```
[sysname-radius-name] primary accounting ip-address [port-number]
```

```
[sysname-radius-name] secondary accounting ip-address [port-number]
```

缺省情况下，主从计费服务器的 IP 地址为 0.0.0.0，UDP 端口号为 1813。

第4步：配置 RADIUS 报文的共享密钥：

```
[sysname-radius-name] key { accounting | authentication } string
```

注意：


在实际组网中，可以指定两台 RADIUS 服务器分别作为主、从认证授权（计费）服务器；也可以一台服务器既作为主认证授权（计费）服务器，又作为从服务器。

在同一个方案中指定的主认证/授权服务器（计费服务器）和从认证/授权服务器（计费服务器）的 IP 地址不能相同，否则配置不成功。

保证设备上的 RADIUS 服务端口与 RADIUS 服务器上的端口设置一致。

保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致。

RADIUS配置（续）



紫光集团 H3C
核心企业 数字化解决方案领导者

- **配置RADIUS报文重传**

```
[sysname-radius-name] retry times
```

- **配置RADIUS服务定时器**

```
[sysname-radius-name] timer response-timeout seconds
[sysname-radius-name] timer quiet minutes
[sysname-radius-name] timer realtime-accounting minutes
```

www.h3c.com

为防止认证请求报文丢失，交换机会重传一定数量的认证请求报文，其重传次数可配置。

```
[sysname-radius-name] retry times
```

RADIUS 的三个定时器含义如下：

- **服务器响应超时定时器（response-timeout）：**如果在 RADIUS 请求报文传出去一段时间后，设备没有得到服务器的回应，交换机将在 response 定时器超时时重传 RADIUS 请求报文；
- **服务器静默定时器（timer quiet）：**当主服务器不可达时，状态变为 block，设备会与从服务器交互。若从服务器可达，设备与从服务器通信，并开启 quiet 定时器，在设定的时间间隔之后，将服务器的状态恢复为 active；

- **实时计费间隔定时器(realtime-accounting)**: 每隔设定的时间, 交换机会向 RADIUS 服务器发送一次在线用户的计费信息。

24.3.6 RADIUS 调试与维护

RADIUS调试与维护	
操作	命令
显示所有或指定ISP域的配 置信息	display domain [isp-name]
显示AAA用 户连接的相关 信息	display dot1x connection [interface interface- type interface-number slot slot-number user- mac mac-addr user-name name-string]

完成 RADIUS 配置后, 在任意视图下执行 **display** 命令可以显示 AAA、RADIUS 的运行情况, 通过查看显示信息验证配置后的效果。

显示指定的 ISP 域的配置信息:

```
[sysname]display domain system
Domain = system
State = Active
Access-limit = Disabled
Accounting method = Required
Default authentication scheme      : radius=h3c.com
Default authorization scheme      : radius=h3c.com
Default accounting scheme         : radius=h3c.com
Domain User Template:
Idle-cut = Disabled
Self-service = Disabled
```

从以上输出可以得知, 名为 **system** 的 ISP 域引用了 **h3c.com** RADIUS 方案作为缺省的认证、授权、计费方案。

显示 AAA 用户的连接信息:

```
[sysname]display connection

Slot ID: 1
User MAC address: 0050-ba25-cb34
Access interface: GigabitEthernet1/0/1
```

```

Username: test@system
Authentication domain: system
IPv4 address: 30.216.172.102
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33
29 31 33 35 37 40 to 100
Authorization ACL ID: 3001
Authorization user profile: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s
Total 1 connection(s) matched.
    
```

从以上输出信息可以得知，当前设备共有 1 个 AAA 用户在线，接入类型为 dot1x，用户名为 test@system，用户的 IP 地址为 30.216.172.102，MAC 地址为 0050-ba25-cb34。还可以查看到该连接用户的详细信息，如用户接入端口号、授权 VLAN、下发的访问控制列表等。

RADIUS调试与维护（续）		紫光集团 H3C 核心企业 数字化解决方案领导者	
操作	命令		
显示本地用户相关信息	display local-user [class { manage network } idle-cut { disable enable } service-type { ftp http https lan-access portal ssh telnet terminal } state { active block } user-name user-name vlan vlan-id]		
显示所有或指定RADIUS方案的配置信息	display radius scheme [radius-scheme-name]		
显示RADIUS报文的统计信息	display radius statistics		
清除RADIUS协议的统计信息	reset radius statistics		

显示本地用户的详细信息：

```

[sysname]display local-user user-name test class network
Network access user test:
State:                      Active
Service Type:               Lan-access
Access limit: Enabled Max access number: 10
Current access number:      1
User Group:                  system
Bind Attributes:
IP Address:                  2.2.2.2
Location Bound:              GigabitEthernet1/0/1
    
```

```

MAC Address:          0001-0001-0001
VLAN ID:              10
Authorization attributes:
Idle TimeOut:         3 (min)
Work Directory:       flash:
ACL Number:           2000
User profile:         test
User Role List:       network-operator, level-0, level-3

```

从以上信息可以看出,本地用户 **test** 的状态为 **active**,用户使用的服务类型为 **lan-access**,接入用户连接数限制为 **10**,当前接入 **1** 个用户,用户所属 **vlan10**,闲置切断时长为 **3** 分钟。

显示指定 **RADIUS** 方案的配置信息:

```

[sysname]display radius scheme h3c.com
RADIUS Scheme Name : h3c.com
Index : 1
Primary Auth Server:
  Host name: radius.com
  IP : 82.0.0.1                      Port: 1812   State: Active
  VPN : Not configured
Primary Acct Server:
  Host name: radius.com
  IP : 82.0.0.1                      Port: 1813   State: Active
  VPN : Not configured
Second Auth Server:
  Host name: radius.com
  IP : 82.0.0.4                      Port: 1812   State: Active
  VPN : Not configured
Second Acct Server:
  Host name: radius.com
  IP : 82.0.0.4                      Port: 1813   State: Active
  VPN : Not configured
Security Policy Server:
  Server: 0      IP: 82.0.0.1      VPN: Not configured
  Accounting-On function : Disabled
  retransmission times : 50
  retransmission interval(seconds) : 3
  Timeout Interval(seconds) : 3
  Retransmission Times : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes) : 5
  Realtime Accounting Interval(minutes) : 12
  NAS IP Address : Not configured
  VPN : Not configured
  User Name Format : without-domain
  Attribute 15 check-mode : Strict

```

以上信息显示, **RADIUS** 方案 **h3c.com** 的索引号为 **1**,配置了主、从认证授权服务器和主、从计费服务器,状态均为 **active**,安全策略服务器为 **82.0.0.1**,用户名格式为 **without-domain**。

另外,在任意视图下可以使用 **display radius statistics** 命令来查看设备中 **RADIUS** 报文的统计信息,并通过在用户视图下执行 **reset radius statistics** 命令来将统计清零。

24.4 TACACS+协议

24.4.1 TACACS+协议概述

TACACS+协议概述



紫光集团 H3C
核心企业 数字化解决方案领导者

- **TACACS+ (Terminal Access Controller Access Control System Plus, 终端访问控制器控制系统协议)** 是一种增强的安全协议
- **H3C设备实现的HWTACACS是在TACACS+基础上进行了功能增强的安全协议**
- **实现了多种类型用户的AAA功能**
- **与RADIUS协议的区别**

www.h3c.com

TACACS+ (Terminal Access Controller Access Control System Plus), 终端访问控制器控制系统协议) 与 RADIUS 类似, 主要通过客户机/服务器模式与 TACACS+服务器通信来实现多种类型用户的 AAA 功能, 可用于终端用户的认证、授权和计费。

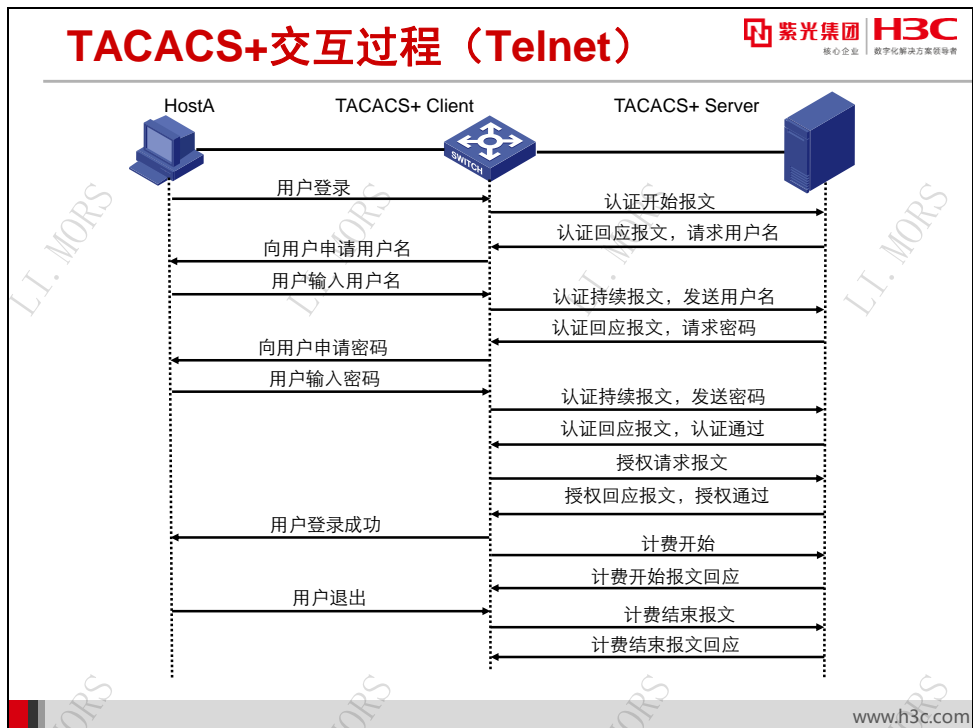
H3C 设备实现的 HWTACACS, 是在 TACACS+基础上进行了功能增强的安全协议。

与 RADIUS 协议相比, TACACS+协议具有更为可靠的传输和加密机制, 更加适合于安全控制。二者的主要区别如表 24-4 所示。

表24-4 RADIUS 协议与 TACACS+协议的比较

RADIUS 协议	TACACS+协议
使用UDP, 网络传输效率更高	使用TCP, 网络传输更可靠
只对验证报文中的密码字段进行加密	除了TACACS+报文头, 对报文主体全部进行加密
协议报文比较简单, 认证和授权结合, 难以分离	协议报文较复杂, 认证和授权分离在不同的安全服务器上实现
不支持对设备的配置命令进行授权使用, 用户登录设备后可以使用的命令行由用户级别决定	支持对设备的配置命令进行授权使用, 用户可使用的命令行受到用户级别和AAA授权的双重限制

24.4.2 TACACS+认证交互流程



Tacacs+认证大多数应用在需要授权功能的场合，如 Telnet 登录管理用户的命令行授权功能。所以在此以 Telnet 用户登录为例，来说明整个认证、授权、计费过程中消息交互流程：

第1步：用户请求登录设备，TACACS+客户端收到请求后，向 TACACS+服务器发送认证开始报文；

第2步：TACACS+服务器发送认证回应报文，请求用户名。TACACS+客户端收到回应报文后，向用户询问用户名；

第3步：TACACS+客户端收到用户名后，向服务器发送持续认证报文，其中包括用户名；

第4步：TACACS+服务器发送认证回应报文，请求登录密码。TACACS+客户端收到回应报文，向用户询问登录密码；

第5步：TACACS+客户端收到登录密码后，向 TACACS+服务器发送持续认证报文，其中包括登录密码；

第6步：TACACS+服务器发送认证回应报文，指示用户通过认证；

第7步：TACACS+客户端向 TACACS+服务器发送授权请求报文；

第8步：TACACS+服务器发送授权回应报文，指示用户通过授权；

第9步：TACACS+客户端收到授权回应成功报文，向用户输出登录设备的配置界面；

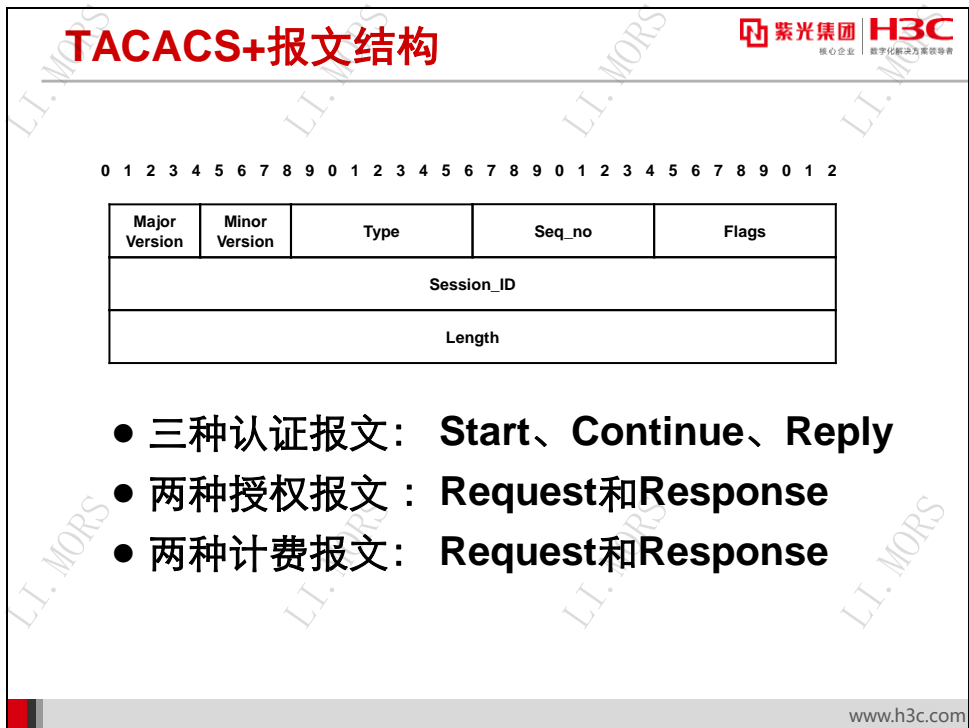
第10步：TACACS+客户端向服务器发送计费开始报文；

第11步： TACACS+服务器发送计费回应报文，指示计费开始报文已经收到；

第12步： 用户退出，TACACS+客户端向 TACACS+服务器发送计费结束报文；

第13步： TACACS+服务器发送计费结束报文，指示计费结束报文已经收到。

24.4.3 TACACS+报文结构




TACACS+报文具有相同的报文头结构，报文在传输过程中不进行加密处理。根据报文头结构中 type 字段的值，分别表示验证、计费、授权报文。各字段解释如下：

- **Major Version:** 主要版本号；
- **Minor Version:** 次要版本号；
- **Type:** 分组类型，0x1 表示认证报文，0x2 表示授权报文，0x3 表示计费报文；
- **Seq_no:** 当前会话的当前分组的序列号。会话中第一个分组序号必须为 1，之后依次递增。NAS 只发送包含奇数序列号的分组，服务器只发送包含偶数序列号的分组；
- **Flags:** 标志位，0x0 表示此报文为加密报文，0x1 表示此报文为非加密报文，0x4 表示一个 TCP 连接上支持多个会话处理；
- **Session_ID:** 会话标识符，表示一次会话业务处理；
- **Length:** 长度字段，表示报文总长度，不包含报文头长度。

TACACS+认证报文分为三种：**Start、Continue、Reply**。**Start** 和 **Continue** 由 NAS 发送，**Reply** 则由 TACACS+服务器发送；授权过程通过授权请求报文(**Request**)和授权响应报文(**Response**)来完成；计费过程与授权过程类似，分为计费请求报文和计费响应报文。

24.4.4 TACACS+配置与维护

TACACS+配置



紫光集团 H3C
核心企业 数字化转型方案领导者

- 创建HWTACACS方案

```
[sysname] hwtacacs scheme hwtacacs-scheme-name
```

- 配置主从认证、授权、计费服务器

```
[sysname-hwtacacs-name] {primary | secondary }  
{ accounting | authentication | authorization } ip-address  
[ port-number ]
```

- 配置报文共享密钥

```
[sysname-hwtacacs-name] key { accounting | authentication  
| authorization } string
```

www.h3c.com

TACACS+的配置是以 TACACS+ 方案为单位进行的。

第1步：在进行其他相关配置前，首先要创建 HWTACACS 方案并进入其视图：

```
[sysname] hwtacacs scheme hwtacacs-scheme-name
```

第2步：配置主认证、授权、计费服务器的 IP 地址和端口号：

```
[sysname-hwtacacs-name] primary authentication ip-address [ port-number ]
```

```
[sysname-hwtacacs-name] primay authorization ip-address [ port-number ]
```

```
[sysname-hwtacacs-name] primary accounting ip-address [ port-number ]
```

缺省情况下，主认证、授权、计费服务的 IP 地址为 0.0.0.0，TCP 端口号为 49。

第3步：配置从认证、授权、计费服务器的 IP 地址和端口号：

```
[sysname-hwtacacs-name] secondary authentication ip-address [ port-number ]
```

```
[sysname-hwtacacs-name] secondary authorization ip-address [ port-number ]
```


```
[sysname-hwtacacs-name] secondary accounting ip-address [ port-number ]
```

缺省情况下，从认证、授权、计费服务器的 IP 地址为 0.0.0.0，TCP 端口号为 49。

第4步：配置共享密钥。交换机与服务器使用 MD5 算法来加密交互的 TACACS+报文，双方通过设置共享密钥来验证报文合法性。只有密钥一致的情况下，双方才能接受对方发来的报文并作出响应。


```
[sysname-hwtacacs-name] key { accounting | authentication | authorization }
string
```

TACACS+配置（续）



- 配置定时器

```
[sysname-hwtacacs-name] timer response-timeout seconds
[sysname-hwtacacs-name] timer quiet minutes
[sysname-hwtacacs-name] timer realtime-accounting minutes
```

- 配置用户名格式

```
[sysname-hwtacacs-name] user-name-format { keep-original
| with-domain | without-domain }
```

www.h3c.com

HWTACACS 与 RADIUS 协议一样，也有相同的定时器，作用与 RADIUS 相似，此处不再赘述。

无论是 RADIUS 认证还是 HWTRACACS 认证，交换机发送给服务器的用户名都有两种格式：带域名或不带域名，即“use@ISP”或“user”两种格式。通过执行以下命令可以切换：

```
[sysname-hwtacacs-name] user-name-format { with-domain / without-domain }
```

TACACS+维护命令		紫光集团 H3C 核心企业 数字化转型领导者
操作	命令	
查看所有或指定 HWTACACS 方案配置信息或统计信息	display hwtacacs [hwtacacs-scheme-name [statistics]]	
清除HWTACACS协议的统计信息	reset hwtacacs statistics { accounting all authentication authorization }	

TACACS+方案配置完成后，可以通过命令查看指定或全部的 TACACS+方案配置信息、统计信息。显示配置的 TACACS+方案信息：

```
[sysname]display hwtacacs test
HWTACACS Scheme Name : test
Index : 1
Primary Auth Server:
  Host name: tacacs.com
  IP : 82.0.0.123      Port: 49      State: Active
  VPN Instance: Not configured
  Single-connection: Disabled
Primary Author Server:
  Host name: tacacs.com
  IP : 82.0.0.123      Port: 49      State: Active
  VPN Instance: Not configured
  Single-connection: Disabled
Primary Acct Server:
  Host name: tacacs.com
  IP : 82.0.0.123      Port: 49      State: Active
  VPN Instance: Not configured
  Single-connection: Disabled
VPN Instance : Not configured
NAS IP Address : Not configured
Server Quiet Period(minutes) : 5
Realtime Accounting Interval(minutes) : 12
Response Timeout Interval(seconds) : 5
Username Format : without-domain
```

从以上输出可以得知，配置了主认证、授权、计费服务器地址为 82.0.0.123，端口号使用缺省 49，从服务器地址为空，用户名不带域。

另外，执行如下命令可以清空 TACACS+的统计：

```
<sysname> reset hwtacacs statistics { accounting | all | authentication |  
authorization }
```

24.5 本章总结

本章总结

- AAA是认证、授权、计费的简称，常使用RADIUS协议和TACACS+协议
- 认证过程分为本地认证和远程认证
- RADIUS基于UDP协议，TLV结构，26号属性用于扩展
- TACACS+基于TCP协议，认证与授权分离

24.6 习题和解答

24.6.1 习题

1. AAA 是____、____、____的缩写，包含了____、____、____三种功能。
2. AAA 可以对如下哪些服务提供安全保证？（ ）
A. FTP B. TELNET C. PPP D. Portal
3. RADIUS 协议基于____传输协议，TACACS+协议基于____传输协议。
A. IP B. TCP C. UDP D. 802.1X
4. RADIUS 协议的认证端口号是____，计费端口号是____。
A. 1645 B. 1812 C. 1646 D. 1813 E. 49
5. NAS 一般指的是（ ）
A. 用户 B. 交换机 C. 认证服务器 D. 计费服务器 E. 授权服务器
6. 对于 AAA 来说，____是客户端，____是服务器端；对于用户来说，____是客户端，____是服务器端。
A. 用户 B. 交换机 C. 认证服务器 D. 计费服务器 E. 授权服务器
7. 如果在 ISP 域上配置了 **authentication radius-scheme radius-scheme-name local**，则针对 local，如下哪些说法正确？（ ）
A. local 表示本地认证
B. 当用户进行远程认证失败时，转为本地认证
C. 当远程服务器不响应时，转为本地认证
D. 本地认证和远程认证同时执行
8. H3C 交换机与 IMC 服务器配合，可完成哪些 AAA 功能？（ ）
A. 记录用户上网时长与流量 B. 服务器将信息透传给用户
C. 下发 EXEC 用户的优先级 D. 下发 FTP 用户的工作目录

24.6.2 习题答案

1. Authentication, Authorization, Accounting, 认证, 授权, 计费
2. ABCD 3. C, B 4. B, D 5. B 6. B, CDE, A, B 7. AC 8. ABCD

第25章 端口接入控制

端口接入控制的主要目的是验证接入用户身份的合法性，以及在认证的基础上对用户的网络接入行为进行授权和计费。目前有多种方式实现端口接入控制。H3C 设备提供的端口接入控制协议主要有 802.1X 认证、MAC 地址认证、端口安全认证，本章将对上述接入控制技术的工作机制和配置进行详细介绍。

25.1 本章目标

课程目标

● 学习完本课程，您应该能够：

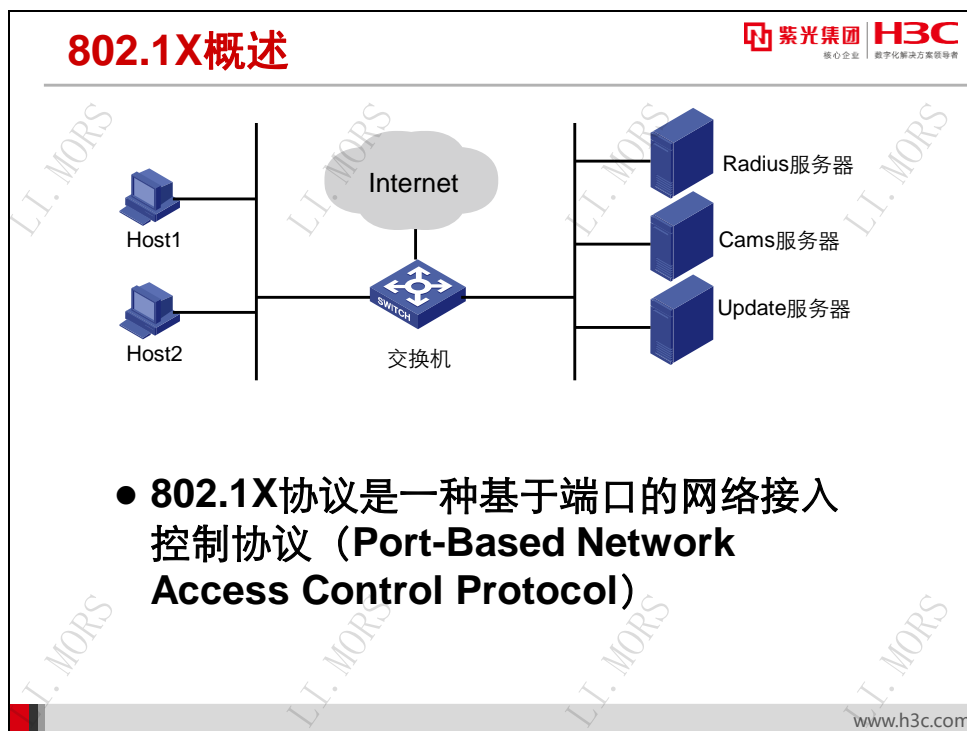
- 掌握802.1X的工作机制和配置
- 掌握MAC地址认证的工作机制和配置
- 掌握端口安全的原理和配置



www.h3c.com

25.2 802.1X协议介绍

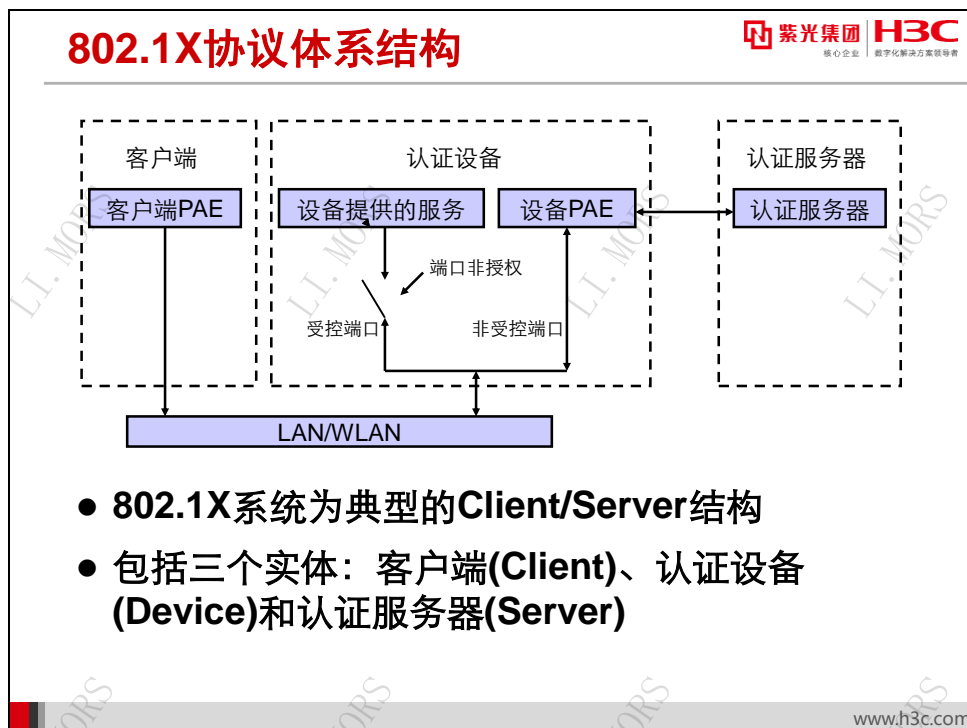
25.2.1 802.1X 概述



2001 年，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，并在 2004 年最终完成了该协议的标准化。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，就可以访问网络中的资源；如果不能通过认证，则无法访问网络中的资源。

25.2.2 802.1X 协议体系结构



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

- **客户端：**是位于局域网链路一端的一个实体，由处于对端的设备端对其进行认证。客户端一般为用户终端设备，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：**是位于局域网链路一端的一个实体，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。

25.2.3 802.1X 基本概念

802.1X基本概念

紫光集团 H3C
核心企业 数字化转型领导者

- **受控/非受控端口：**
 - 受控端口、非受控端口
- **授权/非授权状态：**
 - 强制授权模式、强制非授权模式、自动识别模式
- **受控方向：**
 - 单向受控、双向受控
- **端口接入控制方式：**
 - 基于端口、基于MAC

www.h3c.com

- **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，即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。
- **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。用户可以通过在端口下配置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。

- **受控方向：**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。
- **端口接入控制方式：**包括基于端口/基于 MAC 两种方式。
 - ◆ 当采用基于 MAC 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。
 - ◆ 当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其它接入该端口下的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。

25.2.4 802.1X 认证触发方式和认证方式的分类

802.1X认证触发方式和认证方式的分类

- **802.1X认证触发方式：**
 - 客户端主动触发
 - 设备端主动触发
- **802.1X认证方式：**
 - EAP中继方式（包括EAP-MD5/EAP-TLS/EAP-TTLS/PEAP）
 - EAP终结方式（包括PAP/CHAP）

www.h3c.com

802.1X 的认证触发方式分为两种：客户端主动触发和设备端主动触发。

- **客户端主动触发：**客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文的地址是由 IEEE802.1X 协议分配的一个组播 MAC 地址：01-80-C2-00-00-03。

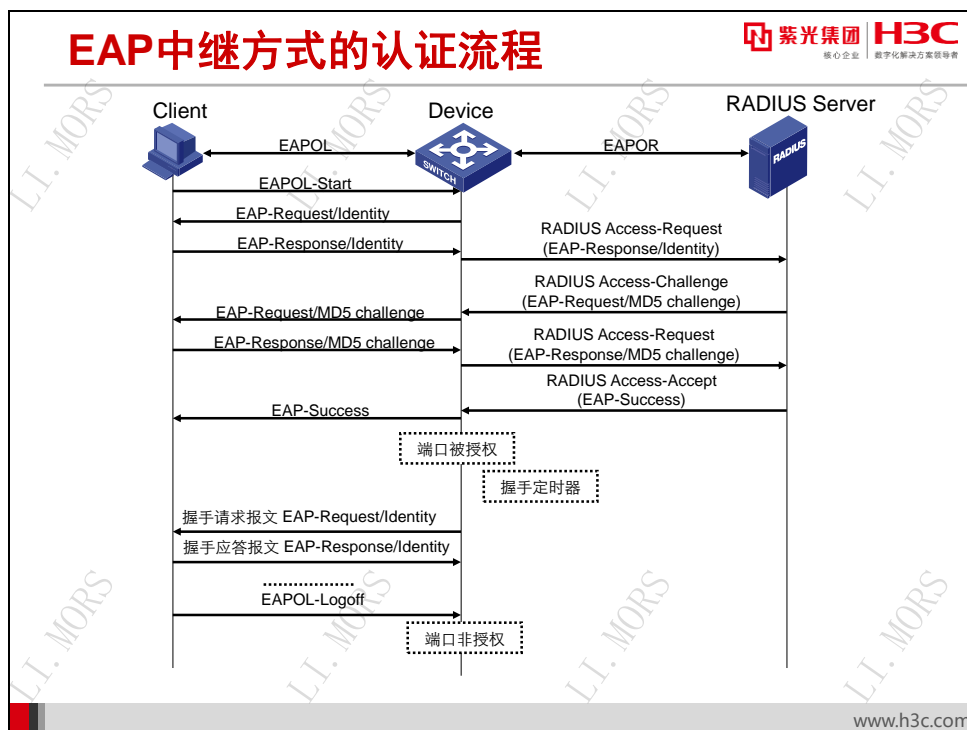
另外，由于网络中可能存在不支持上述的组播报文的设备，从而使得认证设备无法收到客户端的认证请求，因此设备端还支持广播触发方式（即可以接收客户端发送的目的地址为广播 MAC 地址的 EAPOL-Start 报文。这种触发方式需要 H3C iNode 的 802.1X 客户端的配合。）。)

- **设备端主动触发：**设备会以一定的时间间隔（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 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互。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，分为 EAP 中继和 EAP 终结。

- **EAP 中继：**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，包含 MD5、EAP-TLS、EAP-TTLS、PEAP 四种认证方法。
- **EAP 终结：**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 Protocol，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

25.2.5 EAP 中继方式的认证流程



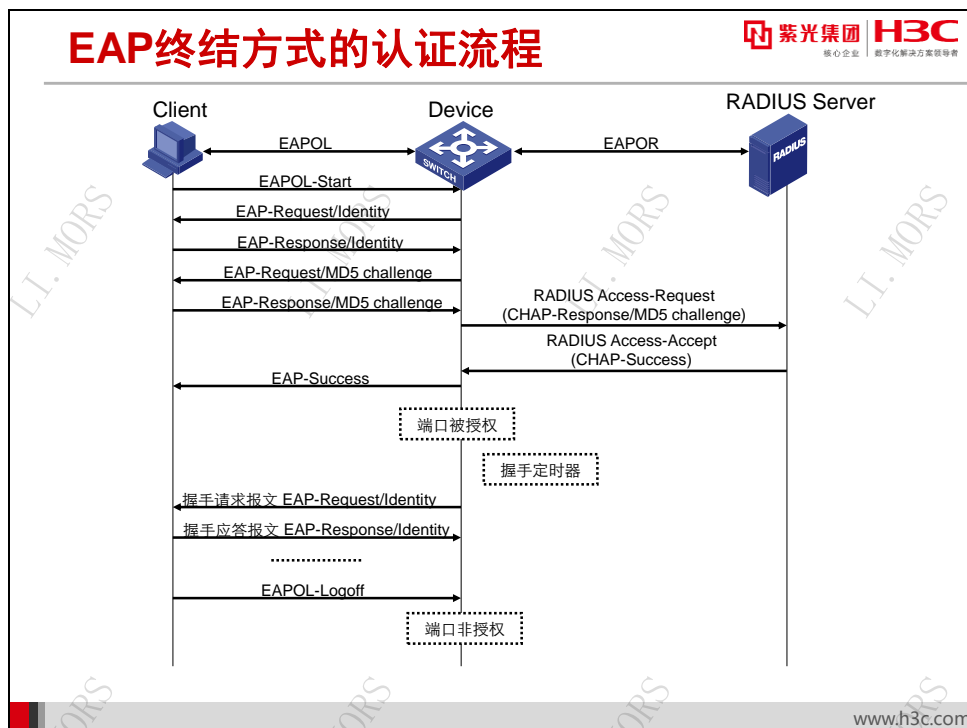
IEEE 802.1X 标准规定的 EAP 中继方式将 EAP（可扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。这里以 EAP-MD5 方式为例介绍基本业务流程，认证过程如下：

- 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，客户端程序将发出请求认证的报文（EAPOL-Start 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，设备端会向客户端定期发送握手报文，以对用户的在线情况进行监测。缺省情况下，如果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。此时设备端会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。

注意：

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，而在设备端，只需要通过 **dot1x authentication-method eap** 命令启动 EAP 中继方式即可。

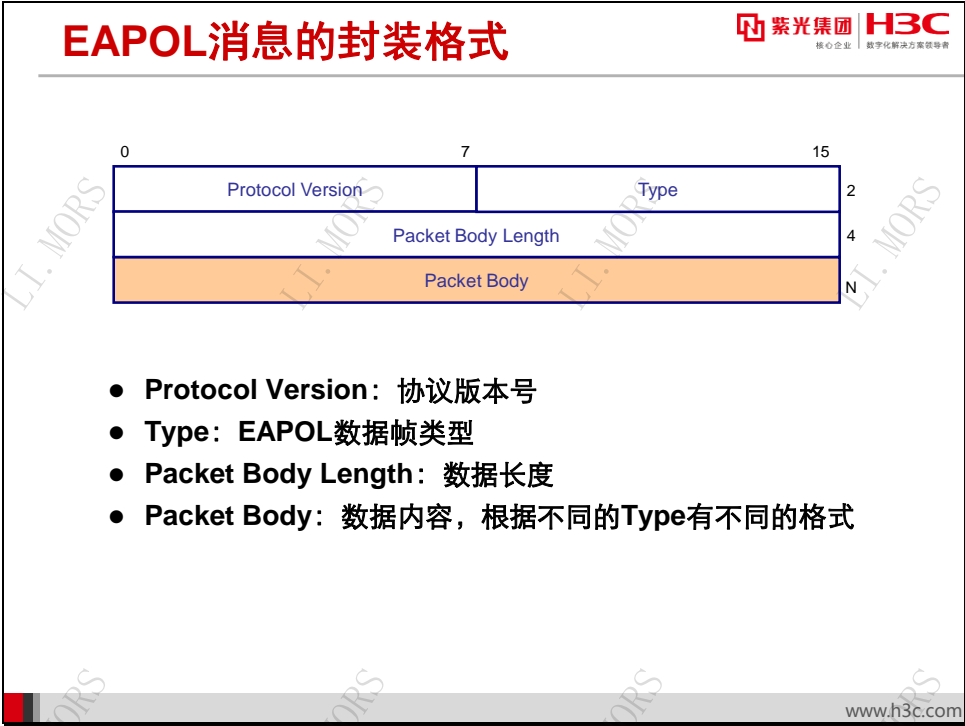
25.2.6 EAP 终结方式的认证流程



EAP 终结方式将 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。这里以 CHAP 认证方法为例介绍基本业务流程，认证过程如上图所示。

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。

25.2.7 EAPOL 消息的封装格式



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 报文, 以允许 EAP 报文在 LAN 上传送。EAPOL 数据包封装时其协议字段为 0x888e。后续各字段含义分别如下:

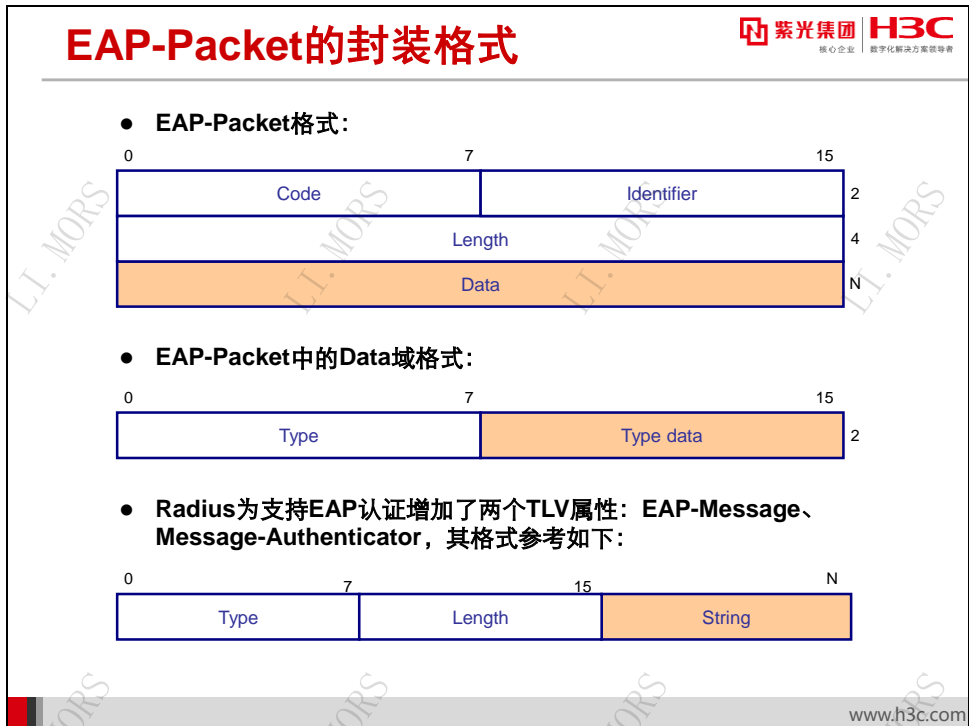
- **Protocol Version**: 表示 EAPOL 帧的发送方所支持的协议版本号。
- **Type**: 表示 EAPOL 数据帧类型, 目前设备上支持的数据类型见下表。

表25-1 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	

- **Packet Body Length**: 表示 Packet Body 域的长度, 单位为字节。如果为 0, 则表示没有 Packet Body。如 EAPOL-Start 和 EAPOL-Logoff 就没有 Packet Body。
- **Packet Body**: 表示数据内容, 根据不同的 Type 有不同的格式。

25.2.8 EAP-Packet 的封装格式



当 EAPOL 数据包 Type 域为 EAP-Packet 时, Packet Body 将按照 CLV 格式进行封装。

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

当 Code 类型为 Success 和 Failure 时, 数据包没有 Data 域, 相应的 Length 域的值 4。

当 Code 类型为 Request 和 Response 时, 数据包的 Data 域的格式如图所示。Type 为 Request 或 Response 类型, Type data 的内容由 Type 决定。例如, Type 值为 1 时代表 Identity, 用来查询对方的身份; Type 值为 2 时, 代表 Notification, 用于传递提示消息给客户端; Type 值为 4 时, 代表 MD5-Challenge, 类似于 PPP CHAP 协议, 包含质询消息。

RADIUS 协议为了支持 EAP 认证也增加了两个 TLV 属性: EAP-Message (EAP 消息) 和 Message-Authenticator (消息认证码)。

- **EAP-Message:** 该属性用来封装 EAP 消息, 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。

- **Message-Authenticator:** 该属性用来避免接入请求包被窃听，类型代码为 80。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。

25.2.9 802.1X、PPPOE 认证和 WEB 认证的对比

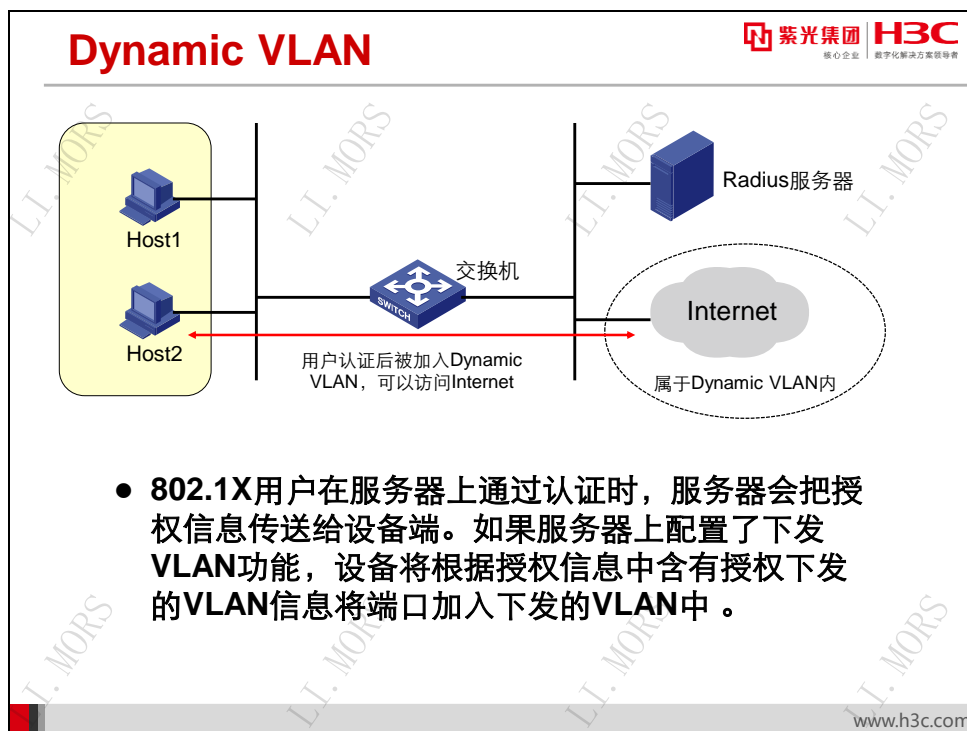
802.1X和PPPOE认证、WEB认证的对比			
	802.1X	PPPOE	WEB认证
是否需要配置客户端软件	是(Windows系统有自带客户端)	是(Windows系统有自带客户端)	否
业务报文效率	高	低，有封装开销	高
组播支持能力	好	低，对设备要求高	好
有线网上的安全性	扩展后可用	可用	可用
设备端的要求	低	高	较高
增值应用支持	简单	复杂	复杂

● **802.1X**适用于运营管理相对简单、业务复杂度较低的企业以及园区，**802.1X**是理想的低成本运营解决方案。

从上表中可以看出，相对于 PPPoE 和 WEB 认证，802.1X 的优势较为明显，是理想的低成本运营解决方案。802.1X 适用于接入设备与接入端口间点到点的连接方式，实现对局域网用户接入的认证与服务管理，常用于运营管理相对简单，业务复杂度较低的企业以及园区。

25.3 802.1X扩展应用

25.3.1 Dynamic VLAN

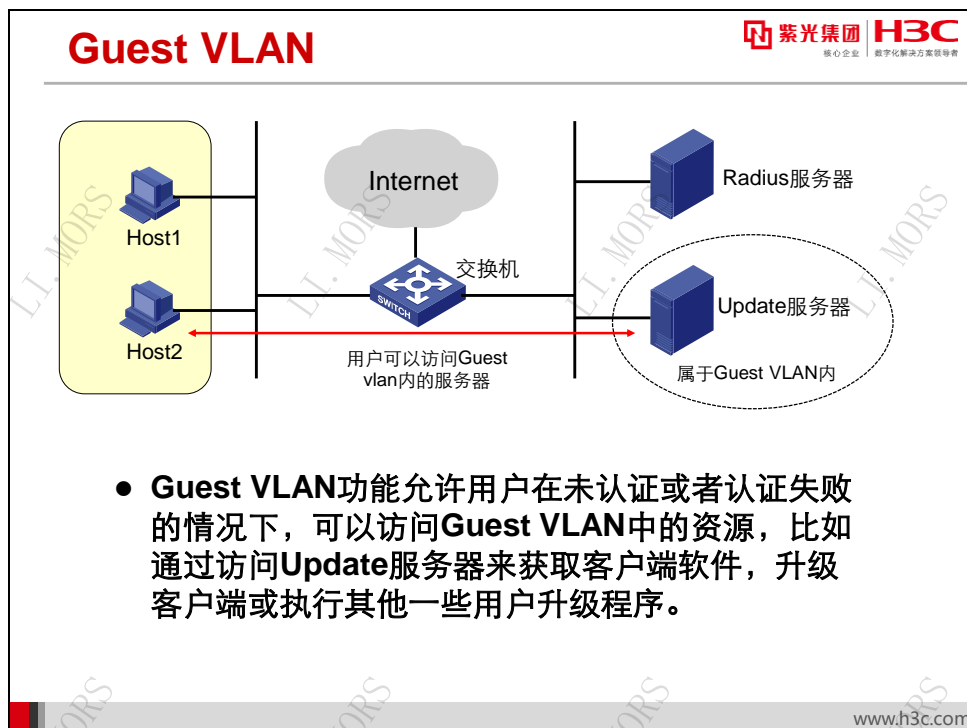


802.1X 用户在服务器上通过认证时，服务器会把授权信息传送给设备端。如果服务器上配置了下发 VLAN 功能，在授权信息中则会包含授权下发的 VLAN 信息，设备根据用户认证上线的端口链路类型，按以下三种情况将端口加入下发 VLAN 中：

- 若端口的链路类型为 Access，当前 Access 端口离开用户配置的 VLAN 并加入授权下发的 VLAN 中。
- 若端口的链路类型为 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。
- 若端口的链路类型为 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。

25.3.2 Guest VLAN



Guest VLAN 功能允许用户在未认证或者认证失败的情况下，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 通常被称为 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。

- **PGV (Port-based Guest VLAN, 基于端口的 Guest VLAN):** 在接入控制方式被配置为 portbased 的端口上启用的 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。

- **MGV (MAC-based Guest VLAN, 基于 MAC 的 Guest VLAN):** 在接入控制方式配置为 `macbased` 的端口上启用的 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。


MGV 需要与基于 MAC 的 VLAN 配合使用，端口配置 MGV 的同时，需要使能 `mac-vlan`。设备会动态地创建基于用户 MAC 的 VLAN 表项，以将未认证或认证失败的用户加入到 Guest VLAN 中。

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。

25.4 802.1X配置和维护

25.4.1 802.1X 基本配置命令

802.1X基本配置命令



- 开启全局的802.1X特性

```
[sysname] dot1x
```
- 开启端口的802.1X特性

```
[sysname-interface-name] dot1x
```
- 设置802.1X用户的认证方法

```
[sysname] dot1x authentication-method { chap | eap | pap }
```
- 设置端口接入控制方式

```
[sysname-interface-name] dot1x port-method { macbased | portbased }
```

www.h3c.com

接入设备的管理者通常会选择使用 RADIUS 或本地认证方法，来配合 802.1X 完成用户的身份认证。因此，在配置 802.1X 时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。

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，配置 802.1X 的基本步骤如下：

第1步： 开启全局的 802.1X 特性

```
[sysname] dot1x
```

第2步： 开启端口的 802.1X 特性

```
[sysname-interface-name] dot1x
```

第3步： 设置 802.1X 用户认证方法

```
[sysname] dot1x authentication-method { chap | eap | pap }
```

缺省情况下，802.1X 用户认证方法为 CHAP 认证，用户可以根据需要设置其认证方法。


第4步：设置端口接入控制方式

```
[sysname] dot1x port-method { macbased | portbased } [ interface interface-list ]
```

缺省情况下，接入控制方式为 macbased。

25.4.2 802.1X 的定时器及配置

802.1X的定时器及配置



紫光集团 H3C
核心企业 数字化解决方案领导者

- 定时器配置:

```
[sysname] dot1x timer { ead-timeout ead-timeout-value | handshake-period handshake-period-value | quiet-period quiet-period-value | reauth-period reauth-period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-value | tx-period tx-period-value }
```

- EAD超时定时器（ead-timeout）——默认30分钟
- 用户名请求超时定时器（tx-period）——默认30秒
- 客户端认证超时定时器（supp-timeout）——默认30秒
- 周期性重认证定时器（reauth-period）——默认3600秒
- 认证服务器超时定时器（server-timeout）——默认100秒
- 握手定时器（handshake-period）——默认15秒
- 静默定时器（quiet-period）——默认60秒
- 开启静默定时器功能:

```
[sysname] dot1x quiet-period
```

- 开启在线用户握手功能:

```
[sysname-GigabitEthernet1/0/1] dot1x handshake
```

www.h3c.com

在 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）：**该定时器包含两种含义。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，设备端会启动此定时器，若在该定时器超时前，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, 设备端会启动 server-timeout 定时器, 若在该定时器超时前, 设备端没有收到认证服务器的响应, 设备将认为认证失败, 启动下一次认证。
- **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。如果设备在指定时间内都没有收到客户端的响应报文时, 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。

配置各个定时器参数的命令如下:

```
[sysname]dot1x timer {ead-timeout ead-timeout-value | handshake-period  
handshake-period-value | quiet-period quiet-period-value | reauth-period reauth-  
period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-  
value | tx-period tx-period-value }
```

缺省情况下, 静默功能处于关闭状态。如果需要防止用户频繁触发认证, 请使用如下命令行开启静默功能:

```
[sysname] dot1x quiet-period
```

另外, 用户可以根据需要, 开启或关闭在线用户握手功能, 在开启在线握手功能后, 设备才会按照 handshake-period 定时器间隔周期发送握手请求报文, 命令行如下:

```
[sysname-GigabitEthernet1/0/1] dot1x handshake
```

25.4.3 配置 Guest VLAN 和 VLAN 下发

配置 Guest VLAN 和 VLAN 下发

 紫光集团 **H3C**
核心企业 数字化解决方案领导者

- 配置指定端口的 Guest VLAN：

```
[sysname-interface-name] dot1x guest-vlan vlan-id
```

- 通过远程服务器下发数字型 VLAN 时，设备不需要创建 VLAN
- 通过远程服务器下发字符型 VLAN 时，设备上需要创建所下发的 VLAN，并配置该 VLAN 的 name，比如：

```
[sysname] vlan 10
[sysname -vlan10] name test
```

- 对于本地用户，下发 VLAN 需要配置如下属性：

```
[sysname] local-user user-name
[sysname -luser- user-name] authorization-attribute vlan vlan-id
```

www.h3c.com

可以在以太网端口视图下配置 Guest VLAN，命令如下：

```
[sysname-GigabitEthernet1/0/1] dot1x guest-vlan vlan-id
```

若通过远程 Radius 服务器下发数字型 VLAN，在设备上不需要创建该 VLAN，用户认证成功根据服务器下发的 VLAN 信息，设备会自动创建该 VLAN。

若通过远程 Radius 服务器下发字符型 VLAN，在设备上需要先创建所下发的 VLAN，并配置该 VLAN 的 name，该 name 要与服务器上设置的一致。比如：

```
[H3C] vlan 10
```

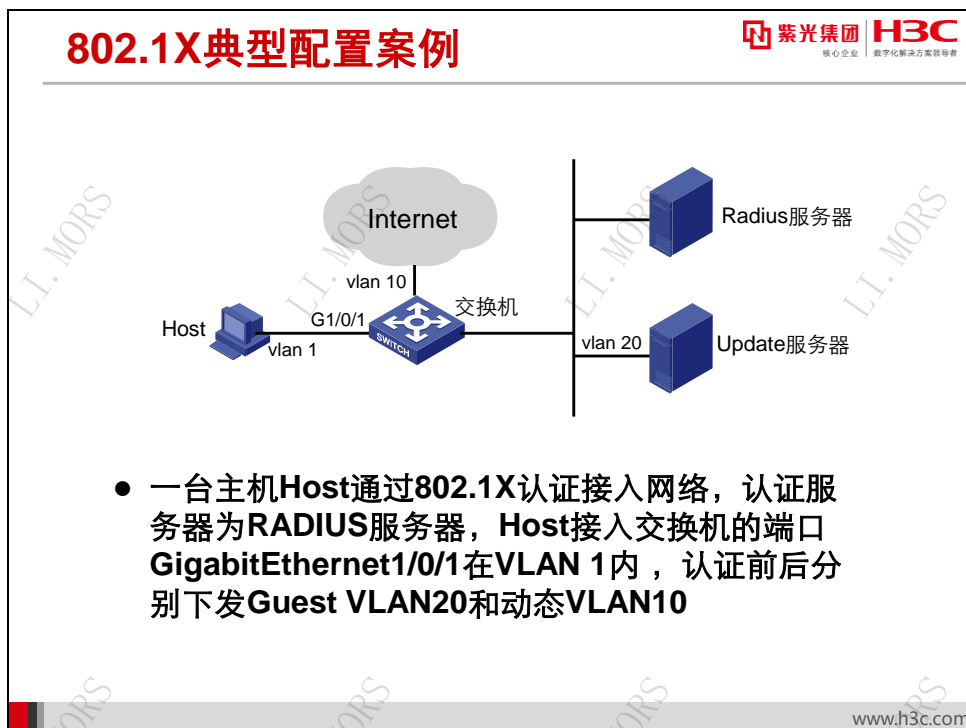
```
[H3C-vlan10] name test
```

若采用本地用户进行认证，下发 VLAN 需要配置如下属性：

```
[H3C] local-user user-name
```

```
[H3C-luser-user-name] authorization-attribute vlan vlan-id
```

25.4.4 802.1X 典型配置案例



组网需求：

- 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 通过交换机的端口 GigabitEthernet1/0/1（该端口在 VLAN 1 内）；Update Server 是用于客户端软件下载和升级的服务器，在 VLAN 20 内；交换机连接 Internet 网络的端口在 VLAN 10 内。
- 在 GigabitEthernet1/0/1 上开启 802.1X 特性并设置 VLAN 20 为的 Guest VLAN，当设备从端口发送触发认证报文（EAP-Request/Identity）超过设定的最大次数而没有收到任何回应报文后，GigabitEthernet1/0/1 被加入 Guest VLAN 中，此时 Host 和 Update Server 都在 VLAN 20 内，Host 可以访问 Update Server 并下载 802.1X 客户端。
- 当用户认证成功上线，认证服务器下发 VLAN 10。此时 Host 和连接 Internet 网络的端口都在 VLAN 10 内，Host 可以访问 Internet。

配置步骤：

配置 RADIUS 方案 h3c

```
<sysname> system-view
[sysname] radius scheme h3c
[sysname-radius-h3c] primary authentication 82.0.0.3 1812
[sysname-radius-h3c] primary accounting 82.0.0.3 1813
[sysname-radius-h3c] key authentication h3c
[sysname-radius-h3c] key accounting h3c
[sysname-radius-h3c] quit
```

配置认证域 h3c，该域使用已配置的 RADIUS 方案 h3c


```
[sysname]domain h3c
[sysname-isp-h3c] authentication default radius-scheme h3c
[sysname-isp-h3c] authorization default radius-scheme h3c
[sysname-isp-h3c] accounting default radius-scheme h3c
[sysname-isp-h3c] quit
```

开启全局 802.1X 特性

```
[sysname] dot1x
```

开启指定端口的 802.1X 特性

```
[sysname]interface GigabitEthernet 1/0/1
[sysname-GigabitEthernet 1/0/1]dot1x
```

配置端口上进行接入控制的方式为 portbased

```
[sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

创建 VLAN 20

```
[sysname] vlan 20
[sysname-vlan20] quit
```

配置指定端口的 Guest VLAN

```
[sysname]interface GigabitEthernet 1/0/1
[sysname- GigabitEthernet 1/0/1] dot1x guest-vlan 20
```


完成上述配置之后触发认证之前，通过命令 **display current-configuration** 或者 **display interface gigabitethernet 1/0/1** 可以查看 Guest VLAN 的配置情况。

在端口 UP 且没有用户主动上线情况下，设备将发送认证请求（EAP-Request/Identity）报文，发送超过设定的最大次数后仍未由用户响应请求，则将该端口自动加入 Guest VLAN。通过命令 **display vlan 20** 可以查看端口配置的 Guest VLAN 是否生效。

在用户认证成功之后，通过 **display interface gigabitethernet 1/0/1** 可以看到用户接入的端口 GigabitEthernet1/0/1 加入了认证服务器下发的授权 VLAN 10 中。

25.4.5 802.1X 显示和维护

802.1X显示和维护

 紫光集团 **H3C**
核心企业 | 数字化解决方案领导者

- 显示802.1X的会话连接信息、相关统计信息或配置信息

`[sysname] display dot1x [sessions | statistics] [interface interface-list]`
- 清除802.1X的统计信息

`<sysname>reset dot1x statistics [interface interface-list]`
- 显示802.1X认证用户的连接信息

`<sysname>display dot1x connection { interface interface-list | slot slot-number | user-mac H-H-H | user-name user-name }`

www.h3c.com

在维护 and 配置过程中，可以通过如下命令来快速 802.1X 用户的会话连接信息、相关统计信息或配置信息：

```
[sysname] display dot1x [sessions | statistics ] [ interface interface-list ]
```

802.1X 用户的相关统计信息还可以通过如下命令清除以便在维护过程中排除历史信息的干扰：

```
<sysname> reset dot1x statistics [ interface interface-list ]
```

当需要确切掌握某个认证用户的更具体信息时，可以使用如下命令查看认证用户详细信息。

```
[sysname] display dot1x [ sessions | statistics ] [ interface interface-list ]
```

25.5 MAC地址认证

25.5.1 MAC 地址认证概述

MAC地址认证概述



紫光集团 H3C
核心企业 数字化解决方案领导者

- **MAC地址认证**是一种基于端口和**MAC地址**对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件，也不需要用户手动输入用户名或者密码。
- **MAC地址认证方式：**
 - 远程RADIUS认证
 - 本地认证
- **MAC地址认证用户名类型：**
 - MAC地址用户名
 - 固定用户名

www.h3c.com

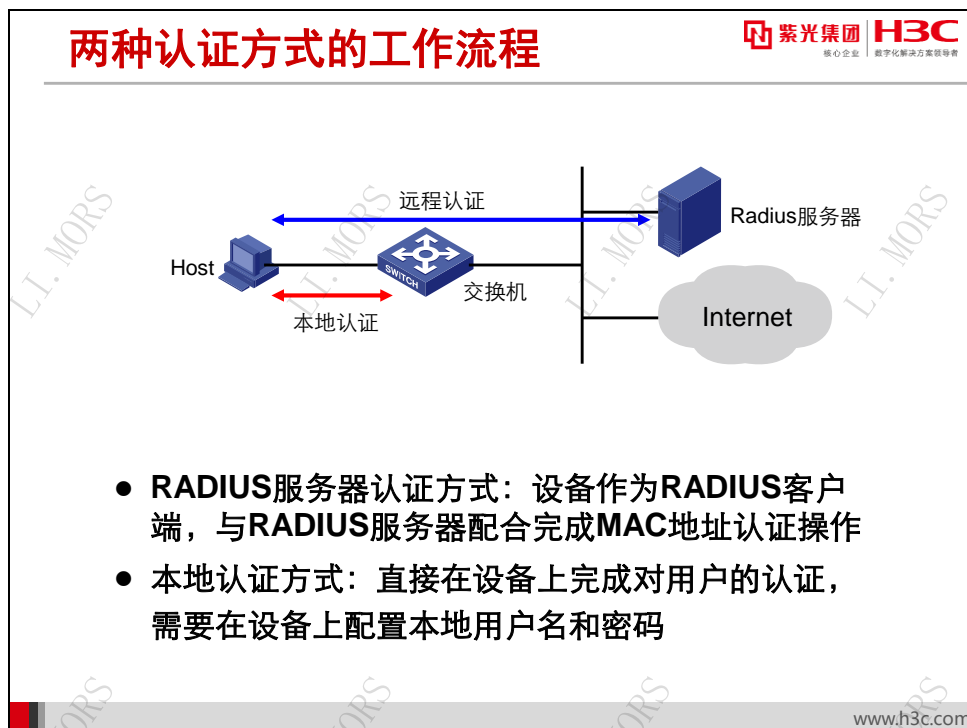
MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，也不需要用户手动输入用户名或者密码。

目前设备支持两种方式的 MAC 地址认证：通过 RADIUS 服务器认证和本地认证。

MAC 地址认证用户名分为两种类型：MAC 地址用户名和固定用户名。

- **MAC 地址用户名：**使用用户的 MAC 地址作为认证时的用户名和密码。
- **固定用户名：**不论用户的 MAC 地址为何值，所有用户均使用在设备上预先配置的用户名和密码进行认证。同一个端口下可以有多个用户进行认证，且均使用同一个固定用户名通过认证。

25.5.2 两种认证方式的工作流程



当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作：

- 采用 MAC 地址用户名时，设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器。
- 采用固定用户名时，设备将已经在本地配置的用户名和密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器。

当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码：

- 采用 MAC 地址用户名时，需要配置的本地用户名为各接入用户的 MAC 地址。
- 采用固定用户名时，需要配置的本地用户名为自定义的，所有用户对应的用户名和密码与自定义的一致。

25.5.3 MAC 地址认证的配置命令

MAC地址认证的配置命令

紫光集团
核心企业 | 数字化解决方案领导者

- 启动全局的MAC地址认证

`[sysname] mac-authentication`
- 启动端口的MAC地址认证

`[sysname-interface-name] mac-authentication`
- 配置MAC地址认证的用户名与密码

`[sysname] mac-authentication user-name-format { fixed [account name] [password { cipher | simple } password] | mac-address [{ with-hyphen | without-hyphen } [lowercase | uppercase]] }`
- 配置MAC认证用户使用的认证域

`[sysname] mac-authentication domain domain-name`

www.h3c.com

通过使用 MAC 地址认证，可以对用户的网络访问权限进行控制，在配置 MAC 地址认证之前，需要首先完成以下配置任务：

- 创建并配置 ISP 域。
- 若采用本地认证方式，需建立本地用户并设置其密码。
- 若采用远程 RADIUS 认证方式，需要确保设备与 RADIUS 服务器之间的路由可达，并添加用户名及密码。

在全局 MAC 地址认证没有开启之前端口可以启动 MAC 地址认证，但不起作用；只有在全局 MAC 地址认证启动后，各端口的 MAC 地址认证配置才会立即生效。MAC 地址认证基本步骤如下：

第1步： 启动全局的 MAC 地址认证

```
[sysname] mac-authentication
```

第2步： 启动端口的 MAC 地址认证

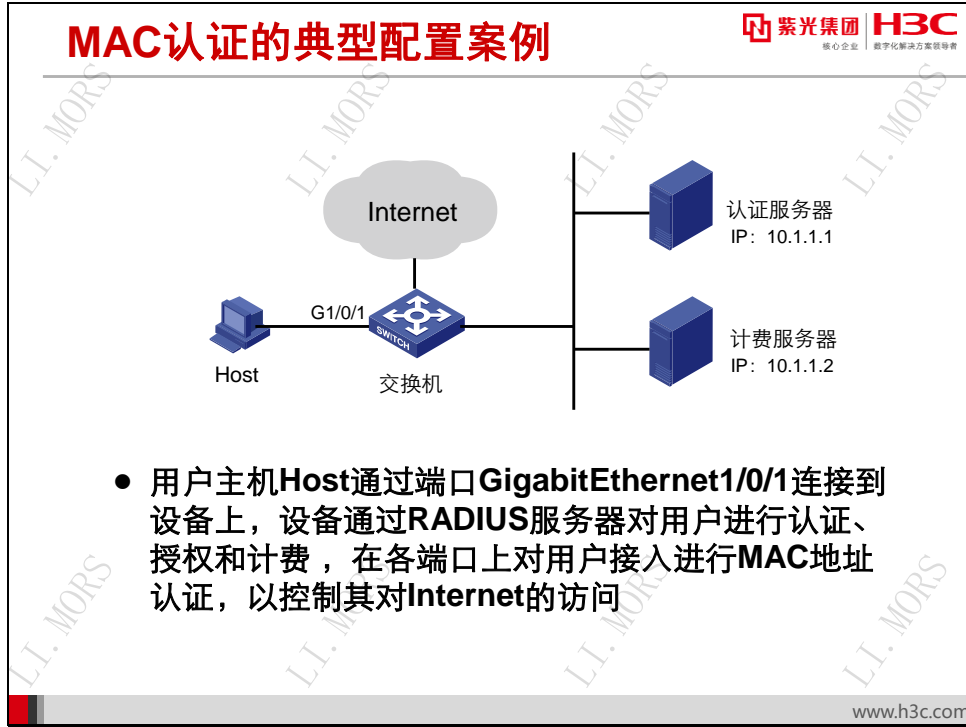
```
[sysname-interface-name] mac-authentication
```

第3步： 配置 MAC 地址认证的用户名与密码

```
[sysname] mac-authentication user-name-format { fixed [ account name ]
[ password { cipher | simple } password ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }
```

第4步：配置 MAC 认证用户使用的认证域

[sysname] **mac-authentication domain** domain-name

25.5.4 MAC 认证的典型配置案例**组网需求：**

用户主机 Host 通过端口 GigabitEthernet1/0/1 连接到设备上，设备通过 RADIUS 服务器对用户进行认证、授权和计费。

- 设备的管理者希望在各端口上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。
- 所有用户都属于域 h3c，认证时采用固定用户名格式，用户名为 aaa，密码为 123456。

配置步骤：**# 配置 RADIUS 方案 h3c**

```
<sysname> system-view
[sysname] radius scheme h3c
[sysname-radius-h3c] primary authentication 10.1.1.1 1812
[sysname-radius-h3c] primary accounting 10.1.1.2 1813
[sysname-radius-h3c] key authentication simple h3c
[sysname-radius-h3c] key accounting simple h3c
[sysname-radius-h3c] user-name-format without-domain
[sysname-radius-h3c] quit
```

#配置 ISP 域的 AAA 方案

```
[sysname]domain h3c
[sysname-isp-h3c] authentication default radius-scheme h3c
[sysname-isp-h3c] authorization default radius-scheme h3c
[sysname-isp-h3c] accounting default radius-scheme h3c
[sysname-isp-h3c] quit
```

#开启全局 MAC 地址认证特性

```
[sysname] mac-authentication
```

#开启指定端口的 MAC 地址认证特性

```
[sysname]interface GigabitEthernet 1/0/1
[sysname-GigabitEthernet 1/0/1]mac-authentication
```

#配置 MAC 地址认证用户所使用的 ISP 域

```
[sysname] mac-authentication domain h3c
```

#配置 MAC 地址认证的定时器

```
[sysname] mac-authentication timer offline-detect 180
[sysname] mac-authentication timer quiet 180
```

#配置 MAC 地址认证使用固定用户名格式：用户名为 aaa，密码为 123456

```
[sysname] mac-authentication user-name-format fixed account aaa password
simple 123456
```


完成上述配置之后，连接认证用户到端口后将触发 MAC 认证，通过命令 **display mac-authentication** 或者 **display mac-authentication connection** 验证配置结果，并可以查看当前 MAC 认证通过的用户。如下所示显示全局 MAC 地址认证信息：

```
[sysname]display mac-authentication
Global MAC authentication parameters:
  MAC authentication      : Enabled
  User name format       : MAC address in lowercase(xxxxxxxxxxxx)
  Username               : mac
  Password               : Not configured
  Offline detect period  : 300 s
  Quiet period           : 60 s
  Server timeout         : 100 s
  Authentication domain  : Not configured, use default domain
  Max MAC-auth users     : 2048 per slot
  Online MAC-auth users  : 1
Silent MAC users:
  MAC address    VLAN ID  From port    Port index
GigabitEthernet1/0/1 is link-up
  MAC authentication      : Enabled
  Authentication domain   : Not configured
  Auth-delay timer       : Disabled
  Re-auth server-unreachable : Logoff
  Guest VLAN             : Not configured
  Critical VLAN          : Not configured
  Host mode              : Single VLAN
  Max online users       : 2048
  Authentication attempts : successful 1, failed 0
  Current online users   : 1
  MAC address    Auth state
00e0-fc12-3456  MAC_AUTHENTICATOR_SUCCESS
```

从如上信息可以发现（MAC 为 00e0-fc12-3456）用户认证成功。

25.5.5 MAC 地址认证的显示和维护

MAC地址认证的显示和维护

 紫光集团 H3C
核心企业 数字化转型方案领导者

- 显示所有或指定端口的MAC认证用户信息
`<sysname>display mac-authentication [interface interface-list]`
- 清除MAC地址认证的统计信息
`<sysname>reset mac-authentication statistics [interface interface-list]`
- 显示MAC认证用户的详细信息
`<sysname>display mac-authentication connection [interface interface-type interface-number | slot slot-number | user-mac mac-addr | user-name user-name]`


www.h3c.com

MAC 认证的维护命令和 802.1X 认证的维护命令基本相同，可以快捷现实全局或指定端口的 MAC 认证用户简要统计信息，同时也提供了相应的统计信息清除命令。当需要查看某个 MAC 认证用户的详细信息时，则需要采用 `display mac-authentication connection` 命令显示。

25.6 端口安全

25.6.1 端口安全概述

端口安全概述



核心企业 | 数字化解决方案领导者

- **端口安全：**
 - 端口安全（Port Security）是一种基于MAC地址对网络接入进行控制的安全机制，是对已有的802.1X认证和MAC地址认证的扩充
- **端口安全模式：**
 - 端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源MAC地址，以达到相应的网络管理效果
- **端口安全的特性：**
 - NeedToKnow特性
 - 入侵检测（IntrusionProtection）特性

www.h3c.com

端口安全（Port Security）是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。

端口安全的特性有 NeedToKnow 特性、入侵检测（IntrusionProtection）特性和 Trap 特性。

- **NeedToKnow 特性：**通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证的设备上，从而防止非法设备窃听网络数据。
- **入侵检测（IntrusionProtection）特性：**指通过检测从端口收到的数据帧的源 MAC 地址，对接收非法报文的端口采取相应的安全策略，包括端口被暂时断开连接、永久断开连接或 MAC 地址被过滤（默认 3 分钟，不可配置），以保证端口的安全性。

25.6.2 端口安全的模式

端口安全模式



紫光集团 H3C
核心企业 数字化转型领导者

- **MAC地址学习类型：**
 - noRestrictions、autolearn、secure
- **802.1X认证类型：**
 - userLogin、userLoginSecure、userLoginSecureExt、userLoginWithOUI
- **MAC地址认证及与802.1X认证组合类型：**
 - macAddressWithRadius、macAddressOrUserLoginSecure、macAddressOrUserLoginSecureExt、macAddressElseUserLoginSecure、macAddressElseUserLoginSecureExt



www.h3c.com

根据用户认证上线方式的不同，可以将端口安全模式划分为三类：**MAC 地址学习类型、802.1X 认证类型、MAC 地址认证及与 802.1X 认证组合类型**。对端口安全模式的具体描述请参见下表。


表25-2 端口安全模式

安全模式类型	描述	特性说明
noRestrictions	表示端口的安全功能关闭，端口处于无限制状态	此时NeedToKnow特性和入侵检测特性无效
autoLearn	此模式下，端口通过配置或学习到的安全MAC地址被保存在安全MAC地址表项中；当端口下的安全MAC地址数超过端口允许学习的最大安全MAC地址数后，端口模式会自动转变为secure模式。之后，该端口停止添加新的安全MAC，只有源MAC地址为安全MAC地址、已配置的静态MAC地址的报文，才能通过该端口	在这两种模式下，当设备发现非法报文后，将触发NeedToKnow特性和入侵检测特性；autoLearn模式下，禁止
secure	禁止端口学习MAC地址，只有源MAC地址为端口上的安全MAC地址、已配置的静态MAC地址的报文，才能通过该端口	学习动态MAC地址

安全模式类型	描述	特性说明
userLogin	对接入用户采用基于端口的802.1X认证；此模式下，端口下一旦有用户通过认证，其他用户也可以访问网络；	此模式下NeedToKnow特性和入侵检测特性不会被触发
userLoginSecure	对接入用户采取基于MAC的802.1X认证；此模式下，端口最多只允许一个802.1X认证用户接入；	在左侧列出的模式下，当设备发现非法报文后，将触发NeedToKnow特性和入侵检测特性
userLoginSecureExt	对接入用户采用基于MAC的802.1X认证；但此模式下允许端口下有多个802.1X认证用户	
userLoginWithOUI	与userLoginSecure模式类似，端口最多只允许一个802.1X认证用户接入；与此同时端口还允许源MAC地址为指定OUI的报文通过	
macAddressWithRadius	对接入用户采用MAC地址认证	
macAddressOrUserLoginSecure	端口同时处于userLoginSecure模式和macAddressWithRadius模式，但802.1X认证优先级大于MAC地址认证；对于非802.1X报文直接进行MAC地址认证。对于802.1X报文直接进行802.1X认证	
macAddressOrUserLoginSecureExt	与macAddressOrUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	
macAddressElseUserLoginSecure	端口同时处于macAddressWithRadius模式和userLoginSecure模式，但MAC地址认证优先级大于802.1X认证；对于非802.1X报文直接进行MAC地址认证。对于802.1X报文先进行MAC地址认证，如果MAC地址认证失败进行802.1X认证	
macAddressElseUserLoginSecureExt	与macAddressElseUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	

25.6.3 端口安全的配置命令

端口安全的配置命令



- 使能端口安全功能

[sysname] port-security enable

- 配置端口允许的最大安全MAC地址数

[sysname-GigabitEthernet1/0/1] port-security max-mac-count count-value

- 配置端口的安全模式

[sysname-GigabitEthernet1/0/1] port-security port-mode { autolearn / mac-authentication / mac-else-userlogin-secure / mac-else-userlogin-secure-ext / secure / userlogin / userlogin-secure / userlogin-secure-ext / userlogin-secure-or-mac / userlogin-secure-or-mac-ext / userlogin-withoui }

www.h3c.com

在端口安全功能未使能的情况下，端口安全模式可以进行配置但不会生效；在端口上有用户在线的情况下，端口安全模式无法改变。端口安全具体配置步骤如下：

第1步：使能端口安全功能，在使能端口安全功能之前，需要关闭全局的 802.1X 和 MAC 地址认证功能。

[sysname] port-security enable

第2步：配置端口允许的最大安全 MAC 地址数，端口安全允许某个端口下有多个用户通过认证，但是允许的用户数不能超过规定的最大值。配置端口允许的最大安全 MAC 地址数有两个作用：一是控制能够通过某端口接入网络的最大用户数，二是控制端口安全能够添加的安全 MAC 地址数。

[sysname-GigabitEthernet1/0/1] port-security max-mac-count count-value

第3步：配置端口安全模式，在配置端口安全模式之前，端口上需要满足以下条件：


- 802.1X 认证关闭、端口接入控制方式为 macbased、端口接入控制模式为 auto。
- MAC 地址认证关闭。
- 端口未加入聚合组或业务环回组。

（否则以上各条件若不满足，系统会提示错误信息，无法进行配置。反之，若端口上配置了端口安全模式，以上配置也不允许改变。）

- 对于 autoLearn 模式，还需要提前设置端口允许的最大安全 MAC 地址数。

```
[sysname-GigabitEthernet1/0/1] port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext | userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }
```

端口安全的配置命令（续）



紫光集团 H3C
核心企业 数字化转型领导者

- 配置端口NeedToKnow特性

```
[sysname-GigabitEthernet1/0/1] port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }
```

- 配置入侵检测特性

```
[sysname-GigabitEthernet1/0/1] port-security intrusion-mode { blockmac | disableport | disableport-temporarily }
```

www.h3c.com

第4步：配置端口 NeedToKnow 特性，该功能用来限制认证端口上出方向的报文转发。即，用户通过认证后，以此 MAC 为目的地址的报文都可以正常转发。可以设置以下三种方式：

- **ntkonly：**仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过
- **ntk-withbroadcasts：**允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过。
- **ntk-withmulticasts：**允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过。

除缺省情况之外，配置了 NeedToKnow 的端口在以上任何一种方式下都不允许未知 MAC 地址的单播报文通过。

```
[sysname-GigabitEthernet1/0/1] port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }
```


第5步：配置入侵检测特性，当设备检测到一个非法的用户通过端口试图访问网络时，该特性用于配置设备可能对其采取的安全措施，包括以下三种方式：

- **blockmac**: 表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中, 源 MAC 地址为阻塞 MAC 地址的报文将被丢弃。此 MAC 地址在被阻塞 3 分钟 (系统默认, 不可配) 后恢复正常。
- **disableport**: 表示将收到非法报文的端口永久关闭。
- **disableport-temporarily**: 表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 **port-security timer disableport** 命令配置。


```
[sysname-GigabitEthernet1/0/1] port-security intrusion-mode { blockmac |
disableport | disableport-temporarily }
```

25.6.4 端口安全配置案例

端口安全配置案例



紫光集团 H3C
核心企业 | 数字化解决方案领导者



Host G1/0/1 交换机 Internet

- 在交换机的端口 **GigabitEthernet1/0/1** 上对接入用户做如下的限制, 允许 64 个用户自由接入, 不进行认证, 将学习到的用户 MAC 地址添加为安全 MAC 地址; 当安全 MAC 地址数量达到 64 后, 停止学习; 当再有新的 MAC 地址接入时, 触发入侵检测, 并将此 MAC 阻塞

www.h3c.com

组网需求:

在交换机的端口 **GigabitEthernet1/0/1** 上对接入用户做如下的限制:

- 允许 64 个用户自由接入, 不进行认证, 将学习到的用户 MAC 地址添加为安全 MAC 地址;
- 当安全 MAC 地址数量达到 64 后, 停止学习; 当再有新的 MAC 地址接入时, 触发入侵检测, 并将此 MAC 阻塞。

配置步骤:

在系统模式下打开端口安全

```
<sysname> system-view
[sysname] port-security enable
```

设置端口允许的最大安全 MAC 地址数为 64

```
[sysname] interface GigabitEthernet 1/0/1
[sysname-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn

```
[sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
```

配置触发入侵检测特性后的保护动作为 blockmac

```
[sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

上述配置完成后，可以用 **display** 命令显示端口安全配置情况，如下：

```
<sysname> display port-security interface GigabitEthernet 1/0/1
Port security parameters:
  Port security          : Enabled
  AutoLearn aging time   : 0 min
  Disableport timeout    : 20 s
  MAC move               : Denied
  Authorization fail     : Online
  NAS-ID profile is not configured
  OUI value list         :
GigabitEthernet1/0/1 is link-up
  Port mode              : autoLearn
  NeedToKnow mode        : Disabled
  Intrusion protection mode : BlockMacAddress
  Security MAC address attribute
    Learning mode        : Sticky
    Aging type           : Periodical
  Max secure MAC addresses : 64
  Current secure MAC addresses : 0
  Authorization          : Permitted
  NAS-ID profile is not configured
```

可以看到端口的最大安全 MAC 数为 64，端口模式为 autoLearn，入侵保护动作为 BlockMacAddress。

配置完成后，允许地址学习，学习到的 MAC 地址数可以用上述命令显示，如学习到 5 个，那么当前的安全 MAC 地址数就为 5，可以在端口视图下用 **display this** 命令查看学习到的 MAC 地址，如：

```
[sysname]display port-security interface GigabitEthernet 1/0/1
Port security parameters:
  Port security          : Enabled
  AutoLearn aging time   : 0 min
  Disableport timeout    : 20 s
  MAC move               : Denied
  Authorization fail     : Online
  NAS-ID profile is not configured
  OUI value list         :
GigabitEthernet1/0/1 is link-up
  Port mode              : autoLearn
  NeedToKnow mode        : Disabled
  Intrusion protection mode : BlockMacAddress
  Security MAC address attribute
    Learning mode        : Sticky
    Aging type           : Periodical
  Max secure MAC addresses : 64
  Current secure MAC addresses : 5
  Authorization          : Permitted
  NAS-ID profile is not configured
```

```
[sysname]interface GigabitEthernet 1/0/1
[sysname-GigabitEthernet1/0/1]dis this
#
interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode autolearn
port-security intrusion-mode blockmac
port-security mac-address security 0000-0000-0001 vlan 1
port-security mac-address security 0000-0000-0002 vlan 1
port-security mac-address security 0000-0000-0003 vlan 1
port-security mac-address security 0000-0000-0004 vlan 1
port-security mac-address security 0000-0000-0005 vlan 1
#
```

当学习到的 MAC 地址数达到 64 后，用命令 **display port-security interface** 可以看到端口模式变为 **secure**，再有新的 MAC 地址到达将触发入侵保护，Trap 信息如下：

```
%Jan 1 23:23:56:828 2013 sysname PORTSEC/5/PORTSEC_VIOLATION: -
IfName=GigabitEthernet1/0/1-MACAddr= 0000-0000-003E-VLANId=1-IfStatus=Up;
Intrusion detected.
```

并且可以通过下述命令看到端口安全将此 MAC 添加为阻塞 MAC：

```
[sysname]display port-security mac-address block
MAC ADDR          Port          VLAN ID
0000-0000-003e    GigabitEthernet1/0/1    1

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
```

25.6.5 端口安全常见故障排查

端口安全常见故障排查



- 无法配置端口安全模式：

- 在当前端口安全模式已配置的情况下，无法直接对端口安全模式进行设置

- 无法配置端口安全MAC地址：

- 端口安全模式为非autoLearn时，不能对安全MAC地址进行设置

- 用户在线情况下无法更换端口安全模式：

- 有802.1X或MAC认证用户在线的情况下，禁止更换端口安全模式

www.h3c.com

- 无法配置端口安全模式：

当前系统无法配置端口安全模式时，会有如下提示：

```
[sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
Error:When we change port-mode, we should first change it to noRestrictions,
then change it to the other.
```

究其原因，是因为在当前端口安全模式已配置的情况下，无法直接对端口安全模式进行设置。这种情况下，需要首先设置端口安全模式为 **noRestrictions** 状态，然后再配置端口安全模式。

```
[sysname-GigabitEthernet1/0/1] undo port-security port-mode
[sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
```

- 无法配置端口安全 MAC 地址：

当前系统无法配置端口安全 MAC 地址时，会有如下提示：

```
[sysname-GigabitEthernet1/0/1]port-security mac-address security 1-1-2 vlan 1
Error:Can not operate security MAC address for current port mode is not
autoLearn!
```

究其原因，是因为端口安全模式为非 **autoLearn** 时，不能对安全 MAC 地址进行设置。

这种情况下，需要首先设置端口安全模式为 **autoLearn** 状态，然后再配置端口安全 MAC 地址。

```
[sysname-GigabitEthernet1/0/1]undo port-security port-mode
[sysname-GigabitEthernet1/0/1]port-security max-mac-count 64
[sysname-GigabitEthernet1/0/1]port-security port-mode autolearn
[sysname-GigabitEthernet1/0/1]port-security mac-address security 1-1-2 vlan 1
```

25.7 本章总结

本章总结

- 介绍了802.1X的协议、扩展应用和配置
- 介绍了MAC地址认证的原理和配置
- 介绍了端口安全的原理和配置

www.h3c.com

25.8 习题和解答

25.8.1 习题

- 802.1X 协议体系结构包括哪几个实体？（ ）
A. 客户端 B. 设备端 C. 终端 D. 认证服务器
- MAC 地址认证不需要用户安装任何客户端软件，但触发认证时需要用户手动输入用户名和密码。（ ）
T. 正确 F. 错误
- 如下关于端口安全特性的描述错误的是？（ ）
A. autoLearn 模式下，当端口下的安全 MAC 地址数超过端口允许学习的最大安全 MAC 地址数后，端口模式会自动转变为 secure 模式。
B. userLogin 模式对接入用户采用基于 MAC 的 802.1X 认证，此模式下，端口最多只允许一个 802.1X 认证用户接入。
C. macAddressOrUserLoginSecure 模式，用户 MAC 认证成功后，仍然可以进行 802.1X 认证。
D. macAddressElseUserLoginSecure 模式，对于 802.1X 报文先进行 MAC 地址认证，如果 MAC 地址认证失败进行 802.1X 认证。
- EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：_____和_____。
- 端口配置基于 port 的 Guest vlan，在什么情况下端口才被加入 Guest Vlan？
- EAP 中继和 EAP 终结两种认证方式有什么不同？

25.8.2 习题答案

- ABD
- F
- B
- EAP-Message、Message-Authenticator
- 答：当设备从端口发送触发认证报文（EAP-Request/Identity）超过设定的最大次数而没有收到任何回应报文后，端口被加入 Guest Vlan。
- 答：EAP 中继方式是将 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，而 EAP 终结方式将 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。

第26章 *网络访问控制

网络信息安全威胁在不断增加，对网络访问的控制成为网络管理的重要内容。网络访问控制通常包含通过安全策略阻止不符合安全要求的终端访问网络，对 WEB 访问用户进行控制，以及通过访问控制列表过滤非法用户对网络的访问。

本章对用于网络访问控制技术中的 EAD 和 PORTAL 技术进行介绍。

26.1 本章目标

课程目标

● 学习完本课程，您应该能够：

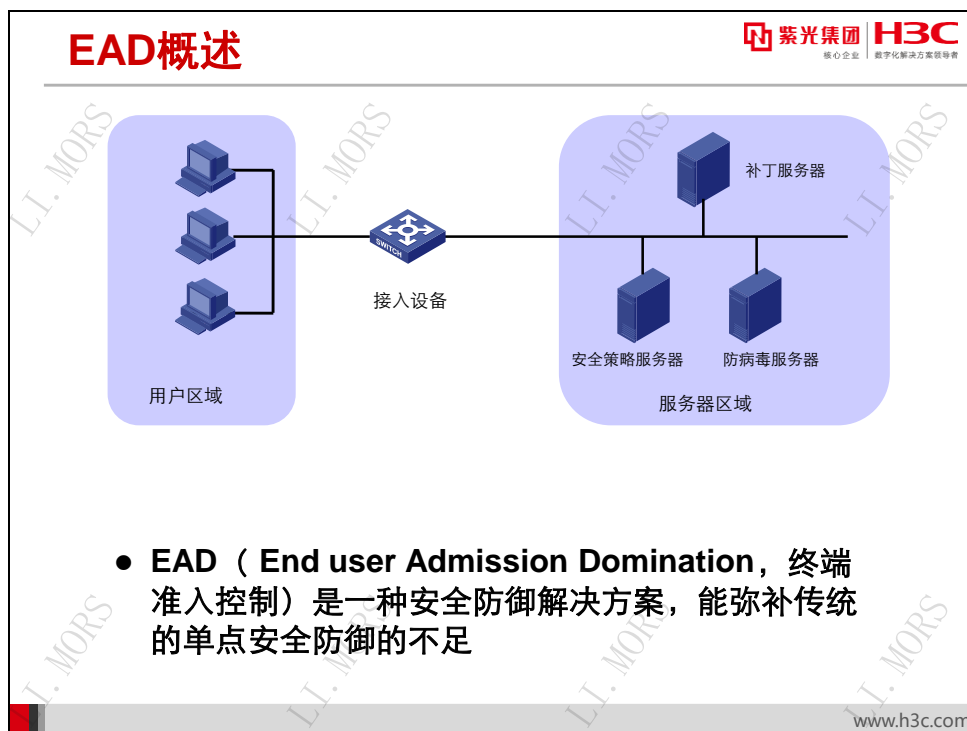
- 掌握EAD安全防御系统原理与配置
- 掌握PORTAL认证原理与配置



www.h3c.com

26.2 EAD解决方案

26.2.1 EAD 概述



传统的针对病毒的防御体系是以孤立的单点防御为主, 如在个人计算机上安装防病毒软件、防火墙软件等。当发现新的病毒或新的网络攻击时, 一般是由网络管理员发布病毒告警或补丁升级公告, 要求网络中的所有计算机安装相关防御软件。传统的防御方式并不能有效应对病毒的威胁, 主要表现在被动防御, 缺乏主动抵抗能力; 单点防御, 对病毒的重复、交叉感染缺乏控制; 分散管理, 安全策略不统一。

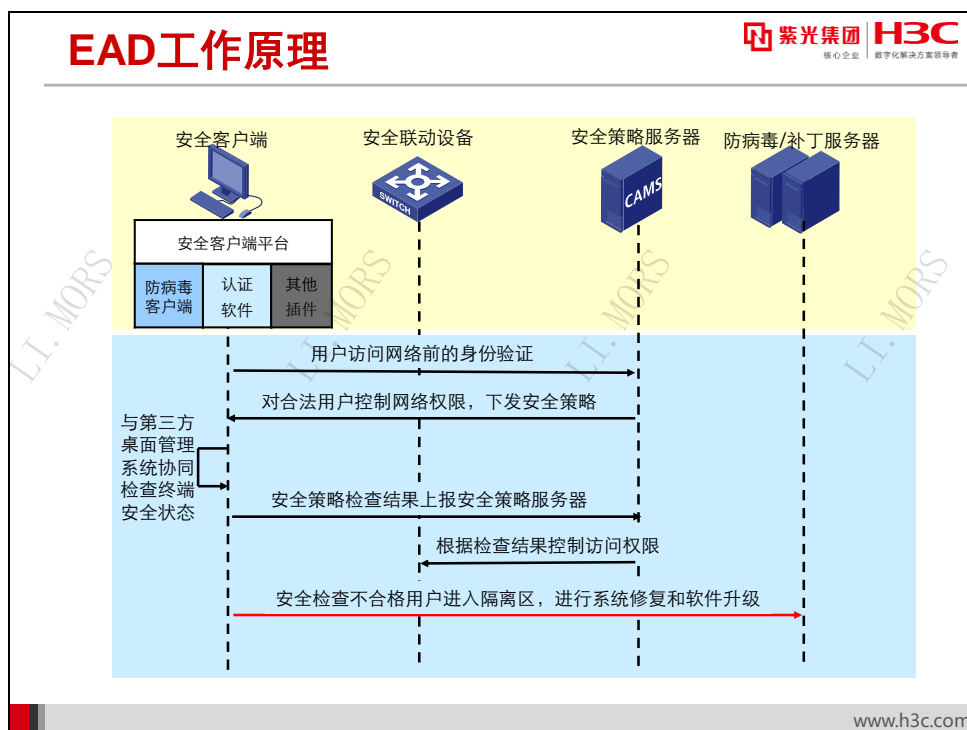
EAD (Endpoint Admission Defense, 端点准入防御) 整合孤立的单点防御系统, 加强对用户的集中管理, 统一实施企业安全策略, 提高网络终端的主动抵抗能力。EAD 方案通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动, 可以将不符合安全要求的终端限制在“隔离区”内, 防止“危险”终端对网络安全的损害, 避免“易感”终端受到病毒的攻击。EAD 的主要功能包括:

- 检查终端用户的安全状态和防御能力;
- 隔离“危险”和“易感”终端;
- 强制修复系统补丁、升级防病毒软件;
- 管理与监控。

EAD 提供了一个全新的安全防御体系, 将防病毒功能与网络接入控制相融合, 加强了对终端用户的集中管理, 提高了网络终端的主动抵抗能力。EAD 具有以下技术特点:

- 整合防病毒与网络接入控制，大幅提高安全性；
- 支持多种认证方式，适用范围广；
- 全面“隔离”危险终端；
- 灵活、方便的部署与维护；
- 详细的安全事件日志与审计；
- 专业防病毒厂商的合作；
- 具有策略实施功能，方便企业实施组织级安全策略；
- 可扩展的安全解决方案，有效保护投资。

26.2.2 EAD 工作原理



EAD 的基本部件包括安全客户端、安全联动设备、安全策略服务器以及防病毒服务器、补丁服务器等第三方服务器。

- 安全客户端是安装在用户终端系统上的软件, 是对用户终端进行身份验证、安全状态评估、以及安全策略实施的主体。
- 安全联动设备是企业网络中安全策略的实施点, 起到强制网络接入终端进行身份验证、隔离不符合安全策略的用户终端、提供基于身份的网络服务的作用。安全联动设备可以是 H3C 的交换机、路由器等。

- 安全策略服务器是 EAD 方案中的管理与控制中心，可运行在 Windows、Linux 平台下，兼具用户管理、安全策略管理、安全状态评估、安全联动控制、以及安全事件审计等功能。
- 第三方服务器是指处于隔离区中、用于终端进行自我修复的防病毒服务器或补丁服务器。

EAD 的基本功能是通过以上组件的联动实现的，其基本过程如下：

第1步：用户终端试图接入网络时，首先通过安全客户端由安全联动设备和安全策略服务器配合进行用户身份认证，非法用户将被拒绝接入网络。

第2步：安全策略服务器对合法用户下发安全策略，并要求合法用户进行安全状态认证。


第3步：由客户端的第三方桌面管理系统协同安全策略服务器对合法终端的补丁版本、病毒库版本等进行检测。之后，安全客户端将安全策略的检查结果上报安全策略服务器。

第4步：安全策略服务器根据检查结果控制用户的访问权限。安全状态合格的用户将实施由安全策略服务器下发的安全设置，并由安全联动设备提供基于身份的网络服务；安全状态不合格的用户将被安全联动设备隔离到隔离区，可以进行系统的修复如补丁、病毒库的升级，直到安全状态合格。

安全认证通过后在安全策略服务器的配合下可以对合法终端进行安全修复和管理工作，主要包括心跳机制、实时监控及监控发现异常后的处理。

26.2.3 EAD 配置

EAD配置



紫光集团 H3C
核心企业 | 数字化解决方案领导者

- 配置策略服务器

[sysname-radius-name] security-policy-server ip-address
- 使能EAD快速部署功能

[sysname] dot1x ead-assistant enable
- 配置EAD快速部署免认证网段

[sysname] dot1x ead-assistant free-ip ip-address
 { mask-address | mask-length }
- 配置EAD快速部署重定向URL

[sysname] dot1x ead-assistant url url-string

www.h3c.com

在 H3C 网络设备上，配置 EAD 的主要任务是设置安全策略服务器。可以在 RADIUS 方案视图下使用如下命令来指定安全策略服务器的 IP 地址：

[SWA-radius-name] security-policy-server *ip-address*

缺省情况下，设备没有指定 RADIUS 服务器的安全策略服务器。

在日常工作中，EAD 客户端的部署工作量很大。例如，网络管理员需要手动为每个 EAD 客户端下载版本、升级客户端软件。在 EAD 客户端数目较多的情况下，这给管理员带来巨大的工作量。通过配置 802.1X 支持的 EAD 快速部署，可以使所有接入网络的终端用户通过访问特定的服务器，从而能够下载并安装 EAD 客户端。它由以下两个功能组成：

- 用户受限访问：802.1X 认证成功前（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；
- 用户 HTTP 访问 URL 重定向：终端用户在 802.1X 认证成功前（包括认证失败），如果使用浏览器访问网络，设备就会将用户访问的 URL 地址重定向到已配置的 URL。

可以在系统视图下配置用户受限访问地址段，其命令为：

[SWA]dot1x ead-assistant enable

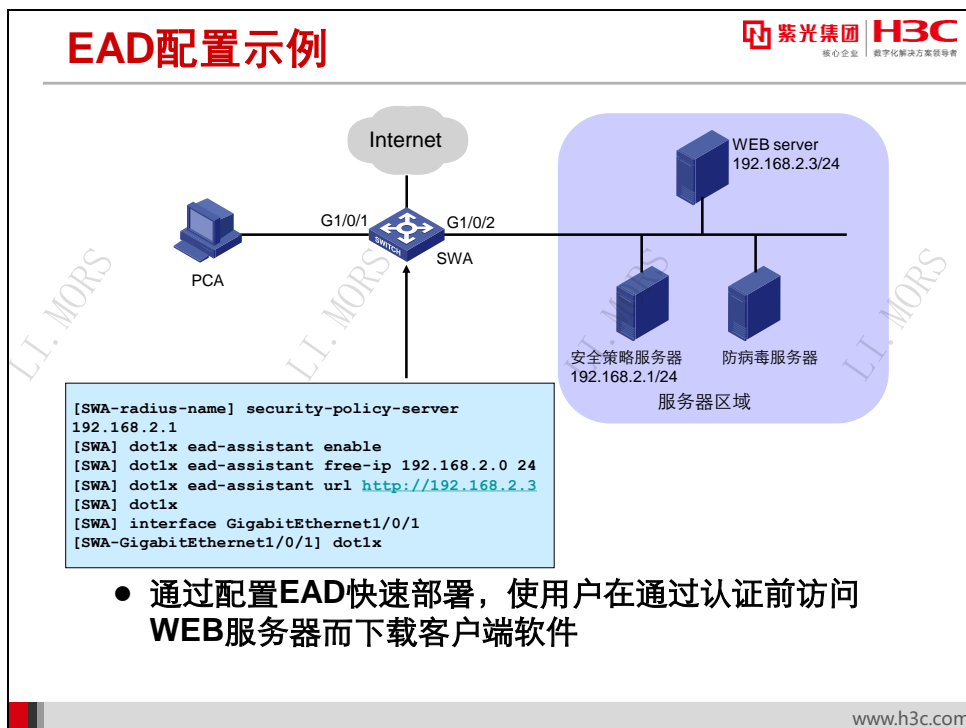
[SWA] dot1x ead-assistant free-ip *ip-address* { *mask-address* | *mask-length* }

同样，在系统视图下配置 HTTP 访问 URL 重定向的地址，其命令为：

[SWA] dot1x ead-assistant url *url-string*

注意：

重定向的 URL 必须处在 Free IP 网段内，否则无法实现重定向。



在上图所示网络中，交换机 SWA 作为安全联动设备，负责实施对用户的访问控制功能。服务器区域中包含有安全策略服务器、防病毒服务器等。为了实现 EAD 快速部署功能，将服务器区域的地址范围配置为 Free IP 网段，以使主机能够在通过认证前从服务器下载 EAD 客户端软件；同时设置 WEB 服务器，以使主机的 HTTP 访问能够被重定向。SWA 上的相关配置如下：

```

[SWA-radius-name] security-policy-server 192.168.2.1
[SWA] dot1x ead-assistant enable
[SWA] dot1x ead-assistant free-ip 192.168.2.0 24
[SWA] dot1x ead-assistant ead-assistant url http://192.168.2.3
  
```

因为 EAD 快速部署需要 802.1X 支持，所以需要在交换机上开启 802.1X 功能。SWA 上的相关配置如下：

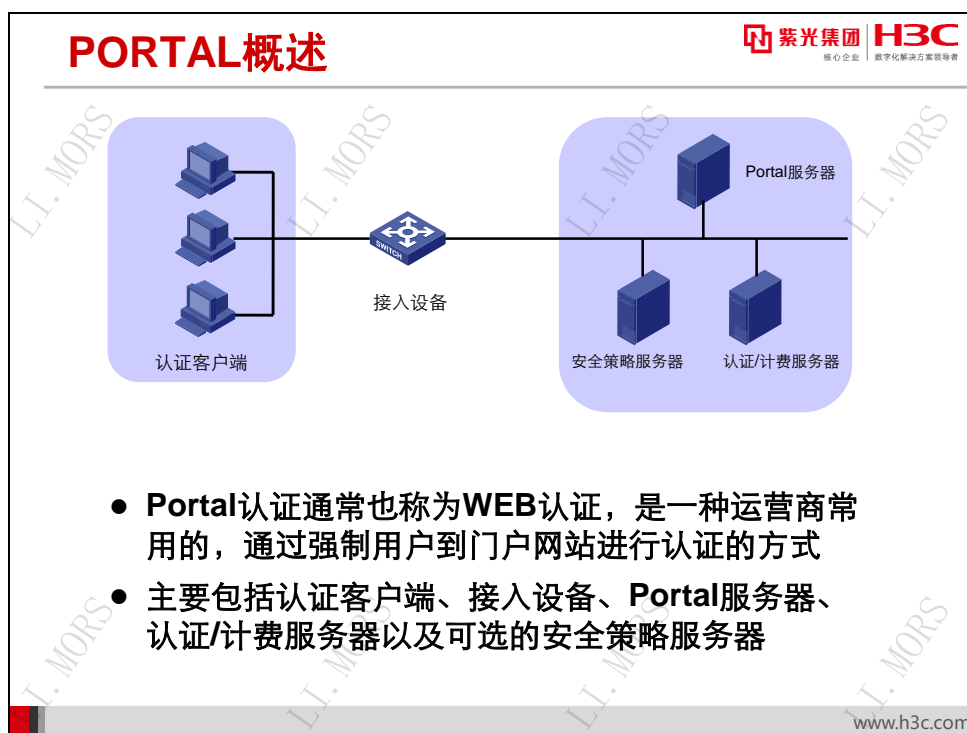
```

[SWA] dot1x
[SWA] interface ethernet1/0/1
[SWA-Ethernet1/0/1] dot1x
  
```

以上配置完成后，用户在 802.1X 认证成功前，通过浏览器访问任何外部网站都会被重定向到 WEB 服务器页面。

26.3 PORTAL 认证

26.3.1 概述



Portal 认证通常也称为 WEB 认证，Portal 认证网站通常也称为门户网站。

在使用 Portal 认证的网路中，未认证用户上网时，设备强制用户登录到特定网站，用户可以免费访问其中的服务。当用户需要使用互联网中的其他信息时，必须在门户网站进行认证。只有认证通过后才可以使用互联网资源。

Portal 业务可以为运营商提供方便的管理功能，门户网站可以开展广告、社区服务、个性化的业务等，使宽带运营商、设备提供商和内容服务提供商形成一个产业生态系统。

Portal 可以通过强制接入终端实施补丁和防病毒策略，加强网络终端对病毒攻击的主动防御能力，其扩展功能主要包括如下：

- 在 Portal 身份认证的基础上增加了安全认证机制，可以检测接入终端上是否安装了防病毒软件、是否更新了病毒库、是否安装了非法软件、是否更新了操作系统补丁等；
- 用户通过身份认证后仅仅获得访问部分互联网资源（非受限资源）的权限，如病毒服务器、操作系统补丁更新服务器等；当用户通过安全认证后便可以访问更多的互联网资源（受限资源）。

Portal 体系主要由 4 个基本要素组成：认证客户端、接入设备、Portal 服务器、认证/计费服务器。除此之外根据桌面安全要求可以选择安装安全策略服务器。

认证客户端是安装于用户终端的客户端系统，为运行 HTTP/HTTPS 协议的浏览器或运行 Portal 客户端软件的主机。

交换机、路由器等宽带接入设备统称接入设备，主要有三方面的作用：

- 在认证之前，将认证网段内用户的所有 HTTP 请求都重定向到 Portal 服务器；
- 在认证过程中，与 Portal 服务器、安全策略服务器、认证/计费服务器交互，完成身份认证/安全检查/计费的功能；
- 在认证通过后，允许用户访问被管理员授权的互联网资源。

Portal 服务器是接收 Portal 客户端认证请求的服务器端系统，提供免费门户服务和基于 WEB 认证的界面，与接入设备交互认证客户端的认证信息。

认证/计费服务器与接入设备交互，完成对用户的认证和计费。

安全策略服务器则与 Portal 客户端、接入设备进行交互，完成对用户的安全认证，并对用户进行授权操作。

以上五个基本要素的交互过程为：

- 未认证用户访问网络时，在 IE 地址栏中输入一个互联网地址，那么此 HTTP 请求在经过接入设备时会被重定向到 Portal 服务器的 WEB 认证主页上；若需要使用 Portal 的扩展认证功能，则用户必须使用 Portal 客户端。
- 用户在认证主页/认证对话框中输入认证信息后提交，Portal 服务器会将用户的认证信息传递给接入设备。
- 然后接入设备再与认证/计费服务器通信进行认证和计费。
- 认证通过后，如果未对用户采用安全策略，则接入设备会打开用户与互联网的通路，允许用户访问互联网资源；如果对用户采用了安全策略，则客户端、接入设备、与安全策略服务器交互，对用户的安全检测通过之后，安全策略服务器根据用户的安全性授权用户访问受限资源。

26.3.2 PORTAL 认证方式

PORTAL 认证方式

紫光集团 H3C
核心企业 数字化转型方案领导者

- 三层认证方式
 - 客户端与接入设备间有三层设备
 - 直接获得IP地址
- 非三层认证方式
 - 客户端与接入设备间没有三层设备
 - 直接获得IP地址进行认证
 - 二次地址分配认证

www.h3c.com

根据客户端与接入设备之间是否有三层设备，Portal 认证方式分为非三层认证方式和三层认证方式。

根据地址分配方式的不同，非三层认证方式又包括有直接认证方式和二次地址分配认证方式。

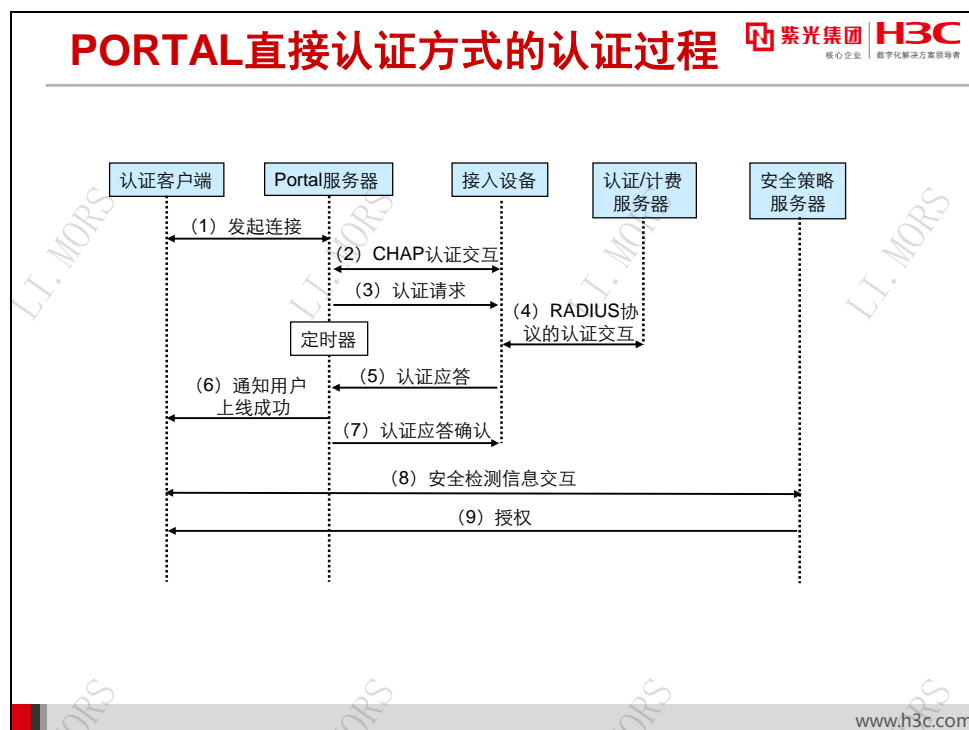
- **直接认证方式：**用户在认证前通过手工配置或 DHCP 直接获取一个 IP 地址，只能访问 Portal 服务器，以及设定的免费访问地址；认证通过后即可访问网络资源。
- **二次地址分配认证方式：**用户在认证前通过 DHCP 获取一个私网 IP 地址，只能访问 Portal 服务器，以及设定的免费访问地址；认证通过后，用户会申请到一个公网 IP 地址，即可访问网络资源。该认证方式解决了 IP 地址规划和分配问题，对未通过认证的用户不分配公网 IP 地址。

在三层认证方式下，客户端的获取 IP 地址方式与直接认证方式类似，直接获取 IP 地址后再到 Portal 服务器进行认证。

三层认证方式与非三层认证方式的区别是：

- 组网方式不同。三层认证方式的认证客户端和接入设备之间可以跨越三层转发设备；非三层认证方式则要求认证客户端和接入设备之间没有三层设备；
- 用户标识不同。三层认证方式中接入设备不会学习认证客户端的 MAC 地址信息，因此以 IP 地址唯一标识用户；非三层认证方式中，以 IP 和 MAC 地址的组合来唯一标识用户。

26.3.3 PORTAL 认证过程

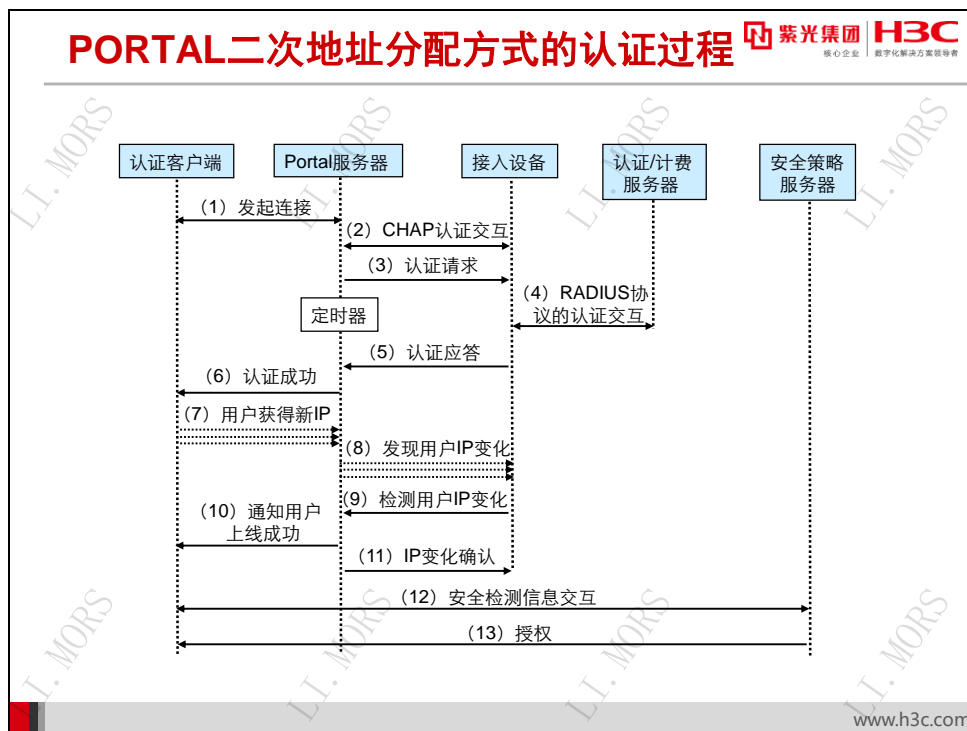


三层认证方式与非三层直接认证方式具有相同的认证流程，其过程如下：

- 1) Portal 用户通过 HTTP 协议发起认证请求。HTTP 报文经过接入设备时，对于访问 Portal 服务器或设定的免费访问地址的 HTTP 报文，设备允许其通过；对于访问其他地址的报文，接入设备将其重定向到 Portal 服务器。Portal 服务器提供 Web 页面供用户输入用户名和密码来进行认证。
- 2) Portal 服务器与接入设备之间进行 CHAP（Challenge Handshake Authentication Protocol, 质询握手验证协议）认证交互，若采用 PAP（Password Authentication Protocol, 密码验证协议）认证则直接进入下一步骤。
- 3) Portal 服务器将用户输入的用户名和密码组装成认证请求报文发往接入设备，同时开启定时器等待认证应答报文。
- 4) 接入设备与 RADIUS 服务器之间进行 RADIUS 协议报文的交互。
- 5) 接入设备向 Portal 服务器发送认证应答报文。
- 6) Portal 服务器向客户端发送认证通过报文，通知客户端认证（上线）成功。
- 7) Portal 服务器向接入设备发送认证应答确认。
- 8) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测接入终端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

- 9) 安全策略服务器根据用户的安全性授权用户访问非授权资源, 授权信息保存到接入设备中, 接入设备将使用该信息控制用户的访问。

以上步骤中, 步骤 8、9 为 Portal 认证扩展功能的交互过程。




三层认证方式下的二次地址分配认证方式流程如上图所示（步骤 1~6 与直接认证方式中的步骤 1~6 相同）：

- 7) 客户端收到认证通过报文后, 通过 DHCP 请求获取新的公网 IP 地址, 并通知 Portal 服务器用户已经获得新 IP 地址。
- 8) Portal 服务器通知接入设备客户端获得新公网 IP 地址。
- 9) 接入设备通过检测 ARP 协议报文发现了用户 IP 变化, 并通告 Portal 服务器已检测到用户 IP 变化。
- 10) Portal 服务器通知客户端上线成功。
- 11) Portal 服务器向接入设备发送 IP 变化确认报文。
- 12) 客户端和安全策略服务器之间进行安全信息交互, 安全策略服务器检测接入终端的安全性是否合格, 包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。
- 13) 安全策略服务器根据用户的安全性授权用户访问非授权资源, 授权信息保存到接入设备中, 接入设备将使用该信息控制用户的访问。

26.3.4 PORTAL 配置

PORTAL配置

 紫光集团 H3C
核心企业 数字化解决方案领导者

- 配置Portal服务器

```
[sysname]portal server server-name
[sysname-portal-server-name]ip ip-address [ key {simple | cipher} ] key-string
[sysname-portal-server-name]port port-id
```
- 配置Portal Web服务器

```
[sysname]portal web-server server-name
[sysname-portal-websvr-name]url url-string
```
- 在接口下启用Portal和Portal web-server并指定认证方式

```
[sysname-Vlan-interface100] portal enable method { direct | layer3 | redhcp }
[sysname-Vlan-interface100] portal apply web-server server-name
```

www.h3c.com

Portal 的基本配置包括配置 Portal 服务器、Portal Web 服务器和在接口上启用 Portal 协议。

可以在系统视图下配置 Portal 服务器，其命令如下：

```
[SWA]portal server server-name
[SWA-portal-server-name]ip ip-address [ key {simple | cipher} ] key-string
[SWA-portal-server-name]port port-id
```

其中主要参数含义如下：

- *server-name*: 指定 Portal 服务器的名字；
- *ip-address*: Portal 服务器的 IP 地址。若配置本地 Portal 服务器，则此地址为接入设备上与 Portal 客户端路由可达的三层接口 IP 地址；
- *key-string*: 与 Portal 服务器通信需要的共享密钥；
- *port-id*: 设备向 Portal 服务器主动发送报文时使用的目的端口号，缺省值为 50100；

对于采用 web 浏览器作为 portal 客户端的用户，可以配置 Portal Web 服务器在 Portal 认证过程中向用户推送认证页面，同时 Portal Web 服务器也是设备强制重定向用户 HTTP 请求报文时所使用的服务器。在系统视图下配置 Portal Web 服务器，其命令如下：

```
[SWA]portal web-server server-name
[SWA-portal-websvr-name]url url-string
```

其中主要参数含义如下：

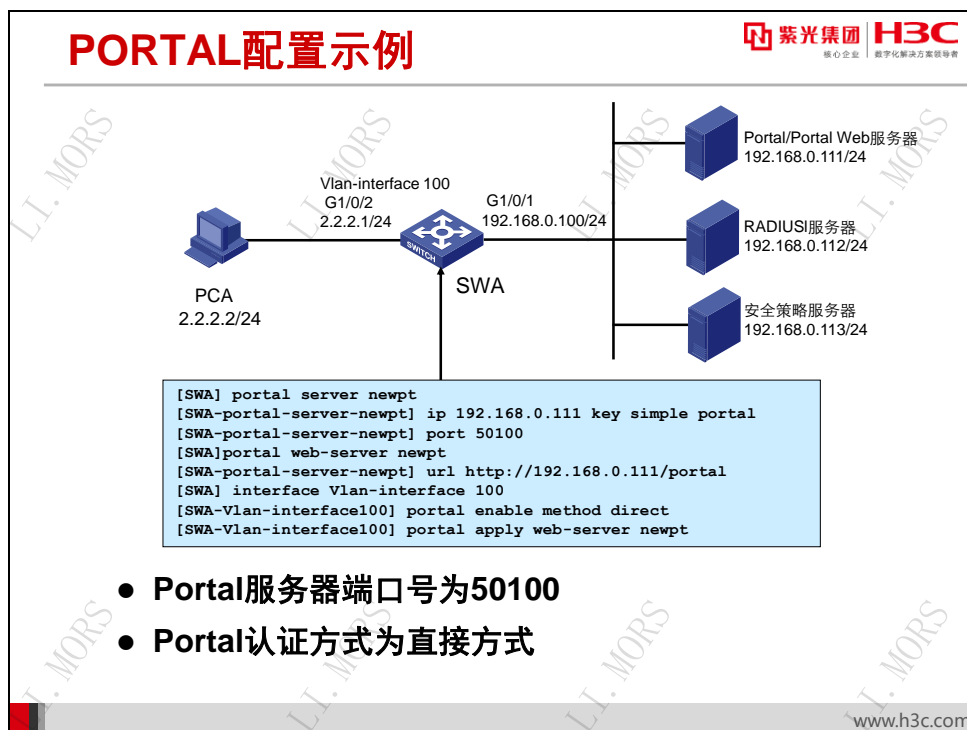
- **server-name**: 指定 Portal Web 服务器的名字；
- **url-string**: HTTP 报文重定向地址，缺省地址格式为 `http://ip-address`。

配置完 Portal 服务器和 Portal Web 服务器后，还需要在接口上使能 Portal 认证，同时指定引用的 Portal Web 服务器、配置认证方式和服务类型。相关命令如下所示：

```
[SWA-Vlan-interface100] portal enable method { direct | layer3 | redhcp }
[SWA-Vlan-interface100] portal apply web-server server-name
```

其中主要参数含义如下：

- **direct**: 直接认证方式；
- **layer3**: 三层认证方式；
- **redhcp**: 二次地址分配认证方式；
- **server-name**: Portal Web 服务器的名字。



如上图所示，主机 PCA 连接到交换机 SWA 上进行接入认证，交换机上进行 Portal 服务器配置，将主机的 HTTP 请求重定向到 Portal Web 服务器，由 Portal Web 服务器将用户的认证信息传递给接入设备；然后接入设备再与认证/计费服务器通信进行认证和计费。

因没有 DHCP 服务器，所以网络中采用三层直接方式的 Portal 认证。

交换机 SWA 上的配置如下：

```
[SWA] portal server newpt
```



```
[SWA-portal-server-newpt]ip 192.168.0.111 key simple portal
[SWA-portal-server-newpt]port 50100
[SWA]portal web-server newpt
[SWA-portal-server-newpt]url http://192.168.0.111/portal
[SWA] interface Vlan-interface 100
[SWA-Vlan-interface100] portal enable method direct
[SWA-Vlan-interface100] portal apply web-server newpt
```

因客户端还需要通过认证/计费服务器通信进行认证和计费；通过安全策略服务器进行网络资源访问授权，所以还需要在 SWA 中增加如下配置：

```
[SWA] radius scheme rs1
[SWA-radius-rs1] primary authentication 192.168.0.112
[SWA-radius-rs1] primary accounting 192.168.0.112
[SWA-radius-rs1] key authentication radius
[SWA-radius-rs1] key accounting radius
[SWA-radius-rs1] service-type extended
[SWA-radius-rs1] security-policy-server 192.168.0.113
[SWA] domain dm1
[SWA-isp-dm1] authentication portal radius-scheme rs1
[SWA-isp-dm1] authorization portal radius-scheme rs1
[SWA-isp-dm1] accounting portal radius-scheme rs1
[SWA] domain default enable dm1
```

26.4 本章总结

本章总结

- EAD是一种安全防御解决方案，它的功能包括检查、隔离、修复、管理和监控
- Portal认证也称为Web认证，认证方式包括非三层认证和三层认证

www.h3c.com

26.5 习题和解答

26.5.1 习题

1. EAD 快速部署可以实现哪些功能？（ ）
 - A. 用户在进行 802.1X 认证前可以访问特定网段地址
 - B. 用户在进行 802.1X 认证失败时可以访问特定网段地址
 - C. 在用户进行 802.1X 认证前，对用户的 HTTP 访问进行 URL 重定向
 - D. 在用户进行 802.1X 认证成功时，对用户的 HTTP 访问进行 URL 重定向
2. 如下哪些属于 Portal 的认证方式？（ ）
 - A. 直接认证 B. EAP 认证 C. 二次地址分配认证 D. 三层认证方式
3. Portal 认证方式中，非三层认证以（ ）作为用户标识，三层认证以（ ）作为用户标识？
 - A. 用户 IP 地址 B. 用户 MAC 地址
 - C. 用户 IP 地址和 MAC 地址信息 D. 用户 IP 地址或 MAC 地址信息
4. 用户在完成 802.1X 认证后要 EAD 安全检查，安全检查失败后系统只允许其访问隔离区。已知隔离区的网络地址为 192.168.42.0/24，如下哪项 ACL 配置可以完成此隔离功能？（ ）
 - A. acl advanced 3000
rule 1 permit ip destination 192.168.42.0 0.0.0.255
 - B. acl advanced 3001
rule 1 deny ip destination 192.168.42.0 0.0.0.255
 - C. acl advanced 3002
rule 1 permit ip destination 192.168.42.0 0.0.0.255
rule 2 deny ip
 - D. acl advanced 3003
rule 1 deny ip destination 192.168.42.0 0.0.0.255
rule 2 permit ip
5. 802.1X 中的 Free-IP 地址段和 EAD 的隔离区都是特定情况下用户被允许访问区域，它们的区别是（ ）。
 - A. Free-IP 是用户进行认证前可访问的地址
 - B. Free-IP 是用户进行认证失败后可访问的地址
 - C. 隔离区是用户进行认证前可访问的地址
 - D. 隔离区是用户进行认证失败后可访问的地址
 - E. 隔离区是用户进行认证成功、安全检查不通过时可访问的地址

26.5.2 习题答案

1. ABD 2. ACD 3. C, A 4. C 5. ABE

第27章 SSH

用于远程登录的 Telnet 应用提供用户名密码验证，以确认登录用户的身份。但是其验证相对简单，且用户名和密码采用明文传输，导致设备的安全性降低。

为了保障设备的安全，采用更为安全可靠的登录方式和验证协议成为趋势，由此诞生了 SSH（Secure Shell）协议。SSH 是一种安全的远程登录协议，基于 TCP 传输层协议，可以采用口令方式或密钥方式实现安全认证，其安全性大大强于 Telnet，在安全性要求较高的网络中，SSH 已经成为远程登录的首选。本章将对 SSH 协议及其应用扩展 SFTP 进行简要介绍。

27.1 本章目标

课程目标

学习完本课程，您应该能够：

- 了解SSH定义及应用
- 掌握SSH和SFTP工作原理
- 掌握SSH和SFTP应用
- 掌握SSH和SFTP的配置及维护



27.2 SSH基本原理

27.2.1 SSH 概述

SSH概述

紫光集团 H3C
核心企业 | 数字化解决方案领导者

- SSH (Secure Shell) 是一种安全的远程登录协议。基于TCP进行传输，端口号是22。
- SSH协议的特点：
 - 支持DES、3DES数据加密算法
 - 支持公钥验证方式、密码验证方式、不验证方式
 - 支持RSA认证，具有防篡改功能

www.h3c.com

Telnet 是互联网上使用最广泛的远程登录协议。但是，Telnet 协议本身并没有提供安全的认证方式，而且通过 TCP 传输的内容都是明文方式，用户名和密码可以通过网络报文分析的方式获得，存在着很大的安全隐患。另外，由于系统对 Telnet 用户采用简单的口令验证，所以 DOS 攻击、主机 IP 地址欺骗、路由欺骗等恶意攻击都可能给系统带来致命的威胁。

SSH (Secure Shell) 是一种安全的远程登录协议。SSH 协议基于 TCP 进行传输，端口号是 22。通过使用 SSH 协议，远程登录访问的安全性得到了很大的提升。此外，SSH 还提供 SFTP (SSH File Transfer Protocol)，对在公共的 Internet 上的数据传输进行了安全保护。

SSH 协议具有如下特点：

- **完善的数据传输机密性：**SSH 协议支持 DES、3DES 数据加密算法。SSH 客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了非法用户对口令的窃听。同时 SSH 服务对传输的数据也进行了加密。保证了数据的安全性和可靠性。
- **多种认证方式：**SSH 支持公钥验证方式、密码验证方式、不验证方式，用户可以灵活进行选择。

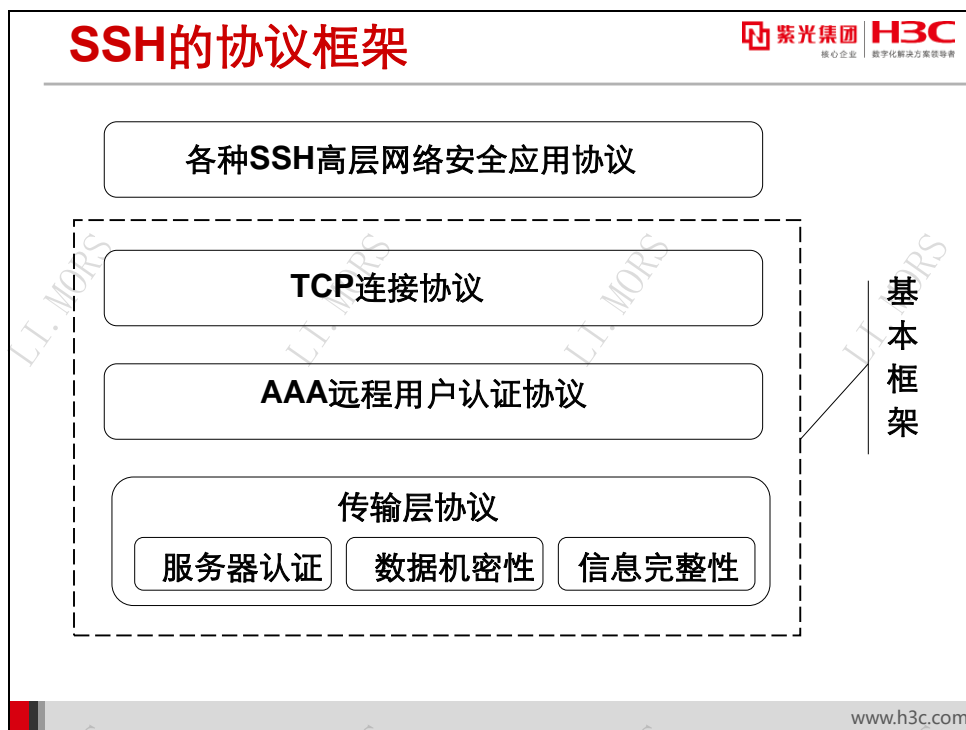
公钥验证方式是 SSH 必须支持的认证方式。使用了公钥验证方式后，客户端生成一段由用户私钥签名的数据发送到服务器，服务器收到用户公钥和签名数据后，会检查用户公钥和签名的合法性，如果都合法则接受该请求，否则拒绝。

密码验证方式为 SSH 可选支持的认证方式之一。Client 将用户名和密码发送给服务器，服务器根据既定的验证方式进行密码验证（本地或远程）验证成功，则接受该请求，否则拒绝。

不验证方式也为可选支持的认证方式之一。配置用户为不认证方式时，服务器在任何情况下必须返回验证通过，此时 SSH 用户认证成功。

- **所支持的 RSA 认证具有攻击防御功能：**SSH 中使用的 RSA 方式是最著名的且被广泛应用的公钥加密体制。RSA 的加密方式为非对称加密，密钥为一对相关密钥（公钥和私钥），其中任一个密钥加密的信息只能用另一个密钥进行解密。私钥的唯一性决定其不仅可以用于加密，还可以作为数字签名，防止非法用户篡改数据。

当前 SSH 有两个版本——SSH1 和 SSH2。但随着 SSH 的成熟应用，大多数实现都已经基于 SSH2。后续介绍将以 SSH2 为基础进行介绍。



SSH 协议框架中最主要的部分是三个协议：传输层协议、用户认证协议和连接协议。同时 SSH 协议框架中还为许多高层的网络安全应用协议提供扩展的支持。它们之间的层次关系可以用上图来表示，在这个框架中：

- 传输层协议（The Transport Layer Protocol）提供服务器认证，数据机密性，信息完整性；
- 用户认证协议（The User Authentication Protocol）为服务器提供客户端的身份鉴别；
- 连接协议（The Connection Protocol）将加密的信息隧道复用成若干个逻辑通道，提供给更高层的应用协议使用。

各种高层应用协议可以相对地独立于 SSH 基本体系之外，并依靠这个基本框架，通过连接协议使用 SSH 的安全机制。

27.2.2 SSH 工作过程

SSH连接建立过程	
阶段	描述
版本号协商阶段	客户端和服务端交换各自所支持SSH协议的版本号，最终协商出双方同意的版本。
密钥和算法协商阶段	客户端和服务端交换算法协商报文，从而协商出最后使用的算法；双方生成会话密钥和会话ID。
认证阶段	客户端向服务器端发送认证请求，服务器端对客户端进行认证。
会话请求阶段	客户端向服务器发送会话请求，服务器等待并处理客户端的请求。
交互会话阶段	双方进入交互会话阶段，数据被加密后双向传送

在整个工作过程中，为实现 SSH 的安全连接，服务器端与客户端要经历如下五个阶段：

1. 版本号协商阶段

版本号协商阶段的主要目的是客户端与服务器端协商双方都能够支持的 SSH 版本，具体步骤如下：

- 服务器打开端口 22，等待客户端连接；
- 客户端向服务器端发起 TCP 初始连接请求，TCP 连接建立后，服务器向客户端发送第一个报文，包括版本标志字符串，格式为“SSH-<主协议版本号>.<次协议版本号>-<软件版本号>”，协议版本号由主版本号和次版本号组成，软件版本号主要是为调试使用；
- 客户端收到报文后，解析该数据包，如果服务器端的协议版本号比自己的低，且客户端能支持服务器端的低版本，就使用服务器端的低版本协议号，否则使用自己的协议版本号；
- 客户端回应服务器，回应报文包含了客户端决定使用的协议版本号；
- 服务器比较客户端发来的版本号，决定是否同客户端一起工作；如果协商成功，则进入密钥和算法协商阶段，否则服务器端断开 TCP 连接。

2. 密钥和算法协商阶段：

在此阶段，客户端和服务端交换算法协商报文，从而协商出最后使用的算法并生成会话密钥和会话 ID。具体步骤如下：

- 服务器端和客户端分别发送算法协商报文给对端，报文中包含自己支持的公钥算法列表、加密算法列表、MAC（Message Authentication Code，消息验证码）算法列表、压缩算法列表等；
- 服务器端和客户端根据对端和本端支持的算法列表得出最终使用的算法；
- 服务器端和客户端利用 DH 交换（Diffie-Hellman Exchange）算法、主机密钥对等参数，生成会话密钥和会话 ID。

通过以上步骤，服务器和客户端就取得了相同的会话密钥和会话 ID。对于后续传输的数据，两端都会使用会话密钥进行加密和解密，保证了数据传送的安全。在认证阶段，两端会使用会话 ID 用于认证过程。

3. 认证阶段：

此阶段涉及到客户机与服务端间的认证过程，具体步骤如下：

- 客户端向服务器发送认证请求，认证请求中包含用户名、认证方法、与该认证方法相关的内容（如：password 认证时，内容为密码）；
- 服务器对客户端进行认证，如果认证失败，则向客户端发送认证失败消息，其中包含可以再次认证的方法列表；
- 客户端从认证方法列表中选取一种认证方法再次进行认证；
- 该过程反复进行，直到认证成功或者认证次数达到上限，服务器关闭连接为止。

SSH 提供两种认证方法：

- password 认证：客户端向服务器发出 password 认证请求，将用户名和密码加密后发送给服务器；服务器将该信息解密后得到用户名和密码的明文，与设备上保存的用户名和密码进行比较，并返回认证成功或失败的消息；
- publickey 认证：采用数字签名的方法来认证客户端。目前，设备上可以利用 RSA 两种公共密钥算法实现数字签名。客户端发送包含用户名、公共密钥和公共密钥算法的 publickey 认证请求给服务器端。服务器对公钥进行合法性检查，如果不合法，则直接发送失败消息；否则，服务器利用数字签名对客户端进行认证，并返回认证成功或失败的消息。

4. 会话请求阶段：

认证通过后，客户端向服务器发送会话请求。服务器等待并处理客户端的请求。在这个阶段，请求被成功处理后，服务器会向客户端回应 SSH2_MSG_CHANNEL_SUCCESS 包，SSH 进入交互会话阶段；否则回应 SSH2_MSG_CHANNEL_FAILURE 包，表示服务器处理请求失败或者不能识别请求。

5. 交互会话阶段：

会话请求成功后，连接进入交互会话阶段。在这个模式下，数据被双向传送。客户端将要执行的命令加密后传给服务器，服务器接收到报文，解密后执行该命令，将执行的结果加密发还给客户端，客户端将接收到的结果解密后显示到终端上。

27.3 SFTP介绍

SFTP概述

- SFTP是SSH 2.0中支持的功能
- SFTP建立在SSH连接的基础之上
- SFTP使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作

www.h3c.com

通常情况下，传输文件、共享资源主要通过 FTP 协议来实现。和 TFTP 协议相比，FTP 提供了必要的可靠性，然而对于一些要求网络安全级别比较高，需要严格防范传输数据被监听的情况来说，FTP 协议就无法胜任了。

SFTP（SSH File Transfer Protocol 或 Secure File Transfer Protocol）是 SSH 2.0 中支持的功能。和 FTP 不同的是，SFTP 传输协议默认采用加密方式来传输数据。SFTP 建立在 SSH 连接的基础之上，它使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。同时，由于设备支持作为客户端的功能，用户可以从本地设备安全登录到远程设备上，进行文件的安全传输。

27.4 配置SSH

27.4.1 配置 SSH 服务器

配置SSH服务器—基本配置

紫光集团 H3C
核心企业 数字化解决方案领导者

- 生成DSA、ECDSA或RSA密钥对

[SWA] public-key local create { dsa | ecdsa | rsa }

- 使能SSH服务器功能

[SWA] ssh server enable

www.h3c.com

在设备上配置 SSH 特性之前，设备必须要生成 DSA 或 RSA 密钥。虽然一个客户端只会采用 DSA 和 RSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上同时生成 DSA 和 RSA 两种密钥对。

在系统视图下配置生成 DSA、ECDSA 或 RSA 密钥，在某些早期软件版本中仅支持 RSA 公钥算法。其参考命令如下：

```
[SWA] public-key local create { dsa | ecdsa | rsa }
```

缺省情况下，SSH 服务器功能处于关闭状态。所以，需要在系统视图下使能 SSH 服务，其参考命令如下：

```
[SWA] ssh server enable
```

上述配置完成后，设备生成了 DSA、ECDSA 或 RSA 密钥对，且具有 SSH 服务器功能。

配置SSH服务器—用户配置

紫光集团 H3C
核心企业 数字化转型领导者

- 配置客户端登录的用户界面为scheme方式

```
[SWA-ui-vty0-4] authentication-mode scheme
```

- 配置所在用户界面支持SSH协议

```
[SWA-ui-vty0-4] protocol inbound { all | ssh | telnet }
```

- 配置SSH用户并指定服务类型和认证方式

```
[SWA] ssh user username service-type stelnet  
authentication-type { password | { any | password-  
publickey | publickey } assign { pki-domain  
domain-name | publickey keyname }}
```

www.h3c.com

SSH 客户端通过 VTY 用户界面访问设备。因此，需要配置 SSH 客户端登录时采用的 VTY 用户界面，使其支持 SSH 远程登录协议。配置结果在客户端下次请求登录时生效。

在 VTY 用户界面视图下配置登录用户界面的认证方式为 scheme 方式，命令如下：

```
[SWA-ui-vty0-4] authentication-mode scheme
```

在 VTY 用户界面视图下配置所在用户界面支持 SSH 协议。命令如下：

```
[SWA-ui-vty0-4] protocol inbound { all | ssh | telnet }
```

缺省情况下，系统支持所有的协议。

SSH 用户具有两种服务类型：Stelnet 和 SFTP。Stelnet 即 Secure Telnet，是指传统的 SSH 服务；SFTP 即 Secure FTP。

如果要使用传统的 SSH 服务，则需要在系统视图下配置 SSH 用户为 Stelnet 服务类型并指定认证方式，命令如下：

```
[SWA] ssh user username service-type stelnet authentication-type { password |  
{ any | password-publickey | publickey } assign { pki-domain domain-name |  
publickey keyname }}
```

命令中参数含义如下：

- **username**: SSH 用户名，为 1~80 个字符的字符串。
- **stelnet**: 服务类型为安全的 Telnet。
- **authentication-type**: SSH 用户的认证方式。包括：

- **password**: 强制指定该用户的认证方式为 password。
- **any**: 指定该用户的认证方式可以是 password，也可以是 publickey。
- **password-publickey**: 强制指定该用户的认证方式为 password 和 publickey 认证同时满足。客户端版本为 SSH1 的用户只要通过其中一种认证即可登录；客户端版本为 SSH2 的用户必须两种认证都通过才能登录。
- **publickey**: 强制指定该用户的认证方式为 publickey。
- **assign**: 指定用于验证客户端的参数。

pki-domain domain-name: 指定验证客户端证书的 PKI 域。domain-name 表示 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写。服务器端使用保存在该 PKI 域中的 CA 证书对客户端证书进行合法性检查，无需提前保存客户端的公钥，能够灵活满足大数量客户端的认证需求。

publickey keyname: 为 SSH 用户分配一个已经存在的公钥。keyname 表示已经配置的客户端公共密钥名。

需要注意的是，对于 AAA 用户，即使没有创建对应的 SSH 用户，只要能够通过 AAA 认证，且设置的服务类型为 SSH，则该用户仍然可以通过 password 认证方式登录服务器。

配置SSH服务器—公钥认证



- 从公钥文件中导入客户端的公钥

```
[SWA] public-key peer keyname import sshkey
filename
```

- 手工配置客户端的公钥

```
[SWA] public-key peer keyname
[SWA-pkey-key-code]直接输入公钥内容
[SWA-pkey-public-key] peer-public-key end
```

www.h3c.com

SSH 用户采用 publickey 认证方式时，需要在服务器端配置客户端的 DSA、ECDSA 或 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 DSA、ECDSA 或 RSA 私钥，以便当客户端登录服务器端时，对客户端进行验证。

可以通过从公钥文件中导入和手工配置两种方式在服务器端配置客户端的公钥。

- 从公钥文件中导入客户端的 `publickey` 公钥时，系统会自动将客户端生成的公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式，并实现客户端公钥的配置。这种方式需要客户端事先将 `publickey` 密钥的公钥文件通过 FTP/TFTP 以二进制（binary）方式上传到服务器端。
- 手工配置客户端的 `publickey` 公钥时，可以采用拷贝粘贴的方式将客户端的主机公钥配置到服务器端。这种方式要求拷贝粘贴的主机公钥必须是未经转换的 DER（Distinguished Encoding Rules，特异编码规则）公钥编码格式。

在系统视图下配置从公钥文件中导入客户端的 `publickey` 公钥，命令如下：

```
[SWA] public-key peer keyname import sshkey filename
```

其参数中 `keyname` 的表示公共密钥名，而 `filename` 是导入公钥数据的文件名。

可以在系统视图下手工配置客户端的公钥，命令如下：

```
[SWA]public-key peer keyname
```

```
[SWA-pkey-public-key]直接输入公钥内容
```

```
[SWA-pkey-public-key]peer-public-key end
```

以上配置过程中，`public-key peer` 命令用来进入公共密钥视图，然后可以开始输入密钥数据。在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。所配置的公钥必须是未经转换的 DER 公钥编码格式的十六进制字符串。

密钥输入完成后，用 `public-key-code end` 命令退回到系统视图，结束公钥的编辑过程，系统自动保存配置的公钥。

27.4.2 配置 SSH 客户端

配置SSH客户端

核心企业 数字化转型领导者

- 为SSH客户端指定源IP地址或源接口

```
[SWA] ssh client source { ip ip-address / interface
interface-type interface-number }
```

- 建立SSH客户端和服务端端的连接

```
<SWA> ssh2 server [ port-number ]
```

www.h3c.com

缺省情况下，客户端用设备路由指定的接口地址访问 SSH 服务器。可以在系统视图下为 SSH 客户端指定源 IP 地址或源接口，命令如下所示：

```
[SWA] ssh client source { ip ip-address | interface interface-type interface-number }
```

在系统视图下建立 SSH 客户端和服务端端的连接，并指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法，命令如下：

```
<SWA>ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-
key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 |
aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex
{ dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des |
aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
[ dscp dscp-value | publickey keyname | source { interface interface-type
interface-number | ip ip-address } ] *
```

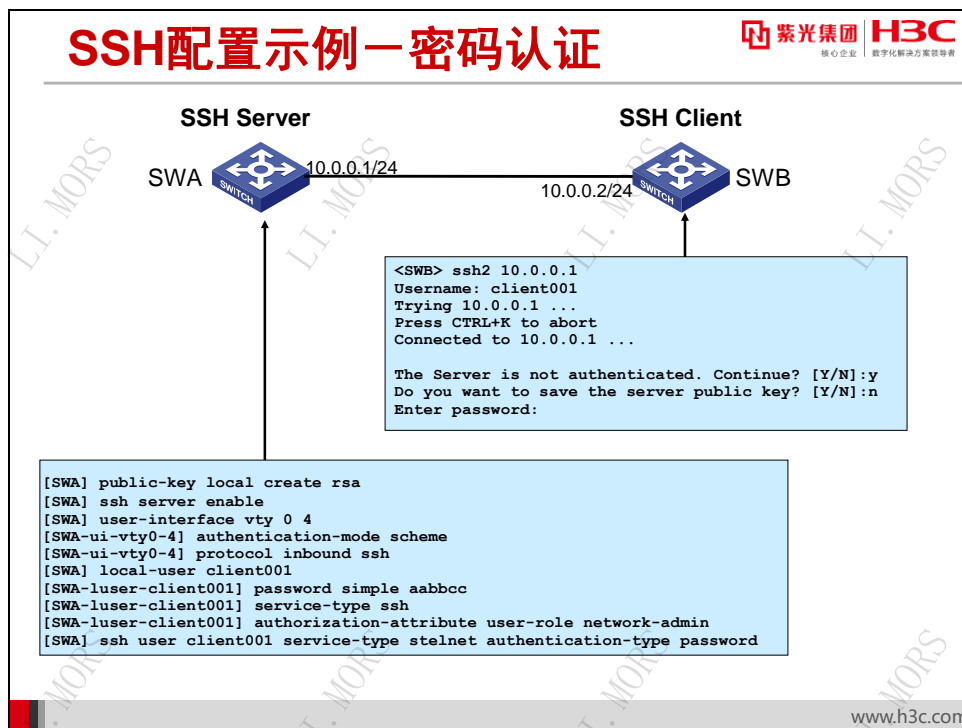
命令中的参数含义如下表所示：

表27-1 算法类型列表

算法名称	描述
dsa	公钥算法为DSA
rsa	公钥算法为RSA
prefer-compress	服务器与客户端之间的首选压缩算法，缺省不支持压缩

算法名称	描述
zlib	压缩算法ZLIB
prefer-ctos-cipher	客户端到服务器端的首选加密算法，缺省算法为aes128
3des	3des-cbc加密算法
aes128	aes128-cbc加密算法
ase256	256位的AES-CBC加密算法
des	des-cbc加密算法
prefer-ctos-hmac	客户端到服务器端的首选HMAC算法，缺省算法为sha1
md5	HMAC算法hmac-md5
md5-96	HMAC算法hmac-md5-96
sha1	HMAC算法hmac-sha1
sha1-96	HMAC算法HMAC-SHA1-96

27.4.3 SSH 配置示例



上图所示网络中，SWA 是 SSH 服务器，SWB 是 SSH 客户端。SSH 用户采用的认证方式为 password 认证。

首先在 SWA 上配置生成 RSA 密钥对，并启动 SSH 服务器。

```
[SWA] public-key local create rsa
[SWA] ssh server enable
```

然后设置 SSH 客户端登录用户界面的认证方式为 AAA 认证，并设置 SWA 上远程用户登录协议为 SSH。


```
[SWA] user-interface vty 0 4
[SWA-ui-vty0-4] authentication-mode scheme
[SWA-ui-vty0-4] protocol inbound ssh
```

创建本地用户 **client001**，并设置用户角色为 **network-admin**；配置 SSH 用户 **client001** 的服务类型为 **stelnet**，认证方式为 **password** 认证。

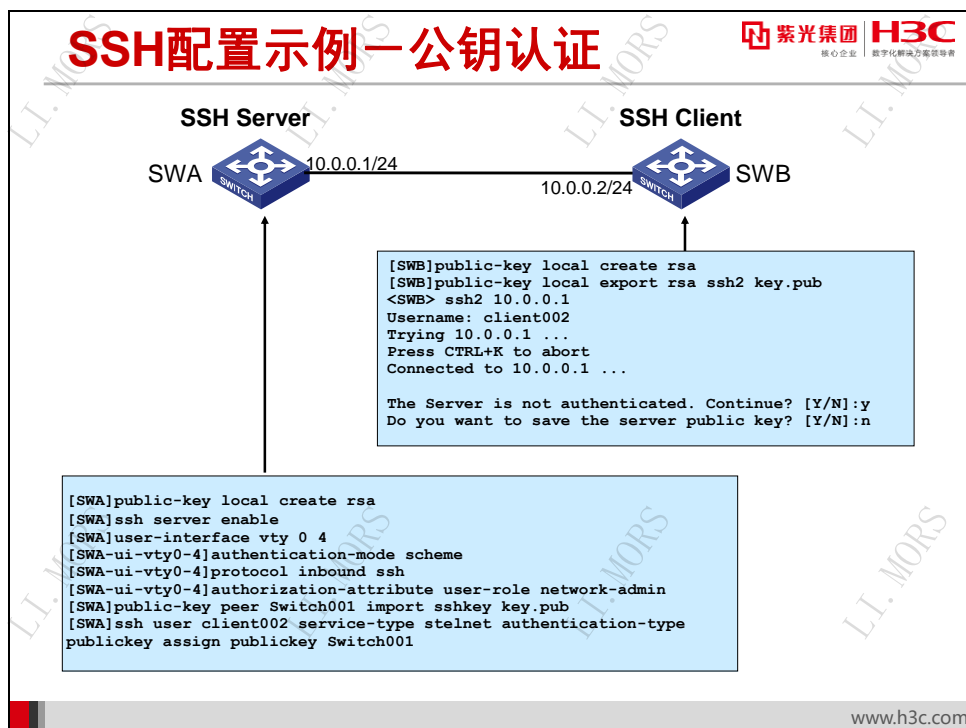
```
[SWA] local-user client001
[SWA-luser-client001] password simple aabbcc
[SWA-luser-client001] service-type ssh
[SWA-luser-client001] authorization-attribute user-role network-admin
[SWA] ssh user client001 service-type stelnet authentication-type password
```

然后在 **SWB** 上建立到服务器的 **SSH** 连接，并指明用户名为 **client001**，密码为 **aabbcc**：

```
<SWB> ssh2 10.0.0.1
Username: client001
Trying 10.0.0.1 ...
Press CTRL+K to abort
Connected to 10.0.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
```

认证成功后，进入到 **SWA** 的用户界面。



上图所示网络中，**SWA** 是 **SSH** 服务器，**SWB** 是 **SSH** 客户端。为了使用 **SSH** 连接具有更强的安全性，网络中 **SSH** 用户采用的认证方式为 **publickey** 认证，公钥算法为 **RSA**。

与密码认证方式一样，需要在 SWA 上配置生成 RSA 密钥对，并启动 SSH 服务器；设置 SSH 客户端登录用户界面的认证方式为 AAA 认证，并设置 SWA 上远程用户登录协议为 SSH。同时，需要配置用户角色为 network-admin。

```
[SWA] public-key local create rsa
[SWA] ssh server enable
[SWA] user-interface vty 0 4
[SWA-ui-vty0-4] authentication-mode scheme
[SWA-ui-vty0-4] protocol inbound ssh
[SWA-ui-vty0-4] authorization-attribute user-role network-admin
```

因为使用公钥认证，所以需要在 SSH 客户端 SWB 上生成 RSA 密钥对，并将生成的 RSA 主机公钥导出到指定文件 key.pub 中。

```
[SWB] public-key local create rsa
[SWB] public-key local export rsa ssh2 key.pub
```

客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到 SSH 服务器 SWA 上。

再返回到 SWA 上，配置从文件 key.pub 中导入客户端的公钥。

```
[SWA] public-key peer Switch001 import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 Switch001。

```
[SWA] ssh user client002 service-type stelnet authentication-type publickey
assign publickey Switch001
```

以上配置完成后，在 SWB 上建立到服务器的 SSH 连接，并指明以用户名 client002 登录：

```
<SWB> ssh2 10.0.0.1
Username: client002
Trying 10.0.0.0 ...
Press CTRL+K to abort
Connected to 10.0.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

认证成功后，进入到 SWA 的用户界面。

注意：

当设备仅支持 RSA 公钥算法时，设备作客户端登录 SSH 服务器时无需指定公钥算法，即缺省采用 RSA 公钥算法协商登录；

当设备支持 DSA 和 RSA 公钥算法时，设备作客户端登录 SSH 服务器时，建议在登录命令中指定公钥算法（identity-key），如果不指定公钥算法，缺省采用的是 DSA 公钥算法协商登录。

27.5 配置SFTP

27.5.1 SFTP 配置

SFTP相关配置

紫光集团 H3C
核心企业 数字化转型方案领导者

- 启动SFTP服务器

[SWA]sftp server enable
- 配置SSH用户并指定服务类型和认证方式

[SWA]ssh user *username* service-type { all | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey *keyname* }
- 建立与SFTP服务器的连接

<SWA>sftp server [*port-number*]

www.h3c.com

缺省情况下，SFTP 服务器处于关闭状态。所以，需要在系统视图下启动 SFTP 服务器，使客户端能用 SFTP 的方式登录到服务器。相关命令如下：

```
[SWA] sftp server enable
```

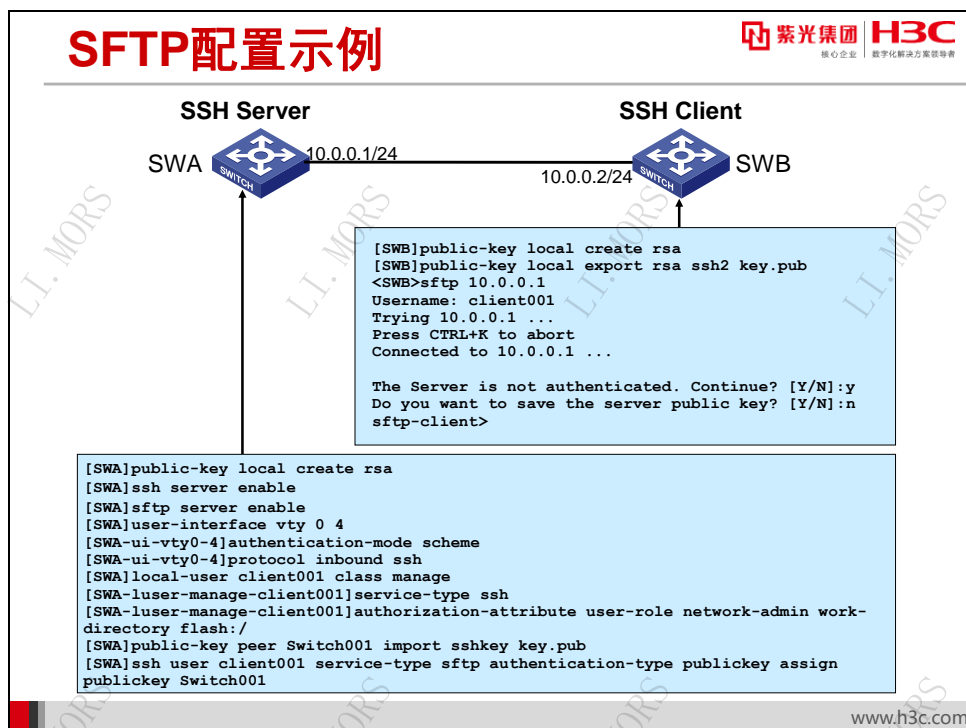
与 SSH 配置用户类似，SFTP 服务器也需要配置 SFTP 用户，并指定所使用的认证方式和工作目录。

```
[SWA] ssh user username service-type { all | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }
```

在客户端上，使用如下命令来建立与 SFTP 服务器的连接，并可以同时指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法，命令如下：

```
<SWA>sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] * [ dscp dscp-value | publickey keyname | source { interface interface-type interface-numbers | ip ip-address } ] *
```

27.5.2 SFTP 配置示例



上图所示网络中，SWA 是 SFTP 服务器，SWB 是 SFTP 客户端。SWB 作为 SFTP 客户端登录到 SWA，进行文件管理和文件传送等操作。SFTP 用户采用的认证方式为 publickey 认证，公钥算法为 RSA。

与 SSH 配置一样，需要在 SWA 上配置生成 RSA 密钥对，并启动 SSH 服务器。与此同时，为了提供 SFTP 服务，还需要在 SWA 上启动 SFTP 服务器。

```

[SWA] public-key local create rsa
[SWA] ssh server enable
[SWA] sftp server enable
  
```

设置 SFTP 客户端登录用户界面的认证方式为 AAA 认证，并设置 SWA 上远程用户登录协议为 SSH。

```

[SWA] user-interface vty 0 4
[SWA-ui-vty0-4] authentication-mode scheme
[SWA-ui-vty0-4] protocol inbound ssh
  
```

因为使用公钥认证，所以需要在 SSH 客户端 SWB 上生成 RSA 密钥对，并将生成的 RSA 主机公钥导出到指定文件 key.pub 中。

```

[SWB] public-key local create rsa
[SWB] public-key local export rsa ssh2 key.pub
  
```

客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到 SSH 服务器 SWA 上。

再返回到 SWA 上，配置从文件 key.pub 中导入客户端的公钥。

```

[SWA] public-key peer Switch001 import sshkey key.pub
  
```

设置 SFTP 用户 **client001** 的服务类型为 **SFTP**，认证方式为 **publickey**，并指定公钥为 **Switch001**，工作目录为 **flash:/**。

```
[SWA]local-user client001 class manage
[SWA-luser-manage-client001]service-type ssh
[SWA-luser-manage-client001]authorization-attribute user-role network-admin
work-directory flash:/
[SWA] ssh user client001 service-type sftp authentication-type publickey
assign publickey Switch001
```


以上配置完成后，在 **SWB** 上建立到服务器的 **SFTP** 连接，并指明以用户名 **client001** 登录：

```
<SWB> sftp 10.0.0.1 identity-key rsa
Username: client001
Trying 10.0.0.0 ...
Press CTRL+K to abort
Connected to 10.0.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp-client>
```

SWB 通过 **SFTP** 连接登录到 **SWA** 上后，可以执行显示、增加、删除目录，上传、下载文件等操作。

27.6 SSH的显示和维护

SSH的显示和维护	
	
操作	命令
在SSH服务器端显示该服务器的状态信息或会话信息	<code>display ssh server { status session }</code>
在SSH服务器端显示SSH用户信息	<code>display ssh user-information [username]</code>
显示本地密钥对中的公钥部分	<code>display public-key local { dsa ecdsa rsa } public</code>
显示保存在本地的远端主机的公钥信息	<code>display public-key peer [brief name publickey-name]</code>

完成在 SSH 服务器、客户端配置之后，可通过命令查看到配置的 SSH 服务器当前的状态和参数，当前连接的信息和 **public key** 的内容。

下表列出常用的 SSH 显示和维护命令。

表27-2 SSH 显示和维护命令

操作	命令
显示本地密钥对的公钥部分	<code>display public-key local rsa public</code>
显示保存在本地的远端公钥信息	<code>display public-key peer [brief name publickey-name]</code>
显示当前为SSH客户端设置的源IP地址或者源接口	<code>display ssh client source</code>
在SSH服务器端显示该服务器的状态信息或会话信息	<code>display ssh server { status session }</code>
在SSH客户端显示客户端保存的服务器端的主机公钥和服务器的对应关系	<code>display ssh server-info</code>
在SSH服务器端显示SSH用户信息	<code>display ssh user-information [username]</code>

27.7 本章总结

本章总结

- **SSH**是一种安全的远程登录协议
- **SSH**的两种认证方式：密码认证和公钥认证
- **SSH**安全连接有五个阶段
- **SFTP**是一种基于**SSH**协议使用的安全远程传输协议

27.8 习题和解答

27.8.1 习题

1. SSH 是____的缩写，协议号是____。
2. SSH 协议支持____、____、____三种验证方式。
3. 下列关于 SSH 的工作过程，说法正确的是____：
 - A. SSH 协商初期，SSH 客户端首先将自己支持的版本信息发送给服务器，格式为“SSH-**<主协议版本号>**.**<次协议版本号>**-**<软件版本号>**”；
 - B. 在 SSH 版本协商过程中，客户端如果发现服务器端的协议版本号比自己的低，且客户端能支持服务器端的低版本，就使用服务器端的低版本协议号；
 - C. 在 SSH 密钥和算法协商阶段，由于密钥没有建立，所以报文传输都是明文进行的；
 - D. SSH 认证阶段，认证的第一步是客户端向服务器发包含用户名的认证请求，服务器检查如果该用户存在并且需要认证，那么服务器回送一个包含认证方法的 `SSH2_MSG_USERAUTH_FAILURE` 报文，通知客户端需要认证。
4. 关于 SFTP 协议下列说法错误的是：
 - A. SFTP 是 SSH1.0 中内置的功能；
 - B. SFTP 是 Secure FTP 的简称；
 - C. SFTP 与 SSH 是两种安全协议，没有直接关系；
 - D. 配置 SFTP 服务器时用户的服务类型可以设置为 SFTP 或者 all。
5. 配置一台设备作为 SSH 服务器且选择 `publickey` 认证方式，以下哪些配置是必选的？
 - A. 启动 `ssh server` 服务；
 - B. 生成本地密钥对；
 - C. 添加 SSH 用户为 `publickey` 方式，指定用户公共密钥；
 - D. 配置用户接口的认证方式和协议类型。

27.8.2 习题答案

1. Secure Shell，22
2. 公钥验证方式，密码验证方式，不验证方式
3. ABD
4. AC
5. ABCD